IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

SEVEN NETWORKS, LLC Plaintiff, v. APPLE INC. Defendant.	Civil Action No. 2:19-cv-00115-JRG **JURY TRIAL DEMANDED**

APPLE INC.'S P.R. 3-3 AND 3-4 INVALIDITY CONTENTIONS

Pursuant to Patent Rules 3-3 and 3-4, and pursuant to the Docket Control Order entered by the Court (Dkt. 39), Defendant Apple Inc. ("Apple") respectfully submits these invalidity contentions and accompanying document production with respect to the claims identified by Plaintiff SEVEN Networks, LLC ("SEVEN") in its Patent Rule 3-1 Disclosure of Asserted Claims, Accused Instrumentalities, and Infringement Contentions. The Asserted Claims include claims 1, 3-7, 9-13, 15-17 of U.S. Patent No. 9,369,539 ("the '539 patent"); claims 1-2, 4, 8-15, 18, 20-21, 25-40 of U.S. Patent No. 9,438,550 ("the '550 patent"); claims 1-5, 7-9, 11-15, 17-19, 21-25, and 27-39 of U.S. Patent No. 9,473,914 ("the '914 patent"); claims 24-50 of U.S. Patent No. 9,516,127 ("the '127 patent"); claims 1-19 of U.S. Patent No. 9,603,056 ("the '056 patent"); claims 1-9, 11-14, 16-29, 31, 33, 35-38 of U.S. Patent No. 9,608,968 ("the '968 patent"); claims 1-28 of U.S. Patent No. 9,648,557 ("the '557 patent"); claims 1-44 of U.S. Patent No. 9,712,476 ("the '476 patent"); claims 1-29 of U.S. Patent No. 9,712,986 ("the '986 patent"); claims 1-26 of U.S. Patent No. 9,769,176 ("the '176 patent"); claims 22-28, 32, 33, 36-42, 46, 50-52 of U.S. Patent No. 10,027,619 ("the '619 patent"); claims 1-24 of U.S. Patent No. 10,039,029 ("the '029 patent"); claims 1-14 of U.S. Patent No. 10,091,734 ("the '734 patent"); claims 1-20 of U.S.

Patent No. 10,110,534 ("the '534 patent"); claims 1-30 of U.S. Patent No. 10,135,771 ("the '771 patent"); and claims 1-44 of U.S. Patent No. 10,243,962 ("the '962 patent") (collectively, "the Asserted Claims" of "the Asserted Patents").

PATENT LOCAL RULE 3-3 DISCLOSURES

1. This disclosure is directed to preliminary invalidity and unenforceability issues only and does not address claim construction or noninfringement. Apple reserves all rights with respect to such issues, including but not limited to its position that claims of the Asserted Patents are to be construed in a particular manner and are not infringed.

2. These invalidity contentions are preliminary and are based on Apple's current knowledge, understanding, and belief as to the facts and information available as of the date of these contentions. Apple has not yet completed its investigation, discovery, or analysis of information related to this action, and additional discovery may require Apple to supplement or amend its invalidity contentions. Apple reserves the right to amend or supplement its contentions once it gains access to relevant materials SEVEN has not yet produced. While Apple has made a good-faith effort to provide a comprehensive list of prior art relevant to this case, it reserves the right to modify or supplement its prior art list and invalidity contentions at a later time with or based upon pertinent information that may be subsequently discovered from SEVEN or third parties. In particular, Apple is currently unaware of the extent, if any, to which SEVEN will contend that limitations of the Asserted Claims of the Asserted Patents are not disclosed in the prior art identified in these Invalidity Contentions. Accordingly, Apple reserves the right to identify other references that would disclose the allegedly missing limitation(s) of the claimed method, device, or system. Moreover, discovery is ongoing and Apple reserves the right to pursue all other defenses that may be available to it, including but not limited to defenses that

the Asserted Patents are unenforceable based on laches, estoppel, waiver, acquiescence, inequitable conduct, patent misuse, patent exhaustion, unfair competition, unclean hands, express or implied license, or any other grounds.

3. Any invalidity analysis depends, ultimately, upon claim construction, which is a question of law reserved for the Court. The Asserted Claims have not yet been construed by the Court in this case and, thus, Apple has not yet had the opportunity to compare the Asserted Claims of the Asserted Patents (as construed by the Court) with the prior art. Apple reserves the right to amend, supplement, or materially modify its invalidity contentions after the claims have been construed by the Court. Apple also reserves the right to amend, supplement, or materially modify its invalidity contentions in response to any claim construction positions that SEVEN may take in this case. Apple also reserves the right to assert that a claim is indefinite, not enabled, or fails to meet the written description requirement based on any claim construction position SEVEN may take in this case or based on any claim construction the Court may adopt in this case.

4. Apple's invalidity contentions are directed to the claims asserted by SEVEN that are identified in SEVEN's P.R. 3-1 & 3-2 Disclosures to Apple. Apple reserves the right to modify, amend, supplement or otherwise alter its invalidity contentions in the event that SEVEN supplements or amends its infringement contentions or takes a claim construction position that is different than or in addition to those set forth in its infringement contentions, or for any other reason constituting good cause to modify, amend, supplement or otherwise alter these invalidity contentions.

5. The Court's Patent Rules and the Court's Docket Control Order (Dkt. No. 39) contemplate that these Invalidity Contentions be prepared and served in response to SEVEN's

Infringement Contentions. However, SEVEN's Infringement Contentions are insufficient, e.g., because they lack proper and complete disclosure as to how SEVEN contends that Apple allegedly infringes the Asserted Claims. Apple wrote to SEVEN regarding these deficiencies, requesting that SEVEN promptly cure them, on July 24, 2019. To date, SEVEN has not cured the defects in its contentions. Due to SEVEN's failure to provide proper and complete disclosure of its Infringement Contentions under P.R. 3-1, Apple reserves the right to seek leave from the Court to modify, amend, and/or supplement these Invalidity Contentions should SEVEN be allowed by the Court to correct, clarify, amend, and/or supplement its Infringement Contentions, or their inherent claim constructions, or following the Court's claim construction.

6. Apple further contends that SEVEN appears to be pursuing overly broad constructions of the Asserted Claims of the Asserted Patents in an effort to piece together an infringement claim where none exists and to accuse products that do not practice the claims as properly construed. At the same time, SEVEN's infringement contentions are in many places too general and vague to discern exactly how SEVEN contends each accused product practices each element of the Asserted Claims. Accordingly, these invalidity contentions are not intended to be, and are not, an admission that the Asserted Claims are infringed by any of Apple's products or technology, that any particular feature or aspect of any of the accused products practices any elements of the Asserted Claims, or that any of SEVEN's proposed constructions are supportable or proper. To the extent that any of the prior art references disclose the same functionality or feature of any of the accused products, Apple reserves the right to argue that said feature or functionality does not practice any element of any of the Asserted Claims, and to argue, in the alternative, that if said feature or functionality is found to practice any element of any of the Asserted Claims of the Asserted Patents, then the prior art reference demonstrates that

that element is not novel, is obvious, or is not patentable. These documents are not intended to reflect Apple's claim construction contentions, which will be disclosed in due course in accordance with the Patent Rules and the Court's Docket Control Order. Instead, the citation of prior art herein and the accompanying exhibits are being disclosed as, and should be construed as, nothing more than Apple's Invalidity Contentions.

7. Attached hereto are representative claim charts that demonstrate how the Asserted Claims of the Asserted Patents are invalid in view of certain prior art. The references cited in the attached claim charts may disclose the limitations of the Asserted Claims of the Asserted Patents expressly and/or inherently, and/or they may be relied upon to show the state of the art in the relevant time frame. Moreover, the suggested obviousness combinations are in the alternative to Apple's contentions regarding anticipation. These obviousness combinations should not be construed to suggest that any reference included in any combination is not anticipatory in its own right.

8. In addition to the references listed below and in the accompanying exhibits, Apple may rely upon any reference cited in the prosecution histories of the Asserted Patents as well as any additional references cited by SEVEN. Identification of elements or limitations in the contentions and the accompanying exhibits is exemplary, not exhaustive or limiting. In its contentions below and in the accompanying claim charts, Apple has endeavored to cite to the most relevant portions of the identified prior art. However, other portions of the identified prior art may additionally disclose, either expressly or inherently, and/or render obvious one or more elements of the Asserted Claims. Apple reserves the right to rely on uncited portions of the identified prior art to establish the invalidity of the Asserted Claims. Moreover, Apple reserves the right to rely on uncited portions of the identified prior art, other prior art, or expert testimony

to provide context to or aid in understanding the cited portions of the identified prior art. Where Apple cites to a particular drawing or figure, the citation encompasses the description of the drawing or figure, as well as any text associated with the drawing or figure. Similarly, where Apple cites to particular text concerning a drawing or figure, the citation encompasses that drawing or figure as well. Additional evidence regarding the features and elements of the prior art reference may be provided by witness testimony, or by additional documents that describe the prior art reference that are discovered through the course of ongoing discovery.

9. In this action, SEVEN asserts that Apple infringes certain claims of the Asserted Patents. Although SEVEN asserts that these claims are either literally infringed or infringed under the doctrine of equivalents, SEVEN has failed to provide sufficient analysis or explanation regarding alleged infringement of the Asserted Claims of the Asserted Patents under the Doctrine of Equivalents. Apple reserves the right to modify, amend, supplement or otherwise alter its preliminary invalidity contentions in the event SEVEN is permitted to modify, amend, supplement, or clarify its infringement contentions with respect to direct infringement (literal and under the doctrine of equivalents).

10. Apple is providing invalidity contentions only for the claims asserted by SEVEN, but hereby reserves the right to seek invalidation of all claims in each of the Asserted Patents.

11. Apple reserves the right to modify, amend, or supplement these disclosures as additional information becomes available, and as its discovery and investigation proceed.

I. THE '539 PATENT

A. Patent Rule 3-3(a): Identification of Prior Art

At this time, Apple contends that at least each of the prior art references described and charted in **Exhibits 539-A and 539-B** anticipates or renders obvious, either alone or in combination, one or more of the Asserted Claims of the '539 patent.

Additional prior art that has not been charted, but is still relevant to the invalidity of the '539 patent is listed in **Exhibit C**, including without limitation as evidence of the state of the art at the alleged time of invention. Apple reserves the right to amend these invalidity contentions to assert these references depending on the claim construction and infringement positions SEVEN may take as the case proceeds. Moreover, Apple reserves the right to use these references in combination with other references to render the claims of the '539 patent obvious in the event SEVEN takes the position that certain claim limitations are missing from the references charted in **Exhibits 539-A and 539-B**.

B. Patent Rule 3-3(b): Whether Each Item Anticipates or Renders Obvious the Asserted Claims

SEVEN asserts claims 1, 3-7, 9-13, and 15-17 of the '539 patent against Apple in this lawsuit. These claims are invalid because the '539 patent fails to meet one or more of the requirements for patentability. The individual bases for invalidity are provided below and in the claim charts attached as **Exhibits 539-A and 539-B**. Each of the foregoing listed prior art documents, the underlying work, and/or the underlying apparatus or method qualifies as prior art under one or more sections of 35 U.S.C. §§ 102 and/or 103.

Although Apple has identified at least one citation per limitation for each reference, each and every disclosure of the same limitation in the same reference is not necessarily identified. Rather, in an effort to focus the issues, Apple has cited representative portions of identified references, even where a reference may contain additional support for a particular claim element. In addition, persons of ordinary skill in the art generally read a prior art reference as a whole and in the context of other publications and literature. Thus, to understand and interpret any specific statement or disclosure within a prior art reference, such persons would rely on other information within the reference, along with other publications and their general scientific knowledge. Apple

may rely upon uncited portions of the prior art references and on other publications and expert testimony to provide context, and as aids to understanding and interpreting the portions that are cited. Apple may also rely on uncited portions of the prior art references, other disclosed publications, and the testimony of experts to establish that a person of ordinary skill in the art would have been motivated to modify or combine certain of the cited references so as to render the claims obvious.

1. Priority

SEVEN's Patent Rule 3-1(e) disclosures provide that the Asserted Claims of the '539 patent are entitled to a priority date of July 26, 2010, which is the filing date of U.S. Provisional Application No. 61/367,870 (the '870 Provisional) and 61/367,871 (the '871 Provisional).

Apple reserves the right to challenge SEVEN's assertion that the '539 patent is entitled to claim the benefit of these provisional applications' filing date to the extent that these provisional applications do not support the full scope of the Asserted Claims, for example, depending on scope of the Asserted Claims as properly construed. To the extent these provisional application do not support the full scope of the Asserted Claims, the priority date of the '539 patent should be the filing date of the first non-provisional patent application to which the '539 patent claims priority, which is August 25, 2014.

SEVEN has provided no evidence to support its contention that the Asserted Claims of the '539 patent are entitled to claim priority back to this or any earlier filed application, and Apple therefore reserves the right to assert a later priority date based on any findings as to the priority date of the Asserted Claims by the Court, information learned through discovery, or otherwise.

a) The Asserted Claims of the '539 Patent Cannot Claim Priority to Provisional Applications

None of the Asserted Claims are entitled to the filing date of the cited provisional applications because claims 1, 7, and 13 do not have written description support in the provisional applications. *See Falko-Gunter Falkner v. Inglis*, 448 F.3d 1357 (Fed. Cir. 2006).

Claims 1, 7, and 13 are not entitled to the provisional applications' filing date because they do not actually or inherently disclose each and every claim element. *PowerOasis, Inc. v. T-Mobile USA, Inc.*, 522 F.3d 1299, 1306-07 (Fed. Cir. 2008). All three independent claims recite power-save features, including entering and exiting a "power save mode" for synchronized devices that share a user account—features found nowhere in the provisional applications. Nothing in the provisional applications shows the inventor possessed and enabled functionalities relating to entering or exiting a "power save mode," based on user input, as recited in claims 1, 7, and 13 (e.g., claim 1 and 7—"querying a user of a first mobile . . . to select whether to enter a power save mode," claim 13—"sending the requested content . . . after the second mobile device exits the power save mode"). Thus, the provisional applications never mention entry/exit of any power save mode recited in the '539 patent claims. The provisional applications do not adequately provide written description support for user selection to enter/exit power save mode.

Further, as to claims 1, 7, and 13, the provisional applications fail to disclose content download to and from mobile devices with a shared user account that is dependent on whether either or both devices are in a power save mode. The provisional applications make no mention of content download, particularly among devices with a shared user account. For example, the '870 Provisional only describes using a server proxy to reduce "the amount of generated network traffic and shorten[] the total time and the number of times the radio module is powered up on the device, thus saving battery." *Id.* at 5. Similarly, the '871 Provisional makes reference to

sustaining "from sending any data to the Device Client. The sending may be resumed, for example, after a specified time, or by Device Client notifying user being active again," but does not describe content download among devices with a shared user account. *See* '871 Provisional at pg. 4. Consequently, the provisional applications do not actually or inherently disclose each and every element of the '539 Patent claims.

The introduction of these features into the claims resulted in the '539 patent claims not being entitled to the filing date of the provisional application, and are, at most, entitled to the filing date of August 25, 2014—the filing date of U.S. Patent Application 14/467,881.

2. Anticipation

Some or all of the Asserted Claims of the '539 patent are invalid as anticipated under 35 U.S.C. § 102 in view of each of the prior art references identified above and in the claim charts included in **Exhibit 539-A**, which identify specific examples of where each limitation of the Asserted Claims is found in the prior art references. As explained above, the cited portions of prior art references identified in the attached claim charts are exemplary only and representative of the content and teaching of the prior art references, and should be understood in the context of the reference as a whole and as they would be understood by a person of ordinary skill in the art.

Apple identifies the following references as anticipating one or more of the Asserted Claims of the '539 patent under 35 U.S.C. § 102. The below table of anticipating references is exemplary, and it does not constitute an admission that any reference anticipates only the listed claims. Further, Apple contends that any prior art reference in the attached charts that is charted for each limitation of any given claim, anticipates that claim, regardless of whether that prior art reference is listed in the following table.

Ex. #	Anticipating Prior Art	Claims
539-A1	U.S. Patent Application 2011/0080422 Al to Kang Lee et al. ("Lee")	1, 3-6, 9-12, 15-17
539-A2	U.S. Patent Publication No. US 2008/0243370 Al to Noam Lando et al. ("Lando")	1, 3-7, 9-12, 15-17
539-A3	U.S. Patent Application No. 9,386,075 B2 to Aldo Adriazola ("Adriazola")	1, 3-7, 9-12, 15-17
539-A4	U.S. Patent Application 2010/0042856 Al to Chieh-Chih Tsai et al. ("Tsai")	1, 3-7, 9-12, 15-17
539-A5	Nokia E72 System	1, 3-7, 9-12, 15-17
539-A6	U.S. Patent 8,904,206 B2 to Gregory Black et al. ("Black")	1, 3-7, 9-12, 15-17
539-A7	U.S. Patent 7,525,289 B2 to Craig Janik et al. ("Janik")	1, 3-7, 9-12, 15-17

To the extent any item of prior art cited above is deemed not to disclose, explicitly or inherently, any limitation of an Asserted Claim of the '539 patent, Apple reserves the right to argue that any difference between that prior art and the corresponding patent claim would have been either inherent to the art, or obvious to a person of ordinary skill in the art, even if Apple has not specifically denoted that the art is to be combined with the knowledge of a person of ordinary skill in the art.

3. Obviousness

To the extent any limitation is deemed not to be exactly met by an item of prior art listed above and in **Exhibit 539-A**, then any purported differences are such that the claimed subject matter as a whole would have been obvious to one skilled in the art at the time of the alleged invention, in view of the state of the art and knowledge of those skilled in the art. The item of prior art would, therefore, render the relevant claims invalid for obviousness under 35 U.S.C. § 103.

In addition, the references identified above render one or more Asserted Claims of the '539 patent obvious when the references are read in combination with each other, and/or when read in view of the state of the art and knowledge of those skilled in the art. Each and every

reference identified is also relevant to the state of the art at the time of the alleged invention. Any of the references disclosed above may be combined with one another to render obvious (and therefore invalid) each of SEVEN's Asserted Claims. Apple may rely upon a subset of the above identified references or all of the references identified above, including all references in **Exhibits 539-A and 539-B, and C**, for purposes of obviousness depending on the Court's claim construction, positions taken by SEVEN during this litigation, and further investigation and discovery.

To the extent the foregoing references are found not to anticipate the Asserted Claims, the foregoing references render the Asserted Claims obvious either alone or in combination with one or more of the other references identified above pursuant to Patent Rule 3-3(a). It would have been obvious to a person of skill in the art at the time of the alleged invention of the Asserted Claims of the '539 patent to combine the various references cited herein so as to disclose the Asserted Claims of the '539 patent.

In accordance with Patent Rule 3-3(b), prior art references rendering the Asserted Claims obvious, alone or in combination with other references, are outlined below and included in **Exhibits 539-A and 539-B**, which include exemplary claim charts for the Asserted Claims of the '539 patent showing specifically where in each reference or combinations of references each Asserted Claim is found, and an explanation of why the prior art renders the Asserted Claim obvious. Where applicable, **Exhibits 539-A and 539-B** include the motivation to combine references.

Moreover, in addition to the information contained elsewhere in these contentions and in particular **Exhibit 539-B**, Apple has identified additional motivations and reasons to combine the various references cited herein. In particular, multiple teachings, suggestions, and/or reasons to

modify any of the references and/or to combine any two or more of the references in **Exhibits 539-A and 539-B** come from many sources, including the prior art (specific and as a whole), common knowledge, common sense, predictability, expectations, industry trends, design incentives or need, market demand or pressure, market forces, obvious to try, the nature of the problem faced, and/or knowledge possessed by one of ordinary skill. In addition, it would have been obvious to try combining the prior art references identified above because there were only a finite number of predictable solutions and/or because known work in one field or endeavor prompted variations based on predictable design incentives and/or market forces either in the same field or a different one. The combination of prior art references identified in these contentions would have been obvious because the claimed combinations represent the known potential options with a reasonable expectation of success. Additionally, one of ordinary skill in the art would have been motivated to create combinations identified in these contentions using: known methods to yield predictable results; known techniques in the same way; a simple substitution of one known, equivalent element for another to obtain predictable results; and/or teaching, suggestion, or motivation in the prior art generally. Also, market forces in the industry, and the desire to improve features and performance, would motivate the addition of features to systems as they become available, become less expensive, become more commonly used, provide better performance, reduce costs, size or weight, or predictably achieve other clearly desirable results.

While Apple reserves the right to rely on any combination of the references reflected in their charts or incorporated herein by reference, Apple provides the following exemplary and non-exhaustive references and/or combinations evidencing invalidity of the claims of the Asserted Patents. The combinations of prior art listed below render obvious the Asserted Claims

under the proper construction of the claims and/or under Plaintiff's apparent interpretation of the claims as set forth by Plaintiff in their Complaint and Infringement Contentions. Each combination renders the identified claims obvious through the express and/or inherent disclosure in the combination of references themselves, as well as in view of the knowledge of a person of ordinary skill in the art.

Obviousness Combinations	Claims
U.S. Patent Publication US 2008/024370 A1 to Noam Lando et al. ("Lando"), in view of one or more of US 2010/0042856 Al to Chieh-Chih Tsai et al. ("Tsai"), and/or US 7,525,289 B2 to Craig Janik et al. ("Janik")	1, 3-7, 9-13, and 15-17
Lando in view of one or more of U.S. Patent No. 9,386,075 B2 to Aldo Adriazola ("Adriazola") and/or U.S. Patent Application 2009/0217065 A1 to Nelson S. Araujo Jr. ("Araujo")	1, 3-7, 9-13, and 15-17
Lee in view of one or more of Adriazola and/or Araujo	1, 3-7, 9-13, and 15-17
Tsai in view of one or more of Lee and/or Adriazola	1, 3-7, 9-13, and 15-17
Tsai in view of one or more of Lando and/or Adriazola	1, 3-7, 9-13, and 15-17
Tsai in view of one or more of Lee, Adriazola, and/or Araujo	1, 3-7, 9-13, and 15-17
Tsai in view of one or more of Lando, Adriazola, and/or Araujo	1, 3-7, 9-13, and 15-17
Tsai in view one or more of Lando and/or Lee	1, 3-7, 9-13, and 15-17
Janik in view of one or more of Adriazola, Tsai, Lando, and/or Lee	1, 3-7, 9-13, and 15-17
Nokia E72 System ("Nokia E72") in view of Adriazola	1, 3-7, 9-13, and 15-17
U.S. Patent 8,904,206 B2 to Gregory Black et al. ("Black") in view of one or more of Janik, Tsai, Lee, Lando, Nokia E72 and/or Adriazola	1, 3-7, 9-13, and 15-17
Lee in view of one or more of Adriazola, Araujo, Lando, Tsai, Janik, Black, Nokia 72, COMBINE: Leveraging the Power of Wireless Peers through Collaborative Downloading, Ganesh Ananthanarayanan et al., MobiSys'07, June 11–14, 2007, San Juan, Puerto Rico, USA ("Combine"), and/or U.S. Patent 5,991,287 A to Diepstraten et al. ("Diepstraten")	1, 3-7, 9-13, and 15-17
Adriazola in view of one or more of Lando, Lee, Tsai, Janik, Nokia E72, Black, US2008/0144559A1 to Victor Griswold ("Griswold"), U.S. Patent 7,724,697 B2 to Lars Dalsgaard ("Dalsgard"), 2008/0146292 A1 to Edward Gilmore ("Gilmore"), U.S. 2007/0266106 A1 to Ayako Kato ("Kato"), and/or U.S. 2010/0174501 to Srikanth Myadam ("Myadam")	1, 3-7, 9-13, and 15-17

Adriazola in view of one or more of Tsai, Lando, and/or U.S. 9400893 B2 to Erick Tseng, et al. ("Tseng")	1, 3-7, 9-13, and 15-17
Adriazola in view of Lee, Tsai, Lando, Araujo, Combine, Griswold, Gilmore, Dalsgaard, Kato, Black, Diepstraten, and/or Nokia E72	1, 3-7, 9-13, and 15-17
Adriazola in view one or more of of Lee Lando, Griswold, Dalsgaard, Tsai, and/or Araujo	1, 3-7, 9-13, and 15-17
Lee in view of one or more of Adriazola, Myadam, Kato, Janik, Nokia E72, Adriazola, Lando, and/or Black	1, 3-7, 9-13, and 15-17
Adriazola in view of one or more of Lee, Tsai, Lando, Janik, Combine, Griswold, and/or Nokia E72	1, 3-7, 9-13, and 15-17
Lee in view of one or more of Diepstraten, Black, Janik, Tsai, Araujo, and/or Lando	1, 3-7, 9-13, and 15-17

In addition to the specific combinations of prior art and the specific combinations of groups of prior art disclosed above, Apple reserves the right to rely on any other combination of any prior art references disclosed herein. Apple further reserves the right to rely upon combinations disclosed within the prosecution history of the references cited herein. These obviousness combinations reflect Apple's present understanding of the potential scope of the claims that SEVEN appears to be advocating and should not be seen as Apple's acquiescence to SEVEN's interpretation of the patent claims.

Apple also reserves the right to amend or supplement these contentions regarding anticipation or obviousness of the Asserted Claims, in view of further information from SEVEN, information discovered during discovery, or a claim construction ruling by the Court. SEVEN has not identified what elements or combinations it alleges were not known to one of ordinary skill in the art at the time. Therefore, for any claim limitation that SEVEN alleges is not disclosed in a particular prior art reference, Apple reserves the right to assert that any such limitation is either inherent in the disclosed reference or obvious to one of ordinary skill in the art at the time in light of the same, or that the limitation is disclosed in another of the references disclosed above and in combination would have rendered the Asserted Claim obvious.

C. Patent Rule 3-3(c): Charts Identifying Where Specifically in Each Alleged Item of Prior Art Each Asserted Claim Is Found

Pursuant to Patent Rule 3-3(c), charts identifying where specifically in each alleged item of prior art each limitation of each Asserted Claim is found, including for each limitation that Apple contends is governed by 35 U.S.C. § 112(6), the identity of the structure(s), act(s), or material(s) in each item of prior art that performs the claimed function, are attached in **Exhibits 539-A and 539-B**.

D. Patent Rule 3-3(d): Other Grounds for Invalidity

Apple identifies the following grounds for invalidity of the Asserted Claims of the '539 patent based on 35 U.S.C. §§ 101 and/or 112. Apple reserves the right to supplement these disclosures based on further investigation and discovery.

1. Invalidity Pursuant to 35 U.S.C. § 112

Apple further asserts that the Asserted Claims of the '539 patent are invalid under 35 U.S.C. § 112. The following are the grounds upon which Apple contends the Asserted Claims are invalid for failure to meet the requirements of 35 U.S.C. § 112, ¶ 1, ¶ 2, ¶ 4 and/or ¶ 6, based on Apple's investigation to date and currently-available information.

For each claim identified as invalid, any dependent claims of those invalid claims are also invalid under 35 U.S.C. § 112, ¶ 1, ¶ 2, ¶ 4, and/or ¶ 6. Apple reserves the right to supplement and amend these contentions based on further discovery and investigation including, in particular, the deposition of any of the named inventors of the Asserted Patent, the parties' claim construction positions, and further investigation of SEVEN's implied infringement positions.

a) Written Description and/or Enablement

At least in view of SEVEN's apparent construction of the claims in its Infringement Contentions, the Asserted Claims of the '539 patent are invalid because the specification as filed

does not contain adequate written description of the claimed inventions sufficient to lead a person of ordinary skill in the art to understand that the named inventors had possession of the purported inventions as claimed as required by 35 U.S.C. § 112, ¶ 1. Likewise, the specification does not enable one of ordinary skill in the art to make or use the claimed inventions without undue experimentation. Based on Apple's present understanding of SEVEN's infringement contentions, Apple asserts that the Asserted Claims of the of the '539 patent are invalid for reciting at least the following claim terms/phrases/limitations:

- Claims 1, 7, and 13 of the '539 patent and its dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain an adequate written description and/or enabling disclosure of "optimizing traffic at the mobile device by blocking transmission of at least some traffic from the mobile device." The specification, as filed, does not contain describe "blocking transmission of at least some traffic from the mobile" as a means for "optimizing traffic." The patent does not describe "blocking" with respect to data requests. Accordingly, the specification fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.
- Claims 1, 7, and 13 of the '539 patent and its dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain an adequate written description and/or enabling disclosure of "wherein content selected for download at the another mobile device from a server is delayed for download at the mobile device when

the mobile device is in the power save mode." The specification as filed does not contain an adequate written description and/or enabling disclosure of the various rules that must govern the mobile device "while in the power save mode," versus the rules when the device "is not in the power save mode," or "exits the power save mode." Rather, to the extent these rules find any support in the patent specification at all, they appear to be randomly selected from disparate sections of the patent describing the behavior of the device in various contexts. The patent does not specify which of these behaviors would apply while "in" a power save mode versus when the device is "out" of the power save mode. Further, the specification fails to describe downloading, and delaying for download, content available at another mobile device. Accordingly, the specification fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

- Claims 1, 7, and 13 of the '539 patent and its dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain an adequate written description and/or enabling disclosure of "wherein another mobile device shares a same user account with the mobile device." The specification, as filed, does not contain an adequate description and/or enabling disclosure of multiple mobile devices sharing a same user account. To the extent the term the term "CE account" ('539 Patent at 23:15-20) is construed to mean more than a user account, as identified in the '539 patent specification, the full scope of the claimed subject matter is not

described or enabled. The phrase "same user account" is not used in the patent's specification, and the patent's disclosures do not otherwise describe or enable the requirement that at least two mobile devices "share[] a same user account." Accordingly, the specification fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

- Claims 1, 7, and 13 of the '539 patent and its dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain an adequate written description and/or enabling disclosure of "querying a user by displaying a notification on a user interface of the mobile device to select whether to enter a power save mode." The specification, as filed, does not contain an adequate description and/or enabling disclosure of a notification on a user interface that prompts the user to enter into a power save mode. The phrase "querying a user" is not used in the patent's specification, and the patent's disclosures do not otherwise describe or enable the requirement that a user is prompted by a notification on the user interface to enter into a power save mode. Accordingly, the specification fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

The limitations requiring "optimizing traffic" at the mobile device "by blocking transmission of at least some traffic" from the mobile device, also lacks written description support and/or is not enabled, at least to the extent that SEVEN contends this limitation is

satisfied by Apple's products. Apple's accused products do not "optimize traffic" by "blocking transmission of at least some traffic." The feature that SEVEN identifies in its infringement contentions does not include "blocking transmission" of traffic at the mobile device. Thus, to the extent the claim is interpreted broad enough to encompass to include features that extend beyond "blocking transmission," this limitation lacks § 112 support.

b) Indefiniteness

At least in view of SEVEN's apparent construction of the claims in its Infringement Contentions, the Asserted Claims of the '539 patent are invalid because they fail to particularly point out and distinctly claim the subject matter which the applicant regards as his invention under 35 U.S.C. § 112, ¶¶ 2, 4, and/or 6. Based on Apple's present understanding of SEVEN's infringement contentions, Apple asserts that the Asserted Claims of the of the '539 patent are invalid for reciting at least the following claim terms/phrases/limitations:

- Claims 5, 11, and 16 of the '539 patent and its dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 2, ¶ 4, and/or ¶ 6 because the specification does not describe or otherwise inform one of ordinary skill about what constitutes "instructions from the user." The '539 patent does not describe or explain how the user instructs the mobile device to exit the power-save mode. As such, one of ordinary skill would not understand the metes and bounds of the identified claims, rendering them indefinite under 35 U.S.C. § 112, ¶ 2. Therefore, the Asserted Claims, when read in light of the specification and the prosecution history, "fail to inform, with reasonable certainty, those skilled in the art about the scope of the invention." *Nautilus, Inc. v. Biosig Instruments, Inc.*, 134 S. Ct. 2120, 2124 (2014).

2. Other Grounds for Invalidity

In addition to the preceding invalidity contentions, Apple further contends that each of the Asserted Claims of the '539 patent is drawn to subject matter that is not patentable under 35 U.S.C. § 101. The '539 patent Asserted Claims are invalid under 35 U.S.C. § 101 for failure to recite patent eligible subject matter. Specifically, all claims of the '539 patent are fatally abstract under the U.S. Supreme Court's decision in *Alice Corp. v. CLS Bank Int'l*, 134 S. Ct. 2345 (2014) and progeny. The ideas presented in the claims are generally directed to concepts of delaying content download when devices are in a power save mode, and selecting and transmitting content when the devices exit a power-save mode. Under *Alice* Step 1, those ideas are abstract, as they relate to a fundamental long prevalent practice. *See Intellectual Ventures I LLC v. Symantec Corp*., 838 F.3d 1307, 1314 (Fed. Cir. 2016). Limiting the invention to a particular technological environment, e.g. generic computer hardware, "do[es] not render an otherwise abstract concept any less abstract." *Intellectual Ventures I LLC v. Capital One Fin. Corp*., 850 F.3d 1332, 1340 (Fed Cir. 2017). Furthermore, because the patent relates to transmission of information, it is likewise abstract, as "information is … an intangible." *Electric Power Group, LLC v. Alstom S.A.*, 830 F.3d 1350, 1353 (Fed. Cir. 2016). Furthermore, under *Alice* Step 2 the '539 patent does not contain any inventive concept. The '539 patent Asserted Claims employs well-known components or functionality, as shown in Apple's invalidity contentions involving anticipation and/or obviousness in this case, which is not enough to impart patent eligibility of an abstract idea. *See, e.g., Alice*, 134 S. Ct. at 2359 (holding that limitations describing "'well-understood, routine, conventional activit[ies]' previously known to the industry" were insufficient to supply an inventive concept (quoting *Mayo*, 132 S. Ct. at 1294)). Further detail regarding Apple's contentions that the Asserted Claims of the '539 patent do not qualify as patent-eligible subject matter are contained in **Exhibit 539-D.**

Apple reserves the right to assert that the asserted patents are invalid under 35 U.S.C. §102(f) and/or (g) in the event Apple obtains evidence that the named inventors of the ’539 patent did not invent (either alone or in conjunction with other parties) the subject matter claimed in the ’539 patent. Should Apple obtain such evidence, it will provide the name of the person(s) from whom and the circumstances under which the invention or any part of it was derived, and/or the circumstances surrounding the making of the invention before the patent application.

Apple reserves the right to supplement these disclosures based on further investigation and discovery.

II. THE ’550 PATENT

A. Patent Rule 3-3(a): Identification of Prior Art

At this time, Apple contends that at least each of the prior art references described and charted in **Exhibits 550-A and 550-B** anticipates or renders obvious, either alone or in combination, one or more of the Asserted Claims of the ’550 patent.

Additional prior art that has not been charted, but is still relevant to the invalidity of the ’550 patent is listed in **Exhibit C**, including without limitation as evidence of the state of the art at the alleged time of invention. Apple reserves the right to amend these invalidity contentions to assert these references depending on the claim construction and infringement positions SEVEN may take as the case proceeds. Moreover, Apple reserves the right to use these references in combination with other references to render the claims of the ’550 patent obvious in the event SEVEN takes the position that certain claim limitations are missing from the references charted in **Exhibits 550-A and 550-B**.

B. Patent Rule 3-3(b): Whether Each Item Anticipates or Renders Obvious the Asserted Claims

SEVEN asserts claims 1-2, 4, 8-15, 18, 20-21, 25-40 of the ’550 patent against Apple in this lawsuit. These claims are invalid because the ’550 patent fails to meet one or more of the requirements for patentability. The individual bases for invalidity are provided below and in the claim charts attached as **Exhibits 550-A and 550-B**. Each of the foregoing listed prior art documents, the underlying work, and/or the underlying apparatus or method qualifies as prior art under one or more sections of 35 U.S.C. §§ 102 and/or 103.

Although Apple has identified at least one citation per limitation for each reference, each and every disclosure of the same limitation in the same reference is not necessarily identified. Rather, in an effort to focus the issues, Apple has cited representative portions of identified references, even where a reference may contain additional support for a particular claim element. In addition, persons of ordinary skill in the art generally read a prior art reference as a whole and in the context of other publications and literature. Thus, to understand and interpret any specific statement or disclosure within a prior art reference, such persons would rely on other information within the reference, along with other publications and their general scientific knowledge. Apple may rely upon uncited portions of the prior art references and on other publications and expert testimony to provide context, and as aids to understanding and interpreting the portions that are cited. Apple may also rely on uncited portions of the prior art references, other disclosed publications, and the testimony of experts to establish that a person of ordinary skill in the art would have been motivated to modify or combine certain of the cited references so as to render the claims obvious.

1. Priority

SEVEN's Patent Rule 3-1(e) disclosures provide that the Asserted Claims of the '550 patent are entitled to a priority date of January 8, 2002, which is the filing date of U.S. Provisional Application No. 60/346,881 ("the '881 Provisional"). SEVEN has provided no evidence to support its contention that the Asserted Claims of the '550 patent are entitled to claim priority back to this or any earlier filed application. As stated below, the '550 patent is not entitled to claim priority to any earlier application. Thus, the priority date for the Asserted Claims should be the filing date of the '550 patent.

The provisional and non-provisional applications to which SEVEN claims priority must "contain a written description of the invention and the manner and process of making and using it, in such full, clear, concise, and exact terms," 35 U.S.C. § 112 ¶ 1, to enable a POSITA to practice the invention claimed in the non-provisional application. *Id*.

a) The Asserted Claims of the '550 Patent Cannot Claim Priority to the '249 Provisional

The Asserted Claims are not entitled to the filing date of the Provisional Application No. 60/403,249 ("the '249 Provisional") because they do not have written description support in the '249 Provisional. *See Falko-Gunter Falkner v. Inglis*, 448 F.3d 1357 (Fed. Cir. 2006).

All of the Asserted Claims recite features relating to power management modes, such as "selecting," "entering," and "exiting" these modes, and using a "predetermined amount of battery to determine when the device should operate in certain modes, and adjusting the "frequency" of some (but not all) "application data requests." None of these features are disclosed in the '249 provisional in the context of a mobile device. Thus, nothing in the '249 provisional application shows the inventor possessed and enabled these functionalities recited in claims 1, 15, and 32.

b) The Asserted Claims of the ’550 Patent Cannot Claim Priority to the ’881 Provisional

The Asserted Claims are not entitled to the filing date of the ’881 Provisional because they do not have written description support in the ’881 Provisional. *See Falko-Gunter Falkner v. Inglis*, 448 F.3d 1357 (Fed. Cir. 2006).

All of the Asserted Claims recite features relating to power management modes, such as “selecting,” “entering,” and “exiting” these modes, and using a “predetermined amount of battery to determine when the device should operate in certain modes, and adjusting the “frequency” of some (but not all) “application data requests.” None of these features are disclosed in the ’881 provisional. Thus, nothing in the ’881 provisional application shows the inventor possessed and enabled these functionalities recited in claims 1, 15, and 32.

c) The Asserted Claims of the ’550 Patent Cannot Claim Priority to the ’565 Patent

The Asserted Claims are not entitled to the filing date of U.S. Patent No. 7,139,565 (“the ’565 patent”) because they do not find written description support in the ’565 patent. *See Falko-Gunter Falkner v. Inglis*, 448 F.3d 1357 (Fed. Cir. 2006).

All of the Asserted Claims recite features relating to “power management modes,” “selecting” a power management mode, “entering”/“exiting” power management modes, “normal operation mode,” “low power mode,” using a “predetermined amount” of battery to determine when the device should operate in certain modes, and adjusting the “frequency” of some (but not all) “application data requests.” None of these features are disclosed in the ’565 patent, to which the ’550 patent claims priority.

2. Anticipation

Some or all of the Asserted Claims of the ’550 patent are invalid as anticipated under 35 U.S.C. § 102 in view of each of the prior art references identified above and in the claim charts

included in **Exhibit 550-A**, which identify specific examples of where each limitation of the Asserted Claims is found in the prior art references. As explained above, the cited portions of prior art references identified in the attached claim charts are exemplary only and representative of the content and teaching of the prior art references, and should be understood in the context of the reference as a whole and as they would be understood by a person of ordinary skill in the art.

Apple identifies the following references as anticipating one or more of the Asserted Claims of the '550 patent under 35 U.S.C. § 102. The below table of anticipating references is exemplary, and it does not constitute an admission that any reference anticipates only the listed claims. Further, Apple contends that any prior art reference in the attached charts that is charted for each limitation of any given claim, anticipates that claim, regardless of whether that prior art reference is listed in the following table.

Ex. #	Anticipating Prior Art	Claims
550-A1	Toshiba e570 Pocket PC ("e570")	1-2, 4, 8-15, 18, 20-21, 25-40
550-A2	Windows CE system ("Windows CE")	1-2, 4, 8-15, 18, 20-21, 25-40
550-A3	Japanese Patent Publication No. 2000/0000092204 to Hasegawa ("Hasegawa")	1-2, 4, 8-15, 18, 20-21, 25-40
550-A4	U.S. Patent No. 6,697,953 to Collins ("Collins")	1-2, 4, 8-15, 18, 20-21, 25-40
550-A5	U.S. Patent No. 7,231,198 to Loughran ("Loughran")	1-2, 4, 8-15, 18, 20-21, 25-40
550-A6	NEC Computers International Pocket PC 2002 ("Pocket PC")	1-2, 4, 8-15, 18, 20-21, 25-40
550-A7	U.S. Patent No. 6,842,433 to West et al. ("West")	1-2, 4, 8-15, 18, 20-21, 25-40
550-A8	U.S. Patent No. 5,870,685 to Flynn ("Flynn")	1-2, 4, 8-15, 18, 20-21, 25-40
550-A9	U.S. Patent No. 6,631,469 to Kelan Silvester ("Silvester")	1-2, 4, 8-15, 18, 20-21, 25-40
550-10	HP Jornada 720 Handheld PC ("Jornada")	1-2, 4, 8-15, 18, 20-21, 25-40
550-11	U.S. Patent No. 6,275,712 to Gray et al. ("Gray")	1-2, 4, 8-15, 18, 20-21, 25-40

550-12	"Windows CE 3.0: Application Programming" authored by Nick Grattan & Marshall Brain ("Grattan")	1-2, 4, 8-15, 18, 20-21, 25-40
550-13	U.S. Patent No. 5,944,829 to Shimoda ("Shimoda")	1-2, 4, 8-15, 18, 20-21, 25-40
550-14	U.S. Patent No. 7,185,211 to Loughran ("Loughran 2")	1-2, 4, 8-15, 18, 20-21, 25-40

To the extent any item of prior art cited above is deemed not to disclose, explicitly or inherently, any limitation of an Asserted Claim of the '550 patent, Apple reserves the right to argue that any difference between that prior art and the corresponding patent claim would have been either inherent to the art, or obvious to a person of ordinary skill in the art, even if Apple has not specifically denoted that the art is to be combined with the knowledge of a person of ordinary skill in the art.

3. Obviousness

To the extent any limitation is deemed not to be exactly met by an item of prior art listed above and in **Exhibit 550-A**, then any purported differences are such that the claimed subject matter as a whole would have been obvious to one skilled in the art at the time of the alleged invention, in view of the state of the art and knowledge of those skilled in the art. The item of prior art would, therefore, render the relevant claims invalid for obviousness under 35 U.S.C. § 103.

In addition, the references identified above render one or more Asserted Claims of the '550 patent obvious when the references are read in combination with each other, and/or when read in view of the state of the art and knowledge of those skilled in the art. Each and every reference identified is also relevant to the state of the art at the time of the alleged invention. Any of the references disclosed above may be combined with one another to render obvious (and therefore invalid) each of SEVEN's Asserted Claims. Apple may rely upon a subset of the

above identified references or all of the references identified above, including all references in **Exhibits 550-A, 550-B, and C**, for purposes of obviousness depending on the Court's claim construction, positions taken by SEVEN during this litigation, and further investigation and discovery.

To the extent the foregoing references are found not to anticipate the Asserted Claims, the foregoing references render the Asserted Claims obvious either alone or in combination with one or more of the other references identified above pursuant to Patent Rule 3-3(a). It would have been obvious to a person of skill in the art at the time of the alleged invention of the Asserted Claims of the '550 patent to combine the various references cited herein so as to disclose the Asserted Claims of the '550 patent.

In accordance with Patent Rule 3-3(b), prior art references rendering the Asserted Claims obvious, alone or in combination with other references, are outlined below and included in **Exhibits 550-A and 550-B**, which include exemplary claim charts for the Asserted Claims of the '550 patent showing specifically where in each reference or combinations of references each Asserted Claim is found, and an explanation of why the prior art renders the Asserted Claim obvious. Where applicable, **Exhibits 550-A and 550-B** include the motivation to combine references.

Moreover, in addition to the information contained elsewhere in these contentions and in particular **Exhibit 550-B**, Apple has identified additional motivations and reasons to combine the various references cited herein. In particular, multiple teachings, suggestions, and/or reasons to modify any of the references and/or to combine any two or more of the references in **Exhibits 550-A and 550-B** come from many sources, including the prior art (specific and as a whole), common knowledge, common sense, predictability, expectations, industry trends, design

incentives or need, market demand or pressure, market forces, obvious to try, the nature of the problem faced, and/or knowledge possessed by one of ordinary skill. In addition, it would have been obvious to try combining the prior art references identified above because there were only a finite number of predictable solutions and/or because known work in one field or endeavor prompted variations based on predictable design incentives and/or market forces either in the same field or a different one. The combination of prior art references identified in these contentions would have been obvious because the claimed combinations represent the known potential options with a reasonable expectation of success. Additionally, one of ordinary skill in the art would have been motivated to create combinations identified in these contentions using: known methods to yield predictable results; known techniques in the same way; a simple substitution of one known, equivalent element for another to obtain predictable results; and/or teaching, suggestion, or motivation in the prior art generally. Also, market forces in the industry, and the desire to improve features and performance, would motivate the addition of features to systems as they become available, become less expensive, become more commonly used, provide better performance, reduce costs, size or weight, or predictably achieve other clearly desirable results.

While Apple reserves the right to rely on any combination of the references reflected in their charts or incorporated herein by reference, Apple provides the following exemplary and non-exhaustive references and/or combinations evidencing invalidity of the claims of the Asserted Patents. The combinations of prior art listed below render obvious the Asserted Claims under the proper construction of the claims and/or under Plaintiff's apparent interpretation of the claims as set forth by Plaintiff in their Complaint and Infringement Contentions. Each combination renders the identified claims obvious through the express and/or inherent disclosure

in the combination of references themselves, as well as in view of the knowledge of a person of ordinary skill in the art.

Obviousness Combinations	Claims
Jornada in view of Hasegawa	All Asserted Claims
Jornada in view of Collins	All Asserted Claims
Pocket PC 2002 in view of Hasegawa	All Asserted Claims
Pocket PC 2002 in view of Collins	All Asserted Claims
Pocket PC 2002 in view of Gray in further view of Windows CE	All Asserted Claims
Pocket PC 2002 in view of Gray in further view of Grattan	All Asserted Claims
e570 in view of Collins	All Asserted Claims
e570 in view of Hasegawa	All Asserted Claims
e570 in view of Gray in further view of West	All Asserted Claims
Jornada in view of Windows CE	All Asserted Claims
Jornada in view of Gray in further view of West	All Asserted Claims
Pocket PC 2002 in view of Collins in further view of Shimoda	All Asserted Claims
Jornada in view of Collins in further view of Loughran	All Asserted Claims
Jornada in view of Hasegawa in further view of Shimoda	All Asserted Claims
Hasegawa in view of Shimoda in further view of Gray	All Asserted Claims
Loughran in view of Jornada	All Asserted Claims
Loughran in view of e570	All Asserted Claims
Loughran in view of Pocket PC 2002	All Asserted Claims
Pocket PC 2002 in view of Loughran in further view of Hasegawa	All Asserted Claims
Loughran in view of Hasegawa	All Asserted Claims
Pocket PC 2002 in view of Shimoda in further view of Hasegawa	All Asserted Claims
Pocket PC 2002 in view of Loughran 2 in further view of Hasegawa	All Asserted Claims
e570 in view of Loughran 2	All Asserted Claims
Jornada in view of Loughran 2	All Asserted Claims
Windows CE in view of Loughran and in further view of Loughran 2	All Asserted Claims
Jornada in view of Collins in further view of Loughran 2	All Asserted Claims

In addition to the specific combinations of prior art and the specific combinations of groups of prior art disclosed above, Apple reserves the right to rely on any other combination of any prior art references disclosed herein. Apple further reserves the right to rely upon

combinations disclosed within the prosecution history of the references cited herein. These obviousness combinations reflect Apple's present understanding of the potential scope of the claims that SEVEN appears to be advocating and should not be seen as Apple's acquiescence to SEVEN's interpretation of the patent claims.

Apple also reserves the right to amend or supplement these contentions regarding anticipation or obviousness of the Asserted Claims, in view of further information from SEVEN, information discovered during discovery, or a claim construction ruling by the Court. SEVEN has not identified what elements or combinations it alleges were not known to one of ordinary skill in the art at the time. Therefore, for any claim limitation that SEVEN alleges is not disclosed in a particular prior art reference, Apple reserves the right to assert that any such limitation is either inherent in the disclosed reference or obvious to one of ordinary skill in the art at the time in light of the same, or that the limitation is disclosed in another of the references disclosed above and in combination would have rendered the Asserted Claim obvious.

C. Patent Rule 3-3(c): Charts Identifying Where Specifically in Each Alleged Item of Prior Art Each Asserted Claim Is Found

Pursuant to Patent Rule 3-3(c), charts identifying where specifically in each alleged item of prior art each limitation of each Asserted Claim is found, including for each limitation that Apple contends is governed by 35 U.S.C. § 112(6), the identity of the structure(s), act(s), or material(s) in each item of prior art that performs the claimed function, are attached in **Exhibits 550-A and 550-B**.

D. Patent Rule 3-3(d): Other Grounds for Invalidity

Apple identifies the following grounds for invalidity of the Asserted Claims of the '550 patent based on 35 U.S.C. §§ 101 and/or 112. Apple reserves the right to supplement these disclosures based on further investigation and discovery.

1. Invalidity Pursuant to 35 U.S.C. § 112

Apple further asserts that the Asserted Claims of the '550 patent are invalid under 35 U.S.C. § 112. The following are the grounds upon which Apple contends the Asserted Claims are invalid for failure to meet the requirements of 35 U.S.C. § 112, ¶ 1, ¶ 2, ¶ 4 and/or ¶ 6, based on Apple's investigation to date and currently-available information.

For each claim identified as invalid, any dependent claims of those invalid claims are also invalid under 35 U.S.C. § 112, ¶ 1, ¶ 2, ¶ 4, and/or ¶ 6. Apple reserves the right to supplement and amend these contentions based on further discovery and investigation including, in particular, the deposition of any of the named inventors of the Asserted Patent, the parties' claim construction positions, and further investigation of SEVEN's implied infringement positions.

a) Written Description and/or Enablement

At least in view of SEVEN's apparent construction of the claims in its Infringement Contentions, the Asserted Claims of the '550 patent are invalid because the specification as filed does not contain adequate written description of the claimed inventions sufficient to lead a person of ordinary skill in the art to understand that the named inventors had possession of the purported inventions as claimed as required by 35 U.S.C. § 112, ¶ 1. Likewise, the specification does not enable one of ordinary skill in the art to make or use the claimed inventions without undue experimentation. Based on Apple's present understanding of SEVEN's infringement contentions, Apple asserts that the Asserted Claims of the of the '550 patent are invalid for reciting at least the following claim terms/phrases/limitations:

- Claims 1, 15, and 32 of the '550 patent and their dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain an adequate written description and/or enabling disclosure of numerous claim limitations. The specification support for

the claims is minimal. For example, all of the '550 patent Asserted Claims include numerous limitations which are entirely missing from the '550 patent specification's written description. *See Lockwood v. Am. Airlines, Inc.*, 107 F.3d 1565, 1572 (Fed. Cir. 1997) ("it is not sufficient for purposes of the written description requirement of § 112 that the disclosure, when combined with the knowledge in the art, would lead one to speculate as to modifications that the inventor might have envisioned, but failed to disclose."); *PowerOasis, Inc. v. T-Mobile USA, Inc.*, 522 F.3d 1299, 1310 (Fed. Cir. 2008) ("at best, this is a statement that it would be obvious to substitute a customer laptop for the user interface disclosed on the vending machine. Obviousness simply is not enough; the subject matter must be disclosed to establish possession"). The test for written description is "whether the disclosure of the application relied upon reasonably conveys to those skilled in the art that the inventor had possession of the claimed subject matter as of the filing date." *Ariad Pharms., Inc. v. Eli Lilly & Co.*, 598 F.3d 1336, 1351 (Fed. Cir. 2010). Below is an exemplary table identifying missing limitations of the '550 patent asserted independent claims:[1]

'550 Patent – Claim 1	**Limitation Missing**
[1pre] A method for transferring data between a mobile device and a host, comprising:	
[1.1] sending, in response to instructions from a processor, application data requests from a mobile device to a host over a first connection at a first frequency;	Missing
[1.2] receiving data from the host responsive to the sent application data requests;	Missing
[1.3] selecting a power management mode, from a plurality of power management modes, based on an amount of battery power remaining on the mobile device, wherein selecting a power management mode is	Missing

[1] This list is exemplary and not exhaustive. Apple reserves its right to modify this list in response to arguments raised by SEVEN and/or its expert(s).

'550 Patent – Claim 1	Limitation Missing
further based on the amount of battery power remaining being below a predetermined amount;	
[1.4] changing the frequency that the application data requests are sent from the first frequency to a second frequency associated with the selected power management mode;	Missing
[1.5] wherein at least two of the power management modes are a low power mode configured to conserve the amount of battery power remaining on the mobile device and a normal operation mode,	Missing
[1.6] wherein the normal operation mode is configured to allow the mobile device to send application data requests more frequently than when the mobile device is in low power mode,	Missing
[1.7] wherein the frequency at which some application data requests are sent is not changed to the second frequency while the mobile device is in the low power mode; and	Missing
[1.8] exiting the low power mode when an amount of battery power remaining is above a predetermined amount.	Missing

'550 Patent – Claim 15	Limitation Missing
[15pre] A mobile device located in a mobile network, comprising:	
[15.1] a battery;	
[15.2] a processor configured to allow the mobile device to:	
[15.3] send application data requests to a host over a first connection at a first frequency;	
[15.4] receive data from the network responsive to the sent application data requests;	Missing
[15.5] select a power management mode from a plurality of power management modes based on an amount of battery power remaining on the mobile device, wherein the selection of a power management mode is further based on the amount of battery power remaining being below a predetermined amount;	Missing
[15.6] change the frequency that application data requests are sent from the first frequency to a second frequency associated with the selected power management mode;	Missing
[15.7] wherein at least two of the power management modes are a low power mode configured to conserve the amount of battery power remaining on the mobile device and a normal	Missing

’550 Patent – Claim 15	Limitation Missing
operation mode,	
[15.8] wherein the normal operation mode is configured to allow the mobile device to send application data requests more frequently than when the mobile device is in the low power mode,	Missing
[15.9] wherein the frequency at which some application data requests are sent is not changed to the second frequency while the mobile device is in the low power mode; and	Missing
[15.10] exit the low power mode when an amount of battery power remaining is above a predetermined amount.	Missing

’550 Patent – Claim 32	Limitation Missing
[32] A mobile device located in a mobile network, comprising:	
[32.1] a battery;	
[32.2] a processor configured to allow the mobile device to:	
[32.3] monitor a remaining battery level of the battery;	
[32.4] send application data requests to a host over a first connection at a first frequency;	
[32.5] receive data from the host responsive to the sent application data requests;	Missing
[32.6] operate in a normal operations mode when a remaining battery level is above a predetermined amount;	Missing
[32.7] select a low power mode from a plurality of power management modes in order to conserve the remaining battery level when the remaining battery level is below the predetermined amount, wherein the low power mode is based on amount of battery power remaining on the mobile device being below a predetermined amount;	Missing
[32.8] change the frequency that application data requests are sent from the first frequency to a second frequency	Missing

’550 Patent – Claim 32	Limitation Missing
associated with the low power management mode;	
[32.9] wherein at least two of the power management modes are the low power mode configured to conserve the amount of battery power remaining on the mobile device and the normal operations mode,	Missing
[32.10] wherein the normal operation mode is configured to allow the mobile device to send application data requests more frequently than when the mobile device is in the low power mode,	Missing
[32.11] wherein the frequency at which some application data requests are sent is not changed to the second frequency while the mobile device is in the low power mode;	Missing
[32.12] exit the low power management mode when the remaining battery level is above the predetermined amount; and	Missing
[32.13] receive a trigger that notifies the mobile device of new data, wherein the trigger at least in part causes the mobile device to send application data requests.	Missing

- Claims 1, 15, and 32 of the ’550 patent and their dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain an adequate written description and/or enabling disclosure of “power management mode(s),” “normal operations mode,” or “low power mode.” The full scope of the claimed subject matter is not described or enabled. The phrases “power management mode,” “power management modes,” “normal operations mode,” and “low power mode” are not used in the patent’s specification, and the patent’s disclosures do not otherwise describe or enable any of these limitations. Moreover, the phrases “power management mode,” “power management modes,” “normal operations mode,”

and “low power mode” fail to appear outside of the claims. Accordingly, the specification fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

- Claims 1, 15, and 32 of the ’550 patent and their dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain an adequate written description and/or enabling disclosure of “predetermined amount.” The full scope of the claimed subject matter is not described or enabled. The phrase “predetermined amount” is not used in the patent’s specification, and the patent’s disclosures do not otherwise describe or enable the “predetermined amount” limitation. Moreover, the phrase “predetermined amount” fails to appear outside of the claims. Accordingly, the specification fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.
- Claims 1, 15, and 32 of the ’550 patent and their dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain an adequate written description and/or enabling disclosure of “application data requests.” The full scope of the claimed subject matter is not described or enabled. The phrase “application data requests” is not used in the patent’s specification, and the patent’s disclosures do not otherwise describe or enable the “application data requests” limitation. Moreover, the phrase “application data requests” was added by amendment during

prosecution, and fails to appear outside of the claims. Accordingly, the specification fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

- Claims 2 and 18 of the '550 patent are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain an adequate written description and/or enabling disclosure of " wherein the trigger is received by the mobile device when the new data is of a type for which a trigger should be sent, wherein the trigger causes the mobile device to send at least one data request associated with the trigger." In particular, "data is of a type for which a trigger should be sent, wherein the trigger causes the mobile device to send at least one data request associated with the trigger" is not described or enabled. The limitation is not used in the patent's specification, and the patent's disclosures do not otherwise describe or enable the limitation. Moreover, the patent's specification does not disclose sending triggers for different types of data nor a trigger causing a mobile device to send at least one data request associated with the trigger. Accordingly, the specification fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.
- Claims 1, 15, and 32 of the '550 patent and their dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain an adequate written description and/or

enabling disclosure of "first frequency." The full scope of the claimed subject matter is not described or enabled. The phrase "first frequency" is not used in the patent's specification, and the patent's disclosures do not otherwise describe or enable the "second frequency" limitation. Moreover, the phrases "first frequency" or "second frequency" fails to appear outside of the claims. Accordingly, the specification fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

- Claims 1, 15, and 32 of the '550 patent and their dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain an adequate written description and/or enabling disclosure of "wherein the frequency at which some application data requests are sent is not changed to the second frequency while the mobile device is in the low power mode." The full scope of the claimed subject matter is not described or enabled. The phrase "wherein the frequency at which some application data requests are sent is not changed to the second frequency while the mobile device is in the low power mode" is not used in the patent's specification, and the patent's disclosures do not otherwise describe or enable limitation. In particular, the specification does not disclose using different frequencies for different application data requests or different frequencies for some applications. Accordingly, the specification fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

- Claim 20 of the ’550 patent is invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain an adequate written description and/or enabling disclosure of “the sent application data requests occur at a first frequency when the mobile device is in a normal operation mode, and at a second frequency when the mobile device is in the low power mode, wherein the first frequency is higher than the second frequency.” The full scope of the claimed subject matter is not described or enabled. The limitation is not used in the patent’s specification, and the patent’s disclosures do not otherwise describe or enable the limitation. In particular, the specification fails to disclose application data requests at first or second frequency nor having those frequencies associated with a power management mode, low power mode, or normal operation mode. Accordingly, the specification fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.
- Claim 25 of the ’550 patent is invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain an adequate written description and/or enabling disclosure of “the processor is further configured to allow the mobile device to receive a notification of new content.” The full scope of the claimed subject matter is not described or enabled. The limitation is not used in the patent’s specification, and the patent’s disclosures do not otherwise describe or enable this limitation. In particular, the specification fails to disclose a processor being configured to allow the mobile device to

receive a notification of new content. Accordingly, the specification fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

- Claims 9 and 26 of the '550 patent are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain an adequate written description and/or enabling disclosure of "the notification is received over a connection that is maintained while the mobile device is in the power management mode." The full scope of the claimed subject matter is not described or enabled. The limitation is not used in the patent's specification, and the patent's disclosures do not otherwise describe or enable this limitation. In particular, the specification fails to disclose a notification or what reasonably could constitute a notification being received over connection that is maintained while the mobile device is in power management mode. The '550 patent fails to disclose power management modes and notifications being sent while in a power management mode. Accordingly, the specification fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.
- Claim 12 of the '550 patent is invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain an adequate written description and/or enabling disclosure of "establishing a subsequent connection for receipt of the content." The limitation is not used in the patent's

specification, and the patent's disclosures do not otherwise describe or enable this limitation. In particular, the specification fails to disclose a processor within the mobile device being configured to allow the mobile device to establish a subsequent connection for receipt of the content. Accordingly, the specification fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

- Claim 29 of the '550 patent is invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain an adequate written description and/or enabling disclosure of "the processor is further configured to allow the mobile device to establish a subsequent connection for receipt of the content." The limitation is not used in the patent's specification, and the patent's disclosures do not otherwise describe or enable this limitation. In particular, the specification fails to disclose a processor within the mobile device being configured to allow the mobile device to establish a subsequent connection for receipt of the content. Accordingly, the specification fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.
- Claim 33 of the '550 patent is invalid for failure to satisfy the requirements of 35 U.S.C. § 112, 1 because the specification as filed does not contain an adequate written description and/or enabling disclosure of "wherein the processor is configured to allow the mobile device to enter the low power mode when the

amount of battery power remaining is below a predetermined amount." The limitation is not used in the patent's specification, and the patent's disclosures do not otherwise describe or enable this limitation. In particular, the specification fails to disclose a processor within the mobile device being configured to allow the mobile device to select a power management mode let alone enter a low power mode when the amount of battery power is below some undisclosed predetermined amount. Accordingly, the specification fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

b) Indefiniteness

At least in view of SEVEN's apparent construction of the claims in its Infringement Contentions, the Asserted Claims of the '550 patent are invalid because they fail to particularly point out and distinctly claim the subject matter which the applicant regards as his invention under 35 U.S.C. § 112, ¶¶ 2, 4, and/or 6. Based on Apple's present understanding of SEVEN's infringement contentions, Apple asserts that the Asserted Claims of the of the '550 patent are invalid for reciting at least the following claim terms/phrases/limitations:

- Claims 1, 15, and 32 of the '550 patent and their dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 2, ¶ 4, and/or ¶ 6 because the specification does not describe or otherwise inform one of ordinary skill about what constitutes a "power management mode." The '550 patent does not describe or explain how to distinguish any "mode" from any other mode of operation, such as a "low power mode." As such, one of ordinary skill would not understand the metes and bounds of the identified claims, rendering them indefinite under 35

U.S.C. § 112, ¶ 2. Therefore, the Asserted Claims, when read in light of the specification and the prosecution history, "fail to inform, with reasonable certainty, those skilled in the art about the scope of the invention." *Nautilus, Inc. v. Biosig Instruments, Inc.*, 134 S. Ct. 2120, 2124 (2014).

- Claims 1, 15, and 32 of the '550 patent and their dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 2, ¶ 4, and/or ¶ 6 because the specification does not describe or otherwise inform one of ordinary skill about what constitutes a "normal operation mode." The '550 patent does not describe or explain how to distinguish any "mode" from any other mode of operation, such as a "power management mode" or "low power mode." As such, one of ordinary skill would not understand the metes and bounds of the identified claims, rendering them indefinite under 35 U.S.C. § 112, ¶ 2. Therefore, the Asserted Claims, when read in light of the specification and the prosecution history, "fail to inform, with reasonable certainty, those skilled in the art about the scope of the invention." *Nautilus, Inc. v. Biosig Instruments, Inc.*, 134 S. Ct. 2120, 2124 (2014).
- Claims 1, 15, and 32 of the '550 patent and their dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 2, ¶ 4, and/or ¶ 6 because the specification does not describe or otherwise inform one of ordinary skill about what constitutes a "predetermined amount." The '550 patent does not describe or explain the threshold for a "predetermined amount." As such, one of ordinary skill would not understand the metes and bounds of the identified claims, rendering them indefinite under 35 U.S.C. § 112, ¶ 2. Therefore, the Asserted

Claims, when read in light of the specification and the prosecution history, "fail to inform, with reasonable certainty, those skilled in the art about the scope of the invention." *Nautilus, Inc. v. Biosig Instruments, Inc.*, 134 S. Ct. 2120, 2124 (2014).

- Claims 1, 15, and 32 of the '550 patent and their dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 2, ¶ 4, and/or ¶ 6 because the specification does not describe or otherwise inform one of ordinary skill about what constitutes a "first frequency." The '550 patent does not describe or explain how to distinguish any "frequency" from any other frequency of operation, such as a "second frequency." As such, one of ordinary skill would not understand the metes and bounds of the identified claims, rendering them indefinite under 35 U.S.C. § 112, ¶ 2. Therefore, the Asserted Claims, when read in light of the specification and the prosecution history, "fail to inform, with reasonable certainty, those skilled in the art about the scope of the invention." *Nautilus, Inc. v. Biosig Instruments, Inc.*, 134 S. Ct. 2120, 2124 (2014).
- Claims 1, 15, and 32 of the '550 patent and their dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 2, ¶ 4, and/or ¶ 6 because the specification does not describe or otherwise inform one of ordinary skill about what constitutes a "application data requests." The '550 patent does not describe or explain how to distinguish any "application data requests" from any other requests. As such, one of ordinary skill would not understand the metes and bounds of the identified claims, rendering them indefinite under 35 U.S.C. § 112, ¶ 2. Therefore, the Asserted Claims, when read in light of the specification and

the prosecution history, "fail to inform, with reasonable certainty, those skilled in the art about the scope of the invention." *Nautilus, Inc. v. Biosig Instruments, Inc.*, 134 S. Ct. 2120, 2124 (2014).

2. Other Grounds for Invalidity

In addition to the preceding invalidity contentions, Apple further contends that each of the Asserted Claims of the '550 patent is drawn to subject matter that is not patentable under 35 U.S.C. § 101. The '550 patent Asserted Claims are invalid under 35 U.S.C. § 101 for failure to recite patent eligible subject matter. Specifically, all claims of the '550 patent are fatally abstract under the U.S. Supreme Court's decision in *Alice Corp. v. CLS Bank Int'l*, 134 S. Ct. 2345 (2014) and progeny. The abstract ideas presented in the claims are generally directed to determining whether a device's battery has sufficient power and placing the device in a power saving mode depending on the power level of the battery. In essence, the claims are directed to an abstract concept of checking how much battery power is available using some undisclosed threshold and placing the battery into a power saving mode if the threshold is exceeded. Under *Alice* Step 1, those ideas are abstract, as they relate to a fundamental long prevalent practice of reducing energy usage when battery power is low. *See Intellectual Ventures I LLC v. Symantec Corp*., 838 F.3d 1307, 1314 (Fed. Cir. 2016). Limiting the invention to a particular technological environment, e.g. generic computer hardware, "do[es] not render an otherwise abstract concept any less abstract." *Intellectual Ventures I LLC v. Capital One Fin. Corp*., 850 F.3d 1332, 1340 (Fed Cir. 2017). Furthermore, under *Alice* Step 2 the '550 patent does not contain any inventive concept. The '550 patent Asserted Claims employs well-known components (e.g., a generic processor) or functionality (e.g., power saving modes), as shown in Apple's invalidity contentions involving anticipation and/or obviousness in this case, which is not enough to impart patent eligibility of an abstract idea. *See, e.g., Alice*, 134 S. Ct. at 2359 (holding that limitations

describing "'well-understood, routine, conventional activit[ies]' previously known to the industry" were insufficient to supply an inventive concept (quoting *Mayo*, 132 S. Ct. at 1294)). Further detail regarding Apple's contentions that the Asserted Claims of the '550 patent do not qualify as patent-eligible subject matter are contained in **Exhibit 550-D**.

Apple reserves the right to assert that the asserted patents are invalid under 35 U.S.C. §102(f) and/or (g) in the event Apple obtains evidence that the named inventors of the '550 patent did not invent (either alone or in conjunction with other parties) the subject matter claimed in the '550 patent. The inventors listed on the provisional applications to which SEVEN claims priority for the '550 patent do not align with those of the actual utility patent applications, including the application that matured into the '550 patent. Apple reserves the right to further explore this inventorship issue during discovery. Should Apple obtain evidence of incorrect claimed inventorship, it will provide the name of the person(s) from whom and the circumstances under which the invention or any part of it was derived, and/or the circumstances surrounding the making of the invention before the patent application.

Apple reserves the right to supplement these disclosures based on further investigation and discovery.

III. THE '914 PATENT

A. Patent Rule 3-3(a): Identification of Prior Art

At this time, Apple contends that at least each of the prior art references described and charted in **Exhibits 914-A and 914-B** anticipates or renders obvious, either alone or in combination, one or more of the Asserted Claims of the '914 patent.

Additional prior art that has not been charted, but is still relevant to the invalidity of the '914 patent is listed in **Exhibit C**, including without limitation as evidence of the state of the art at the alleged time of invention. Apple reserves the right to amend these invalidity contentions

to assert these references depending on the claim construction and infringement positions SEVEN may take as the case proceeds. Moreover, Apple reserves the right to use these references in combination with other references to render the claims of the '914 patent obvious in the event SEVEN takes the position that certain claim limitations are missing from the references charted in **Exhibits 914-A and 914-B**.

B. Patent Rule 3-3(b): Whether Each Item Anticipates or Renders Obvious the Asserted Claims

SEVEN asserts claims 1-5, 7-9, 11-15, 17-19, 21-25 and 27-39 of the '914 patent against Apple in this lawsuit. These claims are invalid because the '914 patent fails to meet one or more of the requirements for patentability. The individual bases for invalidity are provided below and in the claim charts attached as **Exhibits 914-A and 914-B.** Each of the foregoing listed prior art documents, the underlying work, and/or the underlying apparatus or method qualifies as prior art under one or more sections of 35 U.S.C. §§ 102 and/or 103.

Although Apple has identified at least one citation per limitation for each reference, each and every disclosure of the same limitation in the same reference is not necessarily identified. Rather, in an effort to focus the issues, Apple has cited representative portions of identified references, even where a reference may contain additional support for a particular claim element. In addition, persons of ordinary skill in the art generally read a prior art reference as a whole and in the context of other publications and literature. Thus, to understand and interpret any specific statement or disclosure within a prior art reference, such persons would rely on other information within the reference, along with other publications and their general scientific knowledge. Apple may rely upon uncited portions of the prior art references and on other publications and expert testimony to provide context, and as aids to understanding and interpreting the portions that are cited. Apple may also rely on uncited portions of the prior art references, other disclosed

publications, and the testimony of experts to establish that a person of ordinary skill in the art would have been motivated to modify or combine certain of the cited references so as to render the claims obvious.

1. Priority

SEVEN's Patent Rule 3-1(e) disclosures provide that the Asserted Claims of the '914 patent are entitled to a priority date of January 11, 2008, which is the filing date of U.S. Provisional Application No. 12/008,710. SEVEN has provided no evidence to support its contention that the Asserted Claims of the '914 patent are entitled to claim priority back to this or any earlier filed application, and Apple therefore reserves the right to assert a later priority date based on any findings as to the priority date of the Asserted Claims by the Court, information learned through discovery, or otherwise.

The '914 patent claims priority to a provisional application filed on January 11, 2008. Apple reserves the right to challenge SEVEN's assertion that the '914 patent is entitled to claim the benefit of that provisional application's filing date to the extent that the provisional application does not support the full scope of the Asserted Claims, for example, depending on scope of the Asserted Claims as properly construed. To the extent the provisional application does not support the full scope of the Asserted Claims, the priority date of the '914 patent should be the filing date of the patent application of which the '914 patent is a continuation, which is March 22, 2012.

a) The Asserted Claims of the '914 Patent Cannot Claim Priority to the '641 Provisional

None of the Asserted Claims are entitled to the filing date of U.S. Provisional No. 2009/0181641 ("the '641 Provisional") because claims 1, 11, 21 and 27 do not have written

description support in the ’641 Provisional. *See Falko-Gunter Falkner v. Inglis*, 448 F.3d 1357 (Fed. Cir. 2006).

Claims 1, 11, 21 and 27 are not entitled to the ’641 Provisional filing date because the ’641 Provisional does not actually or inherently disclose each and every claim element. *PowerOasis, Inc. v. T-Mobile USA, Inc*., 522 F.3d 1299, 1306-07 (Fed. Cir. 2008).

Claims 1, 11, 21 and 27 recite features relating to authentication of two or more associated devices—features found nowhere in the Provisional to which the ’914 patent claims priority. Nothing in the Provisional shows the inventor possessed and enabled functionalities relating to authenticating multiple devices using authentication tokens and a server recited in claims 1, 11, 21 and 27 (“receiving a unique authentication token from each of a first device and a second device…”), (“wherein each of the first device and the second device transmit a unique authentication token for authenticating each of the first device and the second device”).

Importantly, while the ’641 Provisional does make references to a “unique authentication token,” it does not provide any description of how a system might operate to accommodate multiple devices and multiple authentication tokens. The ’641 Provisional never mentions authenticating multiple devices or how a server might understand two more devices to be associated based on multiple authentication tokens as recited in the ’914 patent claims.

As to claims 1, 11, 21 and 27, the ’641 Provisional fails to disclose “receiving a unique authentication token from each of a first device and a second device” and “wherein each of the first device and the second device transmit a unique authentication token for authenticating each of the first device and the second device.” In terms of authenticating multiple devices using authentication tokens, the ’641 Provisional never discusses the use of more than one authentication token, and never discusses using authentication tokens to associate devices for

duplicating content. The ’641 Provisional describes a “personal computing device” that is configured to “receive an authentication token from the mobile device” in order to “authorize the mobile device 120 prior to providing data and/or services to the mobile device.” ’641 Provisional at [0071]. However, this is the exact authentication system SEVEN disclaimed during the prosecution of the ’914 patent. Specifically, SEVEN stated that prior art reference “Harper does not teach receiving a unique authentication token from each of the first device and the second device. Harper teaches receiving a unique authentication token at one device and that device relaying the authentication token to another device.” ’914 Patent File History, April 16, 2016, Applicant Arguments/Remarks Made in an Amendment at 10. This disclosure of authorization of a mobile device using an authentication token cannot be used to provide written description support for the dual-authentication token system found in claims 1, 11, 21 and 27, especially in light of the prosecution history of the ’914 patent. Thus, the ’641 Provisional does not adequately provide written description support for the dual-authentication token system which allows for content distribution across associated devices.

Consequently, the ’641 Provisional does not actually or inherently disclose each and every element of the ’914 patent claims. *Id*. The introduction of these features into the claims resulted in the ’914 patent claims not being entitled to the filing date of the Provisional, and are, at most, entitled to the filing date of December 28, 2014—the filing date of the ’914 patent.

2. Anticipation

Some or all of the Asserted Claims of the ’914 patent are invalid as anticipated under 35 U.S.C. § 102 in view of each of the prior art references identified above and in the claim charts included in **Exhibit 914-A**, which identify specific examples of where each limitation of the Asserted Claims is found in the prior art references. As explained above, the cited portions of prior art references identified in the attached claim charts are exemplary only and representative

of the content and teaching of the prior art references, and should be understood in the context of the reference as a whole and as they would be understood by a person of ordinary skill in the art.

Apple identifies the following references as anticipating one or more of the Asserted Claims of the '914 patent under 35 U.S.C. § 102. The below table of anticipating references is exemplary, and it does not constitute an admission that any reference anticipates only the listed claims. Further, Apple contends that any prior art reference in the attached charts that is charted for each limitation of any given claim, anticipates that claim, regardless of whether that prior art reference is listed in the following table.

Anticipating Prior Art	Claims	Exhibit No.
U.S. Patent No. 8,001,612 to Wieder ("Wieder")	All Asserted Claims	Exhibit No. 914-A01
U.S. Patent No. 8,880,714 to Collart et al. ("Collart")	All Asserted Claims	Exhibit No. 914-A02
U.S. Patent No. 7,792,756 to Plastina et al. ("Plastina")	All Asserted Claims except 30, 33, 36 and 39	Exhibit No. 914-A03
U.S. Patent No. 8,028,323 to Weel ("Weel")	All Asserted Claims except 30, 33, 36 and 39	Exhibit No. 914-A04
Microsoft Zune	All Asserted Claims except 30, 33, 36 and 39	Exhibit No. 914-A05
U.S. Patent Application No. 2002/0068558 to Janik ("Janik")	All Asserted Claims except 30, 33, 36 and 39	Exhibit No. 914-A06
U.S. Patent No. 7,653,761 to Juster et al. ("Juster")	All Asserted Claims except 7, 8, 9, 17, 18, 19, 30, 33, 36 and 39	Exhibit No. 914-A07
U.S. Patent Application No. 2006/0190413 to Harper ("Harper")	All Asserted Claims except 30, 33, 36 and 39	Exhibit No. 914-A08
iTunes 4.0	All Asserted Claims except 30, 33, 36 and 39	Exhibit No. 914-A09

To the extent any item of prior art cited above is deemed not to disclose, explicitly or inherently, any limitation of an Asserted Claim of the '914 patent, Apple reserves the right to argue that any difference between that prior art and the corresponding patent claim would have been either inherent to the art, or obvious to a person of ordinary skill in the art, even if Apple

has not specifically denoted that the art is to be combined with the knowledge of a person of ordinary skill in the art.

3. Obviousness

To the extent any limitation is deemed not to be exactly met by an item of prior art listed above and in **Exhibit 914-A**, then any purported differences are such that the claimed subject matter as a whole would have been obvious to one skilled in the art at the time of the alleged invention, in view of the state of the art and knowledge of those skilled in the art. The item of prior art would, therefore, render the relevant claims invalid for obviousness under 35 U.S.C. § 103.

In addition, the references identified above render one or more Asserted Claims of the '914 patent obvious when the references are read in combination with each other, and/or when read in view of the state of the art and knowledge of those skilled in the art. Each and every reference identified is also relevant to the state of the art at the time of the alleged invention. Any of the references disclosed above may be combined with one another to render obvious (and therefore invalid) each of SEVEN's Asserted Claims. Apple may rely upon a subset of the above identified references or all of the references identified above, including all references in **Exhibits 914-A, 914-B, and C** for purposes of obviousness depending on the Court's claim construction, positions taken by SEVEN during this litigation, and further investigation and discovery.

To the extent the foregoing references are found not to anticipate the Asserted Claims, the foregoing references render the Asserted Claims obvious either alone or in combination with one or more of the other references identified above pursuant to Patent Rule 3-3(a). It would have been obvious to a person of skill in the art at the time of the alleged invention of the

Asserted Claims of the ’914 patent to combine the various references cited herein so as to disclose the Asserted Claims of the ’914 patent.

In accordance with Patent Rule 3-3(b), prior art references rendering the Asserted Claims obvious, alone or in combination with other references, are outlined below and included in **Exhibits 914-A and 914-B,** which include exemplary claim charts for the Asserted Claims of the ’914 Patent showing specifically where in each reference or combinations of references each Asserted Claim is found, and an explanation of why the prior art renders the Asserted Claim obvious. Where applicable, **Exhibits 914-A and 914-B** include the motivation to combine references.

Moreover, in addition to the information contained elsewhere in these contentions and in particular **Exhibit 914-B,** Apple has identified additional motivations and reasons to combine the various references cited herein. In particular, multiple teachings, suggestions, and/or reasons to modify any of the references and/or to combine any two or more of the references in **Exhibits 914-A and 914-B** come from many sources, including the prior art (specific and as a whole), common knowledge, common sense, predictability, expectations, industry trends, design incentives or need, market demand or pressure, market forces, obvious to try, the nature of the problem faced, and/or knowledge possessed by one of ordinary skill. In addition, it would have been obvious to try combining the prior art references identified above because there were only a finite number of predictable solutions and/or because known work in one field or endeavor prompted variations based on predictable design incentives and/or market forces either in the same field or a different one. The combination of prior art references identified in these contentions would have been obvious because the claimed combinations represent the known potential options with a reasonable expectation of success. Additionally, one of ordinary skill in

the art would have been motivated to create combinations identified in these contentions using: known methods to yield predictable results; known techniques in the same way; a simple substitution of one known, equivalent element for another to obtain predictable results; and/or teaching, suggestion, or motivation in the prior art generally. Also, market forces in the industry, and the desire to improve features and performance, would motivate the addition of features to systems as they become available, become less expensive, become more commonly used, provide better performance, reduce costs, size or weight, or predictably achieve other clearly desirable results.

While Apple reserves the right to rely on any combination of the references reflected in their charts or incorporated herein by reference, Apple provides the following exemplary and non-exhaustive references and/or combinations evidencing invalidity of the claims of the Asserted Patents. The combinations of prior art listed below render obvious the Asserted Claims under the proper construction of the claims and/or under Plaintiff's apparent interpretation of the claims as set forth by Plaintiff in their Complaint and Infringement Contentions. Each combination renders the identified claims obvious through the express and/or inherent disclosure in the combination of references themselves, as well as in view of the knowledge of a person of ordinary skill in the art.

Obviousness Combinations	**Claims**
Wieder in view of one or more of Collart, Plastina, Weel, Microsoft Zune, iTunes 4.0, Janik, Harper, Juster, U.S. Patent Application No. 2009/0265775 to Wisely at al. ("Wisely"), U.K. Patent Application No. 2009/0265775 to Lin ("Lin"), U.S. Patent No. 8,171,531 to Buer, and/or U.S. Patent No. 7,487,537 to Giles et al. ("Giles")	All Asserted Claims
Collart in view of Wieder, Plastina, Weel, Microsoft Zune, iTunes 4.0, Janik, Harper, Juster, Wisely, Lin, Buer, and/or Giles	All Asserted Claims

Obviousness Combinations	Claims
Plastina in view of Wieder, Collart, Weel, Microsoft Zune, iTunes 4.0, Janik, Harper, Juster, Wisely, Lin, Buer, and/or Giles	All Asserted Claims
Janik in view of one or more of Wieder, Collart, Plastina, Weel, Microsoft Zune, iTunes 4.0, Harper, Juster, Wisely, Lin, Buer, and/or Giles	All Asserted Claims
Harper in view of one or more of Wieder, Collart, Plastina, Weel, Microsoft Zune, iTunes 4.0, Janik, Juster, Wisely, Lin, Buer, and/or Giles	All Asserted Claims
Juster in view of one or more of Wieder, Collart, Plastina, Weel, Microsoft Zune, iTunes 4.0, Janik, Harper, Wisely, Lin, Buer, and/or Giles	All Asserted Claims
Weel in view of one or more of Wieder, Collart, Plastina, Microsoft Zune, iTunes 4.0, Janik, Harper, Juster, Wisely, Lin, Buer, and/or Giles	All Asserted Claims
Microsoft Zune in view of one or more of Wieder, Collart, Plastina, Weel, iTunes 4.0, Janik, Harper, Juster, Wisely, Lin, Buer, and/or Giles	All Asserted Claims
iTunes 4.0 in view of one or more of Wieder, Collart, Plastina, Weel, Microsoft Zune, Janik, Harper, Juster, Wisely, Lin, Buer, and/or Giles	All Asserted Claims
Wieder in view of one or more of Collart, Plastina, Weel, Microsoft Zune, iTunes 4.0, Janik, Harper, Juster, U.S. Patent No. 7,392,393 to Taki ("Taki"), U.S. Patent Pub. 2005/0021478 to Gautier et al. ("Gautier"), U.S. Patent Pub. 2005/0108430 to Howarth et al. ("Howarth"), U.S. Patent Pub. 2005/0165795 to Myka et al. ("Myka"), and/or U.S. Patent Pub. 2008/0212944 to Khedouri et al. ("Khedouri")	All Asserted Claims
Collart in view of one or more of Wieder, Plastina, Weel, Microsoft Zune, iTunes 4.0, Janik, Harper, Juster, Taki, Gautier, Howarth, Myka, and/or Khedouri	All Asserted Claims
Plastina in view of one or more of Wieder, Collart, Weel, Microsoft Zune, iTunes 4.0, Janik, Harper, Juster, Taki, Gautier, Howarth, Myka, and/or Khedouri	All Asserted Claims
Janik in view of one or more of Wieder, Collart, Plastina, Weel, Microsoft Zune, iTunes 4.0, Harper, Juster, Taki, Gautier, Howarth, Myka, and/or Khedouri	All Asserted Claims
Harper in view of one or more of Wieder, Collart, Plastina, Weel, Microsoft Zune, iTunes 4.0, Janik,	All Asserted Claims

Obviousness Combinations	Claims
Juster, Taki, Gautier, Howarth, Myka, and/or Khedouri	
Juster in view of one or more of Wieder, Collart, Plastina, Weel, Microsoft Zune, iTunes 4.0, Janik, Harper, Taki, Gautier, Howarth, Myka, and/or Khedouri	All Asserted Claims
Weel in view of one or more of Wieder, Collart, Plastina, Microsoft Zune, iTunes 4.0, Janik, Harper, Huster, Taki, Gautier, Howarth, Myka, and/or Khedouri	All Asserted Claims
Microsoft Zune in view of one or more of Wieder, Collart, Plastina, Weel, iTunes 4.0, Janik, Harper, Taki, Gautier, Howarth, Myka, and/or Khedouri	All Asserted Claims
iTunes 4.0 in view of one or more of Wieder, Collart, Plastina, Weel, Microsoft Zune, Janik, Harper, Taki, Gautier, Howarth, Myka, and/or Khedouri	All Asserted Claims
Wieder in view of one or more of Collart, Plastina, Weel, Microsoft Zune, iTunes 4.0, Janik, Harper, Juster, U.S. Patent No. 8,145,222 to Wormald et al. ("Wormald"), U.S. Patent No. 7,778,971 to Freedman et al. ("Freedman"), U.S. Patent No. 8,270,965 to Bahl et al. ("Bahl"), and/or U.S. Patent No. 9,124,650 to Maharajh et al. ("Maharajh")	All Asserted Claims
Collart in view of one or more of Wieder, Plastina, Weel, Microsoft Zune, iTunes 4.0, Janik, Harper, Juster, Wormald, Freedman, Bahl, and/or Maharajh	All Asserted Claims
Plastina in view of one or more of Wieder, Collart, Weel, Microsoft Zune, iTunes 4.0, Janik, Harper, Juster, Wormald, Freedman, Bahl, and/or Maharajh	All Asserted Claims
Janik, in view of one or more of Wieder, Collart, Plastina, Weel, Microsoft Zune, iTunes 4.0, Harper, Juster, Wormald, Freedman, Bahl, and/or Maharajh	All Asserted Claims
Harper in view of one or more of Wieder, Collart, Plastina, Weel, Microsoft Zune, iTunes 4.0, Janik, Juster, Wormald, Freedman, Bahl, and/or Maharajh	All Asserted Claims
Juster, in view of one or more of Wieder, Collart, Plastina, Weel, Microsoft Zune, iTunes 4.0, Janik, Harper, Wormald, Freedman, Bahl, and/or Maharajh	All Asserted Claims
Weel in view of one or more of Wieder, Collart, Plastina, Microsoft Zune, iTunes 4.0, Janik, Harper, Juster, Wormald, Freedman, Bahl, and/or Maharajh	All Asserted Claims
Microsoft Zune in view of one or more of Wieder, Collart, Plastina, Weel, iTunes 4.0, Janik, Harper, Juster, Wormald, Freedman, Bahl, and/or Maharajh	All Asserted Claims

Obviousness Combinations	Claims
iTunes 4.0 in view of one or more of Wieder, Collart, Plastina, Weel, Microsoft Zune, Janik, Harper, Juster, Wormald, Freedman, Bahl, and/or Maharajh	All Asserted Claims

In addition to the specific combinations of prior art and the specific combinations of groups of prior art disclosed above, Apple reserves the right to rely on any other combination of any prior art references disclosed herein. Apple further reserves the right to rely upon combinations disclosed within the prosecution history of the references cited herein. These obviousness combinations reflect Apple's present understanding of the potential scope of the claims that SEVEN appears to be advocating and should not be seen as Apple's acquiescence to SEVEN's interpretation of the patent claims.

Apple also reserves the right to amend or supplement these contentions regarding anticipation or obviousness of the Asserted Claims, in view of further information from SEVEN, information discovered during discovery, or a claim construction ruling by the Court. SEVEN has not identified what elements or combinations it alleges were not known to one of ordinary skill in the art at the time. Therefore, for any claim limitation that SEVEN alleges is not disclosed in a particular prior art reference, Apple reserves the right to assert that any such limitation is either inherent in the disclosed reference or obvious to one of ordinary skill in the art at the time in light of the same, or that the limitation is disclosed in another of the references disclosed above and in combination would have rendered the Asserted Claim obvious.

C. Patent Rule 3-3(c): Charts Identifying Where Specifically in Each Alleged Item of Prior Art Each Asserted Claim Is Found

Pursuant to Patent Rule 3-3(c), charts identifying where specifically in each alleged item of prior art each limitation of each Asserted Claim is found, including for each limitation that Apple contends is governed by 35 U.S.C. § 112(6), the identity of the structure(s), act(s), or

material(s) in each item of prior art that performs the claimed function, are attached in **Exhibits 914-A and 914-B.**

D. Patent Rule 3-3(d): Other Grounds for Invalidity

Apple identifies the following grounds for invalidity of the Asserted Claims of the '914 patent based on 35 U.S.C. §§ 101 and/or 112. Apple reserves the right to supplement these disclosures based on further investigation and discovery.

1. Invalidity Pursuant to 35 U.S.C. § 112

Apple further asserts that the Asserted Claims of the '914 patent are invalid under 35 U.S.C. § 112. The following are the grounds upon which Apple contends the Asserted Claims are invalid for failure to meet the requirements of 35 U.S.C. § 112, ¶ 1, ¶ 2, ¶ 4 and/or ¶ 6, based on Apple's investigation to date and currently-available information.

For each claim identified as invalid, any dependent claims of those invalid claims are also invalid under 35 U.S.C. § 112, ¶ 1, ¶ 2, ¶ 4, and/or ¶ 6. Apple reserves the right to supplement and amend these contentions based on further discovery and investigation including, in particular, the deposition of any of the named inventors of the Asserted Patent, the parties' claim construction positions, and further investigation of SEVEN's implied infringement positions.

a) Written Description and/or Enablement

At least in view of SEVEN's apparent construction of the claims in its Infringement Contentions, the Asserted Claims of the '914 patent are invalid because the specification as filed does not contain adequate written description of the claimed inventions sufficient to lead a person of ordinary skill in the art to understand that the named inventors had possession of the purported inventions as claimed as required by 35 U.S.C. § 112, ¶ 1. Likewise, the specification does not enable one of ordinary skill in the art to make or use the claimed inventions without undue experimentation. Based on Apple's present understanding of SEVEN's infringement

contentions, Apple asserts that the Asserted Claims of the of the '914 patent are invalid for reciting at least the following claim terms/phrases/limitations:

Claims 1-5, 7-9, 11-15, 17-19, 21-25, and 27-39 of the '914 patent and its dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain an adequate written description and/or enabling disclosure for the two-device architecture embodied in the claims. Independent claims 1, 11, 21, and 27 all discuss the distribution of content between a "first device" and a "second device." However, the words "first device" and "second device" never appear in the specification, nor do the images depict a system that embodies two devices. While the specification discusses distribution content to a device, there are issues specific to content distribution across multiple devices that the specification does not adequately describe or disclose. For example, and as discussed in further detail below, the specification describes a system of authenticating a user device. However, the specification does not describe how authentication occurs across or between multiple devices. The specification describes a system for automatically transmitting content to a device, but does not describe how content is transmitted to a "first device" and then "automatically transmitted" to the "second device." Furthermore, the specification does not describe the relationship, if any, between authentication and content distribution across a first device and a second device. Accordingly, the specification fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

Claims 1, 11, 21, and 27 of the '914 patent and its dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain an adequate written description and/or enabling disclosure of "receiving a unique

authentication token from each of a/the first device and a/the second device" or "each of the first device and the second device transmit a unique authentication token." The specification never discusses the use of more than one authentication token, and never discusses using authentication tokens to associate devices for duplicating content. The specification describes a "personal computing device" that is configured to "receive an authentication token from the mobile device" in order to "authorize the mobile device 120 prior to providing data and/or services to the mobile device." '914 patent at 14:31-34. However, this is the exact authentication system SEVEN disclaimed during the prosecution of the '914 patent. Specifically, SEVEN stated that prior art reference "Harper does not teach receiving a unique authentication token from each of the first device and the second device. Harper teaches receiving a unique authentication token at one device and that device relaying the authentication token to another device." '914 Patent File History, April 16, 2016, Applicant Arguments/Remarks Made in an Amendment at 10. This disclosure of authorization of a mobile device using an authentication token cannot be used to provide written description support for the dual-authentication token system found in claims 1, 11, 21 and 27, especially in light of the prosecution history of the '914 patent. Accordingly, the specification fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

Claims 1, 11, 21 and 27 of the '914 patent are also invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the limitations requiring "transmitting selected content to the first device" and "transmitting the selected content to the second device" lack written description support and/or are not enabled, at least to the extent that SEVEN contends "content" is defined as anything more or other than "digital audio data files, mobile device ring-

tones, e-book data files, picture data files, video data files, e-mail data files, voice message data files, SMS data files, document files, and software applications." '914 patent at 9:15-21.

Claims 1, 11, 21 and 27 of the '914 patent are also invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain an adequate written description and/or enabling disclosure of the phrase: "wherein the selected content is transmitted to the first device through a first connection and transmitted to the second device through a second connection distinct from the first connection." Specifically, the phrase "distinct" is not defined, used, or described in the patent's specification, and the patent's disclosures do not otherwise describe or enable the "distinct connection" limitation. The specification fails to describe what constitutes a distinct connection (i.e. whether one connection must be a certain *type* of connection and the other a different *type* of connection, or whether the connections themselves must just be different). Accordingly, the specification fails to reasonably convey to one or ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

Claims 30, 33, 36 and 39 of the '914 patent are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain an adequate written description and/or enabling disclosure of the phrase: "wherein the wifi or cellular connection is selected based on a size characteristic of the transmitted content." The phrase "size characteristic" is not defined, used, or described in the patent's specification, and the patent's disclosures do not otherwise describe or enable the 'size characteristic' limitation. Furthermore, the specification fails to describe how the server, device, or system determines the size characteristic of the transmitted content and accordingly selects the wifi or cellular

connection. Accordingly, the specification fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

Claims 28, 31, 34 and 37 of the '914 patent are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain an adequate written description and/or enabling disclosure of "directly communicatively connected." The phrase "directly communicatively connected" is not defined, used, or described in the patent's specification, and the patent's disclosures do not otherwise describe or enable the 'directly communicatively connected' limitation." Furthermore, the specification fails to describe how the devices are indirectly communicatively connected to one another rather than directly communicatively connected. Accordingly, the specification fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

b) Indefiniteness

At least in view of SEVEN's apparent construction of the claims in its Infringement Contentions, the Asserted Claims of the '914 patent are invalid because they fail to particularly point out and distinctly claim the subject matter which the applicant regards as his invention under 35 U.S.C. § 112, ¶¶ 2, 4, and/or 6. Based on Apple's present understanding of SEVEN's infringement contentions, Apple asserts that the Asserted Claims of the of the '914 patent are invalid for reciting at least the following claim terms/phrases/limitations:

- Claims 1, 11, 21, and 27 of the '914 patent are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 2, ¶ 4, and/or ¶ 6 because the specification does not describe or otherwise inform one of ordinary skill about what constitutes "receiving/transmitting a unique authentication token." The '914 patent does not

describe or explain what receives the unique authentication or to where the unique authentication token is transmitted. The claims discuss a content provider, but it is unclear whether the content provider is what receives the authentication token, or whether it is the server or computing device. Therefore, the Asserted Claims, when read in light of the specification and the prosecution history, "fail to inform, with reasonable certainty, those skilled in the art about the scope of the invention." *Nautilus, Inc. v. Biosig Instruments, Inc*., 134 S. Ct. 2120, 2124 (2014).

- Claims 28, 31, 34, and 37 of the '914 patent are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 2, ¶ 4, and/or ¶ 6 because the specification does not describe or otherwise inform one of ordinary skill about what constitutes "not directly communicatively connected." The '914 patent does not describe or explain how to distinguish "directly communicatively connected' from 'not directly communicatively connected." As such, one of ordinary skill would not understand the metes and bounds of the identified claims, rendering them indefinite under 35 U.S.C. § 112, ¶ 2. Therefore, the Asserted Claims, when read in light of the specification and the prosecution history, "fail to inform, with reasonable certainty, those skilled in the art about the scope of the invention." *Nautilus, Inc. v. Biosig Instruments, Inc*., 134 S. Ct. 2120, 2124 (2014).

2. Other Grounds for Invalidity

In addition to the preceding invalidity contentions, Apple further contends that each of the Asserted Claims of the '914 patent is drawn to subject matter that is not patentable under 35 U.S.C. § 101. The '914 patent Asserted Claims are invalid under 35 U.S.C. § 101 for failure to recite patent eligible subject matter. Specifically, all claims of the '914 patent are fatally abstract under the U.S. Supreme Court's decision in *Alice Corp. v. CLS Bank Int'l*, 134 S. Ct. 2345 (2014) and progeny. The ideas presented in the claims are generally directed to concepts of

receiving information, analyzing it, selecting content, and transmitting that content. Under *Alice* Step 1, those ideas are abstract, as they relate to a fundamental long prevalent practice. *See Intellectual Ventures I LLC v. Symantec Corp*., 838 F.3d 1307, 1314 (Fed. Cir. 2016). Limiting the invention to a particular technological environment, e.g. generic computer hardware, "do[es] not render an otherwise abstract concept any less abstract." *Intellectual Ventures I LLC v. Capital One Fin. Corp*., 850 F.3d 1332, 1340 (Fed Cir. 2017). Furthermore, because the patent relates to transmission of information, it is likewise abstract, as "information is . . . an intangible." *Electric Power Group, LLC v. Alstom S.A.*, 830 F.3d 1350, 1353 (Fed. Cir. 2016). Furthermore, under *Alice* Step 2 the '986 patent does not contain any inventive concept. The '914 patent Asserted Claims employs well-known components or functionality, as shown in Apple's invalidity contentions involving anticipation and/or obviousness in this case, which is not enough to impart patent eligibility of an abstract idea. *See, e.g., Alice*, 134 S. Ct. at 2359 (holding that limitations describing "'well-understood, routine, conventional activit[ies]' previously known to the industry" were insufficient to supply an inventive concept (quoting *Mayo*, 132 S. Ct. at 1294)). Further detail regarding Apple's contentions that the Asserted Claims of the '914 patent do not qualify as patent-eligible subject matter are contained in **Exhibit 914-D**.

Apple reserves the right to assert that the asserted patents are invalid under 35 U.S.C. §102(f) and/or (g) in the event Apple obtains evidence that the named inventors of the '914 patent did not invent (either alone or in conjunction with other parties) the subject matter claimed in the '914 patent. Should Apple obtain such evidence, it will provide the name of the person(s) from whom and the circumstances under which the invention or any part of it was derived, and/or the circumstances surrounding the making of the invention before the patent application.

Apple reserves the right to supplement these disclosures based on further investigation and discovery.

IV. THE '127 PATENT

A. Patent Rule 3-3(a): Identification of Prior Art

At this time, Apple contends that at least each of the prior art references described and charted in **Exhibits 127-A – 127-B** anticipates or renders obvious, either alone or in combination, one or more of the Asserted Claims of the '127 patent.

Additional prior art that has not been charted, but is still relevant to the invalidity of the '127 patent is listed in **Exhibit C**, including without limitation as evidence of the state of the art at the alleged time of invention. Apple reserves the right to amend these invalidity contentions to assert these references depending on the claim construction and infringement positions SEVEN may take as the case proceeds. Moreover, Apple reserves the right to use these references in combination with other references to render the claims of the '127 patent obvious in the event SEVEN takes the position that certain claim limitations are missing from the references charted in **Exhibits 127-A – 127-B**.

B. Patent Rule 3-3(b): Whether Each Item Anticipates or Renders Obvious the Asserted Claims

SEVEN asserts claims 24-50 of the '127 patent against Apple in this lawsuit. These claims are invalid because the '127 patent fails to meet one or more of the requirements for patentability. The individual bases for invalidity are provided below and in the claim charts attached as **Exhibits 127-A – 127-B**. Each of the foregoing listed prior art documents, the underlying work, and/or the underlying apparatus or method qualifies as prior art under one or more sections of 35 U.S.C. §§ 102 and/or 103.

Although Apple has identified at least one citation per limitation for each reference, each and every disclosure of the same limitation in the same reference is not necessarily identified. Rather, in an effort to focus the issues, Apple has cited representative portions of identified references, even where a reference may contain additional support for a particular claim element. In addition, persons of ordinary skill in the art generally read a prior art reference as a whole and in the context of other publications and literature. Thus, to understand and interpret any specific statement or disclosure within a prior art reference, such persons would rely on other information within the reference, along with other publications and their general scientific knowledge. Apple may rely upon uncited portions of the prior art references and on other publications and expert testimony to provide context, and as aids to understanding and interpreting the portions that are cited. Apple may also rely on uncited portions of the prior art references, other disclosed publications, and the testimony of experts to establish that a person of ordinary skill in the art would have been motivated to modify or combine certain of the cited references so as to render the claims obvious.

1. Priority

SEVEN's Patent Rule 3-1(e) disclosures provide that the Asserted Claims of the '127 patent are entitled to a priority date of March 25, 2013, which is the filing date of U.S. Provisional Application No. 61/805,070. SEVEN has provided no evidence to support its contention that the Asserted Claims of the '127 patent are entitled to claim priority back to this or any earlier filed application, and Apple therefore reserves the right to assert a later priority date based on any findings as to the priority date of the Asserted Claims by the Court, information learned through discovery, or otherwise.

The '127 patent claims priority to a provisional application filed on March 25, 2013. Apple reserves the right to challenge SEVEN's assertion that the '127 patent is entitled to claim

the benefit of that provisional application's filing date to the extent that the provisional application does not support the full scope of the Asserted Claims, for example, depending on scope of the Asserted Claims as properly construed. To the extent the provisional application does not support the full scope of the Asserted Claims, the priority date of the '127 patent should be the filing date of the patent application of which the '127 patent is a continuation, which is March 24, 2014.

The provisional application must "contain a written description of the invention and the manner and process of making and using it, in such full, clear, concise, and exact terms," 35 U.S.C. § 112 ¶ 1, to enable a POSITA to practice the invention claimed in the non-provisional application. *Id*.

a) The Asserted Claims of the '127 Patent Cannot Claim Priority to the '070 Provisional

None of the Asserted Claims are entitled to the filing date of U.S. Provisional Application No. 61/805,070 ("the '070 Provisional") because claims 24, 33, and 42 do not have written description support in the '070 Provisional. *See Falko-Gunter Falkner v. Inglis*, 448 F.3d 1357 (Fed. Cir. 2006).

Claims 24, 33, and 42 are not entitled to the '070 Provisional filing date because the '070 Provisional does not actually or inherently disclose each and every claim element. *PowerOasis, Inc. v. T-Mobile USA, Inc.*, 522 F.3d 1299, 1306-07 (Fed. Cir. 2008).

Claims 24, 33, and 42 recite features relating to entering/exiting a power save mode—features found nowhere in the provisional application to which the '127 patent claims priority. Nothing in the provisional application shows the inventor possessed and enabled functionalities relating to entering/exiting a "power save mode" recited in claims 24, 33, and 42 ("receive a selection from a user whether to enter a power save mode, where the power save mode is based

on a battery level of the mobile device"), ("upon selection to enter the power save mode…"), ("the power save mode is exited based on a battery level or in response to the user directing the mobile device to exit the power save mode").

Importantly, the '070 Provisional never uses the term "power save mode." The '070 Provisional does make one reference to "sleep mode," but does not provide any description of entering "sleep mode," only describing exit of "sleep mode" based on an alarm. '070 Provisional at [00101] ("some applications use alarms associated with wake locks (WakeLock) to bring the device out of sleep mode"). The '070 Provisional never mentions entry/exit of sleep mode (or any power save mode) based on the factors recited in the '127 patent claims.

As to claims 24, 33, and 42, the '070 Provisional fails to disclose receiving "a selection from a user whether to enter a power save mode, where the power save mode is based on a battery level of the mobile device" and "the power save mode is exited based on a battery level or in response to the user directing the mobile device to exit the power save mode." In terms of user selection to enter and exit power save mode, the '070 Provisional never uses the term "enter" and makes only passing reference to user selection in one paragraph, but not in the context of entry/exit of power save mode. '070 provisional at [00103]. Specifically, paragraph [00103] of the '070 Provisional describes a "mode selector" that "allows the user to turn on or off the optimization of resource usage" and "explicitly select or deselect applications for resource usage optimization." However, user selection related to resource usage optimization is insufficient to demonstrate possession of user selection to enter and exit power save mode. In fact, paragraph [00103] of the '070 Provisional is directed to a different feature of claims 24, 33, and 42; namely, receiving a selection from a user whether to optimize traffic of a first application. *Id.* This single disclosure of user selection cannot be used to provide written

description support for the two, very different user selections found in claims 24, 33, and 42. Thus, the ’070 Provisional does not adequately provide written description support for user selection to enter/exit power save mode. *Id*.

Regarding “battery level,” the ’070 Provisional makes just two mentions of battery level, indicating that battery level may be identified, but providing very limited description of how identified battery level impacts device operation. ’070 provisional at [0049] and [0063]. For instance, paragraph [0063] of the ’070 Provisional generically states that the device may “operate and make decisions according to device state.” Here again, however, the ’070 Provisional does not disclose power save mode being based on battery level of the mobile device and this vague, generic statement about operating and making decisions does not adequately show possession of a power save mode being “based on a battery level of the mobile device,” much less the power save mode being “exited based on a battery level.”

Consequently, the ’070 Provisional does not actually or inherently disclose each and every element of the ’127 patent claims. *Id*. T he introduction of these features into the claims resulted in the ’127 patent claims not being entitled to the filing date of the provisional application, and are, at most, entitled to the filing date of March 24, 2014—the filing date of the ’689 application.

Notably, the PTAB addressed this issue in the context of IPRs filed by Samsung. In one of those IPRs (IPR2018-01108), the PTAB found that claims of the ’070 Provisional did not support the claims at issue in that patent, for example, because the ’070 Provisional “does not describe user selection to enter or exit a power save mode.” Institution Decision at 27 (IPR2018-001108) (“Petitioner also avers that the ’070 application does not describe user selection to enter

or exit a power save mode. *Id*. at 10 (citing Ex. 1010 ¶ 103). On this record, we agree with Petitioner.").

2. Anticipation

Some or all of the Asserted Claims of the '127 patent are invalid as anticipated under 35 U.S.C. § 102 in view of each of the prior art references identified above and in the claim charts included in **Exhibit 127-A**, which identify specific examples of where each limitation of the Asserted Claims is found in the prior art references. As explained above, the cited portions of prior art references identified in the attached claim charts are exemplary only and representative of the content and teaching of the prior art references, and should be understood in the context of the reference as a whole and as they would be understood by a person of ordinary skill in the art.

Apple identifies the following references as anticipating one or more of the Asserted Claims of the '127 patent under 35 U.S.C. § 102. The below table of anticipating references is exemplary, and it does not constitute an admission that any reference anticipates only the listed claims. Further, Apple contends that any prior art reference in the attached charts that is charted for each limitation of any given claim, anticipates that claim, regardless of whether that prior art reference is listed in the following table.

Ex.#	Anticipating Prior Art	Claims
127-A01	U.S. Patent Pub. No. 2010/0317374 to Alpert ("Alpert")	24, 26, 28-33, 36-38, 40-42, 44, 46-48, 50
127-A02	U.S. Patent Pub. No. 2007/0286222 to Balasubramanian ("Balasubramanian")	24, 26-30, 32-33, 35-38, 40-42, 44-48, 50
127-A03	U.S. Patent No. 9,146,778 to Jiang ("Jiang")	24-50
127-A04	U.S. Patent Pub. No. 2010/0250986 to Black ("Black V")	24, 26-30, 32-33, 35-38, 40-42, 44-48, 50
127-A05	U.S. Patent No. 8,838,086 to Giaretta ("Giaretta 086")	24-50
127-A06	U.S. Patent NO. 9,264,868 to Giaretta ("Giaretta 868")	24, 26-33, 35-48, 50
127-A07	U.S. Patent No. 8,886,176 to Luna ("Luna 176")	24-50

Ex.#	Anticipating Prior Art	Claims
127-A08	U.S. Patent Pub. No. 2013/0010693 to Luna ("Luna 693")	24-50
127-A09	Application-Driven Power Management for Mobile Communication to Kravets ("Kravets")	24, 26-30, 32-33, 35-38, 40-42, 44-48, 50
127-A10	U.S. Patent No. 8,943,204 to Andrada ("Andrara")	24, 26-30, 32-33, 35-38, 40-42, 44-48, 50
127-A11	U.S. Patent No. 9,043,433 to Backholm ("Backholm")	24-50
127-A12	U.S. Patent No. 9,474,022 to Lin ("Lin")	24, 26-27, 29-30, 32-33, 36-38, 40-42, 44-45, 47-48, 50
127-A13	U.S. Patent Pub. No. 2011/0185202 to Black ("Black I")	24, 26-27, 29-30, 32-33, 36-38, 40-42, 44-45, 47-48, 50
127-A14	U.S. Patent Pub. No. 2011/0131321 to Black ("Black II")	24, 26-27, 29-30, 32-33, 36-38, 40-42, 44-45, 47-48, 50
127-A15	U.S. Patent Pub. No. 2012/0272230 to Lee ("Lee II")	24, 26-27, 29-30, 32-33, 36-38, 40-42, 44-45, 47-48, 50
127-A16	European Patent Pub. No. EP 2343930 A2 to Sengottaiyan ("Sengottaiyan")	24, 26-27, 29-30, 32-33, 36-38, 40-42, 44-45, 47-48, 50
127-A17	U.S. Patent Pub. No. 2012/0023236 to Backholm ("Backholm 236")	24, 26, 28-33, 36-42, 44, 46-50
127-A18	JuiceDefender App	24-50
127-A19	Android devices running an Android OS with Applications ("Android")	24-50
127-A20	U.S. Patent Pub.No. 2014/0195839 ("Chueh")	24-50

To the extent any item of prior art cited above is deemed not to disclose, explicitly or inherently, any limitation of an Asserted Claim of the '127 patent, Apple reserves the right to argue that any difference between that prior art and the corresponding patent claim would have been either inherent to the art, or obvious to a person of ordinary skill in the art, even if Apple has not specifically denoted that the art is to be combined with the knowledge of a person of ordinary skill in the art.

3. Obviousness

To the extent any limitation is deemed not to be exactly met by an item of prior art listed above and in **Exhibit 127-A**, then any purported differences are such that the claimed subject matter as a whole would have been obvious to one skilled in the art at the time of the alleged

invention, in view of the state of the art and knowledge of those skilled in the art. The item of prior art would, therefore, render the relevant claims invalid for obviousness under 35 U.S.C. § 103.

In addition, the references identified above render one or more Asserted Claims of the '127 patent obvious when the references are read in combination with each other, and/or when read in view of the state of the art and knowledge of those skilled in the art. Each and every reference identified is also relevant to the state of the art at the time of the alleged invention. Any of the references disclosed above may be combined with one another to render obvious (and therefore invalid) each of SEVEN's Asserted Claims. Apple may rely upon a subset of the above identified references or all of the references identified above, including all references in **Exhibits 127-A, 127-B, and C**, for purposes of obviousness depending on the Court's claim construction, positions taken by SEVEN during this litigation, and further investigation and discovery.

To the extent the foregoing references are found not to anticipate the Asserted Claims, the foregoing references render the Asserted Claims obvious either alone or in combination with one or more of the other references identified above pursuant to Patent Rule 3-3(a). It would have been obvious to a person of skill in the art at the time of the alleged invention of the Asserted Claims of the '127 patent to combine the various references cited herein so as to disclose the Asserted Claims of the '127 patent.

In accordance with Patent Rule 3-3(b), prior art references rendering the Asserted Claims obvious, alone or in combination with other references, are outlined below and included in **Exhibits 127-A and 127-B**, which include exemplary claim charts for the Asserted Claims of the '127 patent showing specifically where in each reference or combinations of references each

Asserted Claim is found, and an explanation of why the prior art renders the Asserted Claim obvious. Where applicable, **Exhibits 127-A and 127-B** include the motivation to combine references.

Moreover, in addition to the information contained elsewhere in these contentions and in particular **Exhibit 127-B**, Apple has identified additional motivations and reasons to combine the various references cited herein. In particular, multiple teachings, suggestions, and/or reasons to modify any of the references and/or to combine any two or more of the references in **Exhibits 127-A and 127-B** come from many sources, including the prior art (specific and as a whole), common knowledge, common sense, predictability, expectations, industry trends, design incentives or need, market demand or pressure, market forces, obvious to try, the nature of the problem faced, and/or knowledge possessed by one of ordinary skill. In addition, it would have been obvious to try combining the prior art references identified above because there were only a finite number of predictable solutions and/or because known work in one field or endeavor prompted variations based on predictable design incentives and/or market forces either in the same field or a different one. The combination of prior art references identified in these contentions would have been obvious because the claimed combinations represent the known potential options with a reasonable expectation of success. Additionally, one of ordinary skill in the art would have been motivated to create combinations identified in these contentions using: known methods to yield predictable results; known techniques in the same way; a simple substitution of one known, equivalent element for another to obtain predictable results; and/or teaching, suggestion, or motivation in the prior art generally. Also, market forces in the industry, and the desire to improve features and performance, would motivate the addition of features to systems as they become available, become less expensive, become more commonly used,

provide better performance, reduce costs, size or weight, or predictably achieve other clearly desirable results.

While Apple reserves the right to rely on any combination of the references reflected in their charts or incorporated herein by reference, Apple provides the following exemplary and non-exhaustive references and/or combinations evidencing invalidity of the claims of the Asserted Patents. The combinations of prior art listed below render obvious the Asserted Claims under the proper construction of the claims and/or under Plaintiff's apparent interpretation of the claims as set forth by Plaintiff in their Complaint and Infringement Contentions. Each combination renders the identified claims obvious through the express and/or inherent disclosure in the combination of references themselves, as well as in view of the knowledge of a person of ordinary skill in the art.

Obviousness Combinations	Claims
Alpert in view of one or more of U.S. Patent No. 9,338,749 to Kim ("Kim"), Find Which Apps, Process On Android Phone Using Most Battery Power ("Which Apps"), Giaretta 086, JuiceDefender, Luna 176, U.S. Patent Publication No. 2008/0057894 ("Aleksic"), U.S. Patent No. 7,231,198 to Loughran ("Loughran"), U.S. Patent Publication No. 2012/0315960 ("Kim960"), Android, Hackborn, and/or Jiang	Claims 24-50
Balasubramania in view of one or more of Kim, Which Apps, Giaretta 086, Luna 176, JuiceDefender, Aleksic, Loughran, Hackborn, Android and/or Jiang	Claims 24-50
Jiang in view of one or more of Kim, Giaretta 086, Luna 176, JuiceDefender, Aleksic, Loughran, Android, Hackborn, and/or Which Apps	Claims 24-50
Black V in view of one or more of Kim, Which Apps, Luna 176, Giaretta 086, JuiceDefender, Aleksic, Hackborn, Loughran, Android and/or Jiang	Claims 24-50

Obviousness Combinations	Claims
Giaretta 086 in view of one or more of Kim, Which Apps, Luna 176, JuiceDefender, Kim960, Aleksic, Loughran, Hackborn, Android and/or Jiang	Claims 24-50
Giaretta 868 in view of one or more of Kim, Which Apps, Luna 176, JuiceDefender, Giaretta 086, Aleksic, Hackborn, Kim960, Loughran, Android and/or Jiang	Claims 24-50
Luna 176 in view of one or more of Kim, Which Apps, Giaretta 086, JuiceDefender, Aleksic, Loughran, Hackborn, Kim960, Android and/or Jiang	Claims 24-50
Luna 693 in view of one or more of Kim, Which Apps, Giaretta 086, Luna 176, JuiceDefender, Aleksic, Hackborn, Loughran, Android and/or Jiang	Claims 24-50
Kravets in view of one or more of Kim, Which Apps, Giaretta 086, Luna 176, JuiceDefender, Aleksic, Hackborn, Loughran, Android and/or Jiang	Claims 24-50
Andrara in view of one or more of Kim, Which Apps, Giaretta 086, Luna 176, JuiceDefender, Aleksic, Hackborn, Loughran, Android and/or Jiang	Claims 24-50
Backholm in view of one or more of Kim, Giaretta 086, Which Apps, Luna 176, JuiceDefender, Aleksic, Hackborn, Kim960, Loughran, Android and/or Jiang	Claims 24-50
Lin in view of one or more of Kim, Which Apps, Giaretta 086, Luna 176, JuiceDefender, Aleksic, Loughran, Hackborn, Android and/or Jiang	Claims 24-50
Black I in view of one or more of Kim, Which Apps, Giaretta 086, Luna 176, Hackborn, JuiceDefender, Aleksic, Loughran, Android and/or Jiang	Claims 24-50
Black II in view of one or more of Kim, Which Apps, Giaretta 086, Luna 176, JuiceDefender, Aleksic, Hackborn, Loughran, Android and/or Jiang	Claims 24-50
Lee II in view of one or more of Kim, Which Apps, Giaretta 086, Luna 176, Hackborn, JuiceDefender, Loughran, Android and/or Jiang	Claims 24-50

Obviousness Combinations	Claims
Sengottaiyan in view of one or more of Kim, Which Apps, Giaretta 086, Luna 176, JuiceDefender, Aleksic, Loughran, Kim960, Android and/or Jiang	Claims 24-50
Backholm 236 in view of one or more of Kim, Which Apps, Giaretta 086, Luna 176, JuiceDefender, Aleksic, Loughran, Kim960, Hackborn, Android and/or Jiang	Claims 24-50
JuiceDefender in view of one or more of Kim, Which Apps, Giaretta 086, Luna 176, Hackborn, Aleksic, Loughran, Kim960, Android, and/or Jiang	Claims 24-50
Android in view of one or more of Kim, Which Apps, Giaretta 086, Luna 176, JuiceDefender, Aleksic, Loughran, Kim960, Hackborn, and/or Jiang	Claims 24-50
Chueh in view of one or more of Android, Kim, Which Apps, Giaretta 086, Hackborn, Luna 176, JuiceDefender, Aleksic, Loughran, Kim960, and/or Jiang	Claims 24-50

In addition to the specific combinations of prior art and the specific combinations of groups of prior art disclosed above, Apple reserves the right to rely on any other combination of any prior art references disclosed herein. Apple further reserves the right to rely upon combinations disclosed within the prosecution history of the references cited herein. These obviousness combinations reflect Apple's present understanding of the potential scope of the claims that SEVEN appears to be advocating and should not be seen as Apple's acquiescence to SEVEN's interpretation of the patent claims.

Apple also reserves the right to amend or supplement these contentions regarding anticipation or obviousness of the Asserted Claims, in view of further information from SEVEN, information discovered during discovery, or a claim construction ruling by the Court. SEVEN has not identified what elements or combinations it alleges were not known to one of ordinary skill in the art at the time. Therefore, for any claim limitation that SEVEN alleges is not

disclosed in a particular prior art reference, Apple reserves the right to assert that any such limitation is either inherent in the disclosed reference or obvious to one of ordinary skill in the art at the time in light of the same, or that the limitation is disclosed in another of the references disclosed above and in combination would have rendered the Asserted Claim obvious.

Apple further incorporates by reference the arguments and exhibits presented in the petitions in IPR2018-01051, IPR2018-01052, IPR2018-01108, IPR2019-00460, IPR2018-01106, IPR2019-00458, IPR2019-00457.

C. Patent Rule 3-3(c): Charts Identifying Where Specifically in Each Alleged Item of Prior Art Each Asserted Claim Is Found

Pursuant to Patent Rule 3-3(c), charts identifying where specifically in each alleged item of prior art each limitation of each Asserted Claim is found, including for each limitation that Apple contends is governed by 35 U.S.C. § 112(6), the identity of the structure(s), act(s), or material(s) in each item of prior art that performs the claimed function, are attached in **Exhibits 127-A and 127-B**.

D. Patent Rule 3-3(d): Other Grounds for Invalidity

Apple identifies the following grounds for invalidity of the Asserted Claims of the '127 patent based on 35 U.S.C. §§ 101 and/or 112. Apple reserves the right to supplement these disclosures based on further investigation and discovery.

1. Invalidity Pursuant to 35 U.S.C. § 112

Apple further asserts that the Asserted Claims of the '127 patent are invalid under 35 U.S.C. § 112. The following are the grounds upon which Apple contends the Asserted Claims are invalid for failure to meet the requirements of 35 U.S.C. § 112, ¶ 1, ¶ 2, ¶ 4 and/or ¶ 6, based on Apple's investigation to date and currently-available information.

For each claim identified as invalid, any dependent claims of those invalid claims are also invalid under 35 U.S.C. § 112, ¶ 1, ¶ 2, ¶ 4, and/or ¶ 6. Apple reserves the right to supplement and amend these contentions based on further discovery and investigation including, in particular, the deposition of any of the named inventors of the Asserted Patent, the parties' claim construction positions, and further investigation of SEVEN's implied infringement positions.

a) Written Description and/or Enablement

At least in view of SEVEN's apparent construction of the claims in its Infringement Contentions, the Asserted Claims of the '127 patent are invalid because the specification as filed does not contain adequate written description of the claimed inventions sufficient to lead a person of ordinary skill in the art to understand that the named inventors had possession of the purported inventions as claimed as required by 35 U.S.C. § 112, ¶ 1. Likewise, the specification does not enable one of ordinary skill in the art to make or use the claimed inventions without undue experimentation. Based on Apple's present understanding of SEVEN's infringement contentions, Apple asserts that the Asserted Claims of the of the '127 patent are invalid for reciting at least the following claim terms/phrases/limitations:

- Claims 24, 33, and 42 of the '127 patent and their dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain an adequate written description and/or enabling disclosure of "optimize background traffic." The specification does not provide any support for background traffic nor the optimization of background traffic. The only disclosure related to "background" in the specification is the disclosure of an "application state detector (e.g., foreground/background state)." The specification does not provide any support as to what is foreground vs. background state, what entails background traffic, nor how to optimize

background traffic. Accordingly, the specification fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

- Claims 32, 40, and 50 of the '127 patent and their dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain an adequate written description and/or enabling disclosure of "wherein to adjust a timing of activities comprises to adjust activities related to background traffic of the second application." As discussed above, the specification does not provide any support for background traffic. The only disclosure related to "background" in the specification is the disclosure of an "application state detector (e.g., foreground/background state)." Given inadequate disclosure of background traffic, "activities related to background traffic" lacks further written description. Accordingly, the specification fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.
- Claims 24, 33, and 42 of the '127 patent and their dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain an adequate written description and/or enabling disclosure of "receiving a selection from a user whether to enter power save mode, where the power save mode is based on a battery level of the mobile device." The specification does not provide any support for the user selection to

enter power save mode, nor a power save mode that is based on a battery level of the mobile device. In fact, the term power save mode is only used in the claims, and never used in the specification. The limitation requiring "receiving a selection from a user whether to enter a power save mode, where the power save mode is based on a battery level of the mobile device" also lacks written description support and/or is not enabled, at least to the extent that SEVEN contends this limitation is satisfied by Apple's products. Apple's accused products do not have a "power save mode" that is based on the battery level of the mobile device. The feature that SEVEN identifies in its infringement contentions is not "based on a battery level of the mobile device." Thus, to the extent the claim is interpreted broad enough to encompass to include features that are not "based on a battery level of the mobile device," this limitation lacks 112 support. Accordingly, the specification fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

- Claims 24, 33, and 42 of the '127 patent and their dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain an adequate written description and/or enabling disclosure of "upon selection to enter the power save mode, adjust a timing of activities of a second application executing in the background of the mobile device to reduce usage of at least one resource of the mobile device." The specification does not provide any support for the user selection to enter power save mode, nor adjusting a timing of activities of a second application executing

in the background of the mobile device to reduce usage of at least one resource of the mobile device upon selection to enter the power save mode. In fact, the term power save mode is only used in the claims, and never used in the specification. The limitation requiring "upon selection to enter the power save mode, adjust a timing of activities of a second application executing in the background of the mobile device to reduce usage of at least one resource of the mobile device" also lacks written description support and/or is not enabled, at least to the extent that SEVEN contends this limitation is satisfied by Apple's products. Apple's accused products do not have a "power save mode" that adjusts a timing of activities of a second application executing in the background of the mobile device to reduce usage of at least one resource of the mobile device upon selection to enter the power save mode. The feature that SEVEN identifies in its infringement contentions does not "upon selection to enter the power save mode, adjust a timing of activities of a second application executing in the background of the mobile device to reduce usage of at least one resource of the mobile device." Thus, to the extent the claim is interpreted broad enough to encompass to include features that do not "upon selection to enter the power save mode, adjust a timing of activities of a second application executing in the background of the mobile device to reduce usage of at least one resource of the mobile device," this limitation lacks 112 support. Accordingly, the specification fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

- Claims 24, 33, and 42 of the ’127 patent and their dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain an adequate written description and/or enabling disclosure of “exit the power save mode, wherein the power save mode is exited based on a battery level or in response to the user directing the mobile device to exit the power save mode.” The specification does not disclose any support for the power save mode, nor exiting a power save mode based on batter level or in response to the user selection. As discussed above, the specification does not use the word power save mode, and how to exit power save mode. Accordingly, the specification fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.
- Claims 25, 34, and 43 of the ’127 patent and their dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain an adequate written description and/or enabling disclosure of “receive a selection from a user to enter the power save mode is in response to a query to the user on a user interface of the mobile device.” The specification does not disclose any support for the power save mode, nor entering the power save mode is in response to a query to the user on a user interface of the mobile device. As discussed above, the specification does not use the word power save mode, or mention a query to the user.

b) Indefiniteness

At least in view of SEVEN's apparent construction of the claims in its Infringement Contentions, the Asserted Claims of the '127 patent are invalid because they fail to particularly point out and distinctly claim the subject matter which the applicant regards as his invention under 35 U.S.C. § 112, ¶¶ 2, 4, and/or 6. Based on Apple's present understanding of SEVEN's infringement contentions, Apple asserts that the Asserted Claims of the of the '127 patent are invalid for reciting at least the following claim terms/phrases/limitations:

- Claims 24, 33, and 42 of the '127 patent and their dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 2, ¶ 4, and/or ¶ 6 because the specification does not describe or otherwise inform one of ordinary skill about what constitutes "application executing in a background of the mobile device." The patent does not specify how one distinguishes between "application executing in a background" (as opposed to application executing in a foreground). As such, one of ordinary skill would not understand the metes and bounds of the identified claims, rendering them indefinite under 35 U.S.C. § 112, ¶ 2. Therefore, these claims, when read in light of the specification and the prosecution history, "fail to inform, with reasonable certainty, those skilled in the art about the scope of the invention." *Nautilus, Inc. v. Biosig Instruments, Inc*., 134 S. Ct. 2120, 2124 (2014).
- Claims 24, 33, and 42 of the '127 patent and their dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 2, ¶ 4, and/or ¶ 6 because the specification does not describe or otherwise inform one of ordinary skill about what constitutes "background traffic." The patent does not specify

how one distinguishes between "background traffic" (as opposed to foreground traffic). As such, one of ordinary skill would not understand the metes and bounds of the identified claims, rendering them indefinite under 35 U.S.C. § 112, ¶ 2. Therefore, these claims, when read in light of the specification and the prosecution history, "fail to inform, with reasonable certainty, those skilled in the art about the scope of the invention." *Nautilus, Inc. v. Biosig Instruments, Inc.*, 134 S. Ct. 2120, 2124 (2014).

- Claims 31, 39, and 49 of the '127 patent and their dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 2, ¶ 4, and/or ¶ 6 because the specification does not describe or otherwise inform one of ordinary skill about what constitutes "adjust[ing] timing activities of the second application based on predicted user activity of the second application." The patent does not specify what "based on predicted user activity of the second application" constitutes. As such, one of ordinary skill would not understand the metes and bounds of the identified claims, rendering them indefinite under 35 U.S.C. § 112, ¶ 2. Therefore, these claims, when read in light of the specification and the prosecution history, "fail to inform, with reasonable certainty, those skilled in the art about the scope of the invention." *Nautilus, Inc. v. Biosig Instruments, Inc.*, 134 S. Ct. 2120, 2124 (2014).
- Claims 32, 40, and 50 of the '127 patent and their dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 2, ¶ 4, and/or ¶ 6 because the specification does not describe or otherwise inform one of ordinary skill about what constitutes "activities related to background traffic." The patent

does not specify how one distinguishes between "background traffic" (as opposed to foreground traffic). Furthermore, the patent specification does not specify what constitutes "activities related to background traffic." As such, one of ordinary skill would not understand the metes and bounds of the identified claims, rendering them indefinite under 35 U.S.C. § 112, ¶ 2. Therefore, these claims, when read in light of the specification and the prosecution history, "fail to inform, with reasonable certainty, those skilled in the art about the scope of the invention." *Nautilus, Inc. v. Biosig Instruments, Inc*., 134 S. Ct. 2120, 2124 (2014).

2. Other Grounds for Invalidity

In addition to the preceding invalidity contentions, Apple further contends that each of the Asserted Claims of the '127 patent is drawn to subject matter that is not patentable under 35 U.S.C. § 101. The '127 patent Asserted Claims are invalid under 35 U.S.C. § 101 for failure to recite patent eligible subject matter. Specifically, all claims of the '127 patent are fatally abstract under the U.S. Supreme Court's decision in *Alice Corp. v. CLS Bank Int'l*, 134 S. Ct. 2345 (2014) and progeny.

The claims of the '127 patent as whole relate to optimizing traffic and resource of mobile phones by grouping or changing the timing of activities. At the most basic level, the claims of the '127 patent are directed to adjusting the timing of activities, which is a long prevalent human activity. The asserted claims of the '127 patent do not contain any inventive concept. At the time of the alleged invention, the elements of the asserted claims were well understood, routine, and/or conventional in the mobile computing and/or computer networking industries. The '127 patent Asserted Claims employ well-known components or functionality, as shown in Apple's invalidity contentions involving anticipation and/or obviousness in this case, which is not enough

to impart patent eligibility of an abstract idea. Further detail regarding Apple's contentions that the Asserted Claims of the '127 patent do not qualify as patent-eligible subject matter are contained in **Exhibit 127-D**.

Apple reserves the right to assert that the asserted patents are invalid under 35 U.S.C. §102(f) and/or (g) in the event Apple obtains evidence that the named inventors of the '127 patent did not invent (either alone or in conjunction with other parties) the subject matter claimed in the '127 patent. Should Apple obtain such evidence, it will provide the name of the person(s) from whom and the circumstances under which the invention or any part of it was derived, and/or the circumstances surrounding the making of the invention before the patent application.

Apple reserves the right to supplement these disclosures based on further investigation and discovery.

V. THE '056 PATENT

A. Patent Rule 3-3(a): Identification of Prior Art

At this time, Apple contends that at least each of the prior art references described and charted in **Exhibits 056-A and 056-B** anticipates or renders obvious, either alone or in combination, one or more of the Asserted Claims of the '056 patent.

Additional prior art that has not been charted, but is still relevant to the invalidity of the '056 patent is listed in **Exhibit C**, including without limitation as evidence of the state of the art at the alleged time of invention. Apple reserves the right to amend these invalidity contentions to assert these references depending on the claim construction and infringement positions SEVEN may take as the case proceeds. Moreover, Apple reserves the right to use these references in combination with other references to render the claims of the '056 patent obvious in the event SEVEN takes the position that certain claim limitations are missing from the references charted in **Exhibits 056-A and 056-B**.

B. Patent Rule 3-3(b): Whether Each Item Anticipates or Renders Obvious the Asserted Claims

SEVEN asserts claims 1-19 of the ’056 patent against Apple in this lawsuit. These claims are invalid because the ’056 patent fails to meet one or more of the requirements for patentability. The individual bases for invalidity are provided below and in the claim charts attached as **Exhibits 056-A and 056-B.** Each of the foregoing listed prior art documents, the underlying work, and/or the underlying apparatus or method qualifies as prior art under one or more sections of 35 U.S.C. §§ 102 and/or 103.

Although Apple has identified at least one citation per limitation for each reference, each and every disclosure of the same limitation in the same reference is not necessarily identified. Rather, in an effort to focus the issues, Apple has cited representative portions of identified references, even where a reference may contain additional support for a particular claim element. In addition, persons of ordinary skill in the art generally read a prior art reference as a whole and in the context of other publications and literature. Thus, to understand and interpret any specific statement or disclosure within a prior art reference, such persons would rely on other information within the reference, along with other publications and their general scientific knowledge. Apple may rely upon uncited portions of the prior art references and on other publications and expert testimony to provide context, and as aids to understanding and interpreting the portions that are cited. Apple may also rely on uncited portions of the prior art references, other disclosed publications, and the testimony of experts to establish that a person of ordinary skill in the art would have been motivated to modify or combine certain of the cited references so as to render the claims obvious.

1. Priority

SEVEN's Patent Rule 3-1(e) disclosures provide that the Asserted Claims of the '056 patent are entitled to a priority date of July 26, 2010, which is the filing date of U.S. Provisional Application Nos. 61/367,870 ("870 provisional application") and 61/367,871 ("871 provisional application").

Apple reserves the right to challenge SEVEN's assertion that the '056 patent is entitled to claim the benefit of these provisional applications' filing date to the extent that these provisional applications do not support the full scope of the Asserted Claims, for example, depending on scope of the Asserted Claims as properly construed. To the extent the provisional application does not support the full scope of the Asserted Claims, the priority date of the '056 patent should be no earlier than the filing date of the '056 patent's application, which is July 8, 2016.

SEVEN has provided no evidence to support its contention that the Asserted Claims of the '056 patent are entitled to claim priority back to this or any earlier filed application, and Apple therefore reserves the right to assert a later priority date based on any findings as to the priority date of the Asserted Claims by the Court, information learned through discovery, or otherwise.

a) The Asserted Claims of the '056 Patent Cannot Claim Priority to the '870 or '871 Provisional Applications

None of the Asserted Claims are entitled to the filing date of the '870 or '871 provisional applications (the earliest priority date claimed) because they do not have written description support in these provisional applications. *See, e.g., Falko-Gunter Falkner v. Inglis,* 448 F.3d 1357 (Fed. Cir. 2006). Significant portions of the '871 provisional application were reproduced tin the specification of the '056 patent, and for at least the reasons provided below in Apple's contentions as to why the '056 patent specification does not support the Asserted Claims, this

provisional application likewise do not provide support for these claims. Furthermore, the '870 provisional application, which names an inventor that does not appear on the face of the '056 patent, also do not provide support for the Asserted Claims. For example, neither the '870 or '871 provisional application discuss "batch[ing] data from a first application and a second application" while a backlight is off in response to inactivity or "allow[ing] a first message from a remote server distinct from the first application server and the second application server to be received while the batched data from the first application and the second application is batched."

b) The Asserted Claims of the '056 Patent Cannot Claim Priority to Any Other Provisional Application

The remaining provisional applications also do not provide support for the Asserted Claims. The majority of these provisional applications were purportedly invented by individuals who are not named as inventors of the '056 patent. *See* Provisional Application Nos. 61/408,839; 61/408,846; 61/408,854; 61/408,826; 61/416,020; 61/416,033; 61/430,828. The remaining provisional applications also do not provide support for the limitations discussed below in Apple's written description and enablement contentions. *See* Provisional Application Nos. 61/408,820; 61/408,829; 61/408,858.

2. Anticipation

Some or all of the Asserted Claims of the '056 patent are invalid as anticipated under 35 U.S.C. § 102 in view of each of the prior art references identified above and in the claim charts included in **Exhibit 056-A**, which identify specific examples of where each limitation of the Asserted Claims is found in the prior art references. As explained above, the cited portions of prior art references identified in the attached claim charts are exemplary only and representative of the content and teaching of the prior art references, and should be understood in the context of the reference as a whole and as they would be understood by a person of ordinary skill in the art.

Apple identifies the following references as anticipating one or more of the Asserted Claims of the ’056 patent under 35 U.S.C. § 102. The below table of anticipating references is exemplary, and it does not constitute an admission that any reference anticipates only the listed claims. Further, Apple contends that any prior art reference in the attached charts that is charted for each limitation of any given claim, anticipates that claim, regardless of whether that prior art reference is listed in the following table.

Ex.#	Anticipating Prior Art	Claims
056-A01	U.S. Patent Application No. 2009/0217065A1 to Araujo et. al. (“Araujo”)	Claims 1-19
056-A02	U.S. Patent Application No. 2010/0077035 to Li et al. (“Li”)	Claims 1-19
056-A03	U.S. Patent No. 6,463,307 to Mikael Larsson et al. (“Larsson”)	Claims 1-19
056-A04	U.S. Patent No. 8,904,206 to Gregory R. Black et al. (“Black 206”)	Claims 1-19
056-A05	U.S. Published Patent Application No. 2006/0200849 to Prabakar Sundarrajan et al. (“Sundarrajan”)	Claims 1-19
056-A07	U.S. Published Patent Application No. 2010/0088387 to Pablo Calamera (“Calamera”)	Claims 1-19
056-A08	U.S. Published Patent Application No. 2005/0108075 to Fredrick Douglis et al. (“Douglis”)	Claims 1-19
056-A09	U.S. Patent No. 7,873,349 to Corey Smith et al. (“Smith”)	Claims 1-19
056-A11	Nokia E72 System	Claims 1-19
056-A14	Android User Guide / Nexus One User Guide (“Android User Guide”)	Claims 1-2, 4-5, 7-8, 10-11, 13-14, 16-17, 19

To the extent any item of prior art cited above is deemed not to disclose, explicitly or inherently, any limitation of an Asserted Claim of the ’056 patent, Apple reserves the right to argue that any difference between that prior art and the corresponding patent claim would have been either inherent to the art, or obvious to a person of ordinary skill in the art, even if Apple has not specifically denoted that the art is to be combined with the knowledge of a person of ordinary skill in the art.

3. Obviousness

To the extent any limitation is deemed not to be exactly met by an item of prior art listed above and in **Exhibit 056-A**, then any purported differences are such that the claimed subject matter as a whole would have been obvious to one skilled in the art at the time of the alleged invention, in view of the state of the art and knowledge of those skilled in the art. The item of prior art would, therefore, render the relevant claims invalid for obviousness under 35 U.S.C. § 103.

In addition, the references identified above render one or more Asserted Claims of the '056 patent obvious when the references are read in combination with each other, and/or when read in view of the state of the art and knowledge of those skilled in the art. Each and every reference identified is also relevant to the state of the art at the time of the alleged invention. Any of the references disclosed above may be combined with one another to render obvious (and therefore invalid) each of SEVEN's Asserted Claims. Apple may rely upon a subset of the above identified references or all of the references identified above, including all references in **Exhibits 056-A, 056-B, and C,** for purposes of obviousness depending on the Court's claim construction, positions taken by SEVEN during this litigation, and further investigation and discovery.

To the extent the foregoing references are found not to anticipate the Asserted Claims, the foregoing references render the Asserted Claims obvious either alone or in combination with one or more of the other references identified above pursuant to Patent Rule 3-3(a). It would have been obvious to a person of skill in the art at the time of the alleged invention of the Asserted Claims of the '056 patent to combine the various references cited herein so as to disclose the Asserted Claims of the '056 patent.

In accordance with Patent Rule 3-3(b), prior art references rendering the Asserted Claims obvious, alone or in combination with other references, are outlined below and included in **Exhibits 056-A and 056-B**, which include exemplary claim charts for the Asserted Claims of the '056 patent showing specifically where in each reference or combinations of references each Asserted Claim is found, and an explanation of why the prior art renders the Asserted Claim obvious. Where applicable, **Exhibits 056-A and 056-B** include the motivation to combine references.

Moreover, in addition to the information contained elsewhere in these contentions and in particular **Exhibit 056-B**, Apple has identified additional motivations and reasons to combine the various references cited herein. In particular, multiple teachings, suggestions, and/or reasons to modify any of the references and/or to combine any two or more of the references in **Exhibits 056-A and 056-B** come from many sources, including the prior art (specific and as a whole), common knowledge, common sense, predictability, expectations, industry trends, design incentives or need, market demand or pressure, market forces, obvious to try, the nature of the problem faced, and/or knowledge possessed by one of ordinary skill. In addition, it would have been obvious to try combining the prior art references identified above because there were only a finite number of predictable solutions and/or because known work in one field or endeavor prompted variations based on predictable design incentives and/or market forces either in the same field or a different one. The combination of prior art references identified in these contentions would have been obvious because the claimed combinations represent the known potential options with a reasonable expectation of success. Additionally, one of ordinary skill in the art would have been motivated to create combinations identified in these contentions using: known methods to yield predictable results; known techniques in the same way; a simple

substitution of one known, equivalent element for another to obtain predictable results; and/or teaching, suggestion, or motivation in the prior art generally. Also, market forces in the industry, and the desire to improve features and performance, would motivate the addition of features to systems as they become available, become less expensive, become more commonly used, provide better performance, reduce costs, size or weight, or predictably achieve other clearly desirable results.

While Apple reserves the right to rely on any combination of the references reflected in their charts or incorporated herein by reference, Apple provides the following exemplary and non-exhaustive references and/or combinations evidencing invalidity of the claims of the Asserted Patents. The combinations of prior art listed below render obvious the Asserted Claims under the proper construction of the claims and/or under Plaintiff's apparent interpretation of the claims as set forth by Plaintiff in their Complaint and Infringement Contentions. Each combination renders the identified claims obvious through the express and/or inherent disclosure in the combination of references themselves, as well as in view of the knowledge of a person of ordinary skill in the art.

Obviousness Combinations	**Claims**
Araujo in view of Li, Larsson, Black 206, Sundarrajan, Quintana, Calamera, Douglis, Smith, U.S. Published Patent Application No. 2014/0362702 to Michael Luna et al. ("Luna 702"), Nokia E72 System, U.S. Published Patent Application No. 2014/0366042 to David Michael Chan et. al. ("Chan"), Wei Huang, Android Cloud to Device Messaging ("Huang"), Android User Guide, and/or U.S. Patent No. 6,697,953 to Collins et al. ("Collins")	Claims 1-19
Li in view of Araujo, Larsson, Black 206, Sundarrajan, Quintana, Calamera, Douglis, Smith, Luna 702, Nokia E72 System, Chan, Huang, Android User Guide, and/or Collins	Claims 1-19
Larsson in view of Araujo, Li, Black 206, Sundarrajan, Quintana, Calamera, Douglis, Smith, Luna 702, Nokia E72 System, Chan, Huang, Android User Guide, and/or Collins	Claims 1-19

Black 206 in view of Araujo, Li, Larsson, Quintana, Calamera, Douglis, Smith, Huang, Android User Guide, and/or Collins	Claims 1-19
Sundarrajan in view of Araujo, Li, Larsson, Black 206, Quintana, Calamera, Douglis, Smith, Luna 702, Nokia E72, Chan, Huang, Android User Guide, and/or Collins	Claims 1-19
Calamera in view of Araujo, Li, Larsson, Black 206, Sundarrajan, Calamera, Douglis, Smith, Luna 702, Nokia E72, Chan, Huang, Android User Guide, and/or Collins	Claims 1-19
Douglis in view of Araujo, Li, Larsson, Black 206, Sundarrajan, Quintana, Calamera, Smith, Luna 702, Nokia E72, Chan, Huang, Android User Guide, and/or Collins	Claims 1-19
Smith in view of Araujo, Li, Larsson, Black 206, Sundarrajan, Quintana, Calamera, Douglis, Smith, Luna 702, Nokia E72 System, Chan, Huang, Android User Guide, and/or Collins	Claims 1-19
Luna 702 in view of Chan, Smith, Sundarrajan, Black 206, Araujo, Larsson, Quintana, Calamera, Huang, Android User Guide, Collins, and/or Douglis	Claims 1-19
Nokia E72 System in view of Araujo, Li, Larsson, Black 206, Sundarrajan, Quintana, Calamera, Douglis, Smith, Luna 702, Chan, Huang, Android User Guide, and/or Collins	Claims 1-19
Chan in view of Luna 702, Smith, Sundarrajan, Black 206, Araujo, Li, Larsson, Quintana, Calamera, Huang, Android User Guide, Collins, and/or Douglis	Claims 1-19
Android User Guide in view of Araujo, Li, Larsson, Black 206, Sundarrajan, Quintana, Calamera, Douglis, Smith, Luna 702, Nokia E72 System, Chan, Huang, Android User Guide, and/or Collins	Claims 1-19
Collins in view of Araujo, Li, Larsson, Black 206, Sundarrajan, Quintana, Calamera, Douglis, Smith, Luna 702, Nokia E72 System, Chan, Huang, Android User Guide, and/or Collins	Claims 1-19

In addition to the specific combinations of prior art and the specific combinations of groups of prior art disclosed above, Apple reserves the right to rely on any other combination of any prior art references disclosed herein. Apple further reserves the right to rely upon combinations disclosed within the prosecution history of the references cited herein. These obviousness combinations reflect Apple's present understanding of the potential scope of the claims that SEVEN appears to be advocating and should not be seen as Apple's acquiescence to SEVEN's interpretation of the patent claims.

Apple also reserves the right to amend or supplement these contentions regarding anticipation or obviousness of the Asserted Claims, in view of further information from SEVEN, information discovered during discovery, or a claim construction ruling by the Court. SEVEN has not identified what elements or combinations it alleges were not known to one of ordinary skill in the art at the time. Therefore, for any claim limitation that SEVEN alleges is not disclosed in a particular prior art reference, Apple reserves the right to assert that any such limitation is either inherent in the disclosed reference or obvious to one of ordinary skill in the art at the time in light of the same, or that the limitation is disclosed in another of the references disclosed above and in combination would have rendered the Asserted Claim obvious.

C. Patent Rule 3-3(c): Charts Identifying Where Specifically in Each Alleged Item of Prior Art Each Asserted Claim Is Found

Pursuant to Patent Rule 3-3(c), charts identifying where specifically in each alleged item of prior art each limitation of each Asserted Claim is found, including for each limitation that Apple contends is governed by 35 U.S.C. § 112(6), the identity of the structure(s), act(s), or material(s) in each item of prior art that performs the claimed function, are attached in **Exhibits 056-A and 056-B.**

D. Patent Rule 3-3(d): Other Grounds for Invalidity

Apple identifies the following grounds for invalidity of the Asserted Claims of the ’056 patent based on 35 U.S.C. §§ 101 and/or 112. Apple reserves the right to supplement these disclosures based on further investigation and discovery.

1. Invalidity Pursuant to 35 U.S.C. § 112

Apple further asserts that the Asserted Claims of the ’056 patent are invalid under 35 U.S.C. § 112. The following are the grounds upon which Apple contends the Asserted Claims

are invalid for failure to meet the requirements of 35 U.S.C. § 112, ¶ 1, ¶ 2, ¶ 4 and/or ¶ 6, based on Apple's investigation to date and currently-available information.

For each claim identified as invalid, any dependent claims of those invalid claims are also invalid under 35 U.S.C. § 112, ¶ 1, ¶ 2, ¶ 4, and/or ¶ 6. Apple reserves the right to supplement and amend these contentions based on further discovery and investigation including, in particular, the deposition of any of the named inventors of the Asserted Patent, the parties' claim construction positions, and further investigation of SEVEN's implied infringement positions.

a) Written Description and/or Enablement

At least in view of SEVEN's apparent construction of the claims in its Infringement Contentions, the Asserted Claims of the '056 patent are invalid because the specification as filed does not contain adequate written description of the claimed inventions sufficient to lead a person of ordinary skill in the art to understand that the named inventors had possession of the purported inventions as claimed as required by 35 U.S.C. § 112, ¶ 1. Likewise, the specification does not enable one of ordinary skill in the art to make or use the claimed inventions without undue experimentation. Based on Apple's present understanding of SEVEN's infringement contentions, Apple asserts that the Asserted Claims of the of the '056 patent are invalid for reciting at least the following claim terms/phrases/limitations:

Claims 1, 10, and 19 of the '056 patent and their dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain an adequate written description and/or enabling disclosure of "[batching data] from a first application and a second application for transmission to a respective first application server and a second application server over the wireless network." Although the patent specification mentions the notion of "batches" or "batching" at various places, it does not disclose that data from a ***first*** application and a ***second*** application can be batched together. Accordingly, the

specification fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

Claims 1, 10, and 19 of the '056 patent and their dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain an adequate written description and/or enabling disclosure of "[batching data] while a backlight of the mobile device is off in response to inactivity of the mobile device." During prosecution of the '056 patent, the Applicant identified paragraph [00235] of the patent application as support for this claim element. However, this paragraph is devoid of any mention of a backlight, much less the notion of batching data while a backlight is off in response to inactivity. Accordingly, the specification fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

Claims 1, 10, and 19 of the '056 patent and their dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain an adequate written description and/or enabling disclosure of "allow[ing] a first message from a remote server distinct from the first application server and the second application server to be received while the batched data from the first application and the second application is batched" or "receiv[ing] a first message directed to the first application on the mobile device from a remote server distinct from the first application server and the second application server while the batching occurs." Accordingly, the specification fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

Claims 1, 10, and 19 of the ’056 patent and their dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain an adequate written description and/or enabling disclosure of “transmit[ting] the batched data to the respective first application server and the second application server over the wireless network while the backlight of the mobile device remains off.” Accordingly, the specification fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

Claims 5 and 14 of the ’056 patent are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain an adequate written description and/or enabling disclosure of “transmit[ting] the batched data from the first application and the second application based on a time that one of the first application and the second application was last accessed.” Accordingly, the specification fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

Claims 8 and 17 of the ’056 patent are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain an adequate written description and/or enabling disclosure of “wherein the first message from the remote server is received over a first communication channel between the remote server and the mobile device, and the new data is received over a second communication channel between the first application server and the mobile device.” Accordingly, the specification fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

b) Indefiniteness

At least in view of SEVEN's apparent construction of the claims in its Infringement Contentions, the Asserted Claims of the '056 patent are invalid because they fail to particularly point out and distinctly claim the subject matter which the applicant regards as his invention under 35 U.S.C. § 112, ¶¶ 2, 4, and/or 6. Based on Apple's present understanding of SEVEN's infringement contentions, Apple asserts that the Asserted Claims of the of the '056 patent are invalid for reciting at least the following claim terms/phrases/limitations:

- Claims 1 and 19 of the '056 patent and their dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 2, ¶ 4, and/or ¶ 6 because these claims recite that a mobile device is "configured to" perform various steps and include various features. Based on SEVEN's infringement contentions, SEVEN asserts these claims against products that must be modified to include the accused features. For example, Apple's products, as sold, are in an "off" state and are thus not "configured" to perform steps such as receiving or transmitting messages. As another example, SEVEN appears to accuse functionality that is dependent upon how end users modify their devices, which applications end users install on their devices, how app developers program those applications (as running on mobile devices and as running on application servers). As such, one of ordinary skill would not understand the metes and bounds of the identified claims, rendering them indefinite under 35 U.S.C. § 112, ¶ 2. Therefore, the Asserted Claims, when read in light of the specification and the prosecution history, "fail to inform, with reasonable certainty, those skilled in the art about the scope of the invention." *Nautilus, Inc. v. Biosig Instruments, Inc.*, 134 S. Ct. 2120, 2124 (2014).

2. Other Grounds for Invalidity

In addition to the preceding invalidity contentions, Apple further contends that each of the Asserted Claims of the ’056 patent is drawn to subject matter that is not patentable under 35 U.S.C. § 101. The ’056 patent Asserted Claims are invalid under 35 U.S.C. § 101 for failure to recite patent eligible subject matter. Specifically, all claims of the ’056 patent are fatally abstract under the U.S. Supreme Court’s decision in *Alice Corp. v. CLS Bank Int’l*, 134 S. Ct. 2345 (2014) and progeny. The ideas presented in the claims are generally directed to concept of when a mobile device can transmit and receive data. Under *Alice* Step 1, those ideas are abstract, as they relate to a fundamental long prevalent practice. *See Intellectual Ventures I LLC v. Symantec Corp*., 838 F.3d 1307, 1314 (Fed. Cir. 2016). Limiting the invention to a particular technological environment, e.g. generic computer hardware, “do[es] not render an otherwise abstract concept any less abstract.” *Intellectual Ventures I LLC v. Capital One Fin. Corp*., 850 F.3d 1332, 1340 (Fed Cir. 2017). Furthermore, because the patent relates to transmission of information (i.e., generic “data” or “messages”), it is likewise abstract, as “information is … an intangible.” *Electric Power Group, LLC v. Alstom S.A.*, 830 F.3d 1350, 1353 (Fed. Cir. 2016). Furthermore, under *Alice* Step 2 the ’056 patent does not contain any inventive concept. The ’056 patent Asserted Claims employs well-known components or functionality, as shown in Apple’s invalidity contentions involving anticipation and/or obviousness in this case, which is not enough to impart patent eligibility of an abstract idea. *See, e.g., Alice*, 134 S. Ct. at 2359 (holding that limitations describing “‘well-understood, routine, conventional activit[ies]’ previously known to the industry” were insufficient to supply an inventive concept (quoting *Mayo*, 132 S. Ct. at 1294)). Further detail regarding Apple’s contentions that the Asserted Claims of the ’056 patent do not qualify as patent-eligible subject matter are contained in **Exhibit 056-D**.

Apple reserves the right to assert that the asserted patents are invalid under 35 U.S.C. §102(f) and/or (g) in the event Apple obtains evidence that the named inventors of the ’056 patent did not invent (either alone or in conjunction with other parties) the subject matter claimed in the ’056 patent. Should Apple obtain such evidence, it will provide the name of the person(s) from whom and the circumstances under which the invention or any part of it was derived, and/or the circumstances surrounding the making of the invention before the patent application.

Apple reserves the right to supplement these disclosures based on further investigation and discovery.

VI. THE ’968 PATENT

A. Patent Rule 3-3(a): Identification of Prior Art

At this time, Apple contends that at least each of the prior art references described and charted in **Exhibits 968-A and 968-B** anticipates or renders obvious, either alone or in combination, one or more of the Asserted Claims of the ’968 patent.

Additional prior art that has not been charted, but is still relevant to the invalidity of the ’968 patent is listed in **Exhibit C**, including without limitation as evidence of the state of the art at the alleged time of invention. Apple reserves the right to amend these invalidity contentions to assert these references depending on the claim construction and infringement positions SEVEN may take as the case proceeds. Moreover, Apple reserves the right to use these references in combination with other references to render the claims of the ’968 patent obvious in the event SEVEN takes the position that certain claim limitations are missing from the references charted in **Exhibits 968-A and 968-B**.

B. Patent Rule 3-3(b): Whether Each Item Anticipates or Renders Obvious the Asserted Claims

SEVEN asserts claims 1-9, 11-14, 16-29, 31, 33, 35-38 of the ’968 patent against Apple in this lawsuit. These claims are invalid because the ’968 patent fails to meet one or more of the requirements for patentability. The individual bases for invalidity are provided below and in the claim charts attached as **Exhibits 968-A and 968-B.** Each of the foregoing listed prior art documents, the underlying work, and/or the underlying apparatus or method qualifies as prior art under one or more sections of 35 U.S.C. §§ 102 and/or 103.

Although Apple has identified at least one citation per limitation for each reference, each and every disclosure of the same limitation in the same reference is not necessarily identified. Rather, in an effort to focus the issues, Apple has cited representative portions of identified references, even where a reference may contain additional support for a particular claim element. In addition, persons of ordinary skill in the art generally read a prior art reference as a whole and in the context of other publications and literature. Thus, to understand and interpret any specific statement or disclosure within a prior art reference, such persons would rely on other information within the reference, along with other publications and their general scientific knowledge. Apple may rely upon uncited portions of the prior art references and on other publications and expert testimony to provide context, and as aids to understanding and interpreting the portions that are cited. Apple may also rely on uncited portions of the prior art references, other disclosed publications, and the testimony of experts to establish that a person of ordinary skill in the art would have been motivated to modify or combine certain of the cited references so as to render the claims obvious.

1. Priority

SEVEN's Patent Rule 3-1(e) disclosures provide that the Asserted Claims of the '968 patent are entitled to a priority date of January 8, 2002, which is the filing date of U.S. Provisional Application No. 60/346,881. SEVEN's Patent Rule 3-1(e) disclosures also provide that the Asserted Claims of the '968 patent claim the benefit of U.S. Provisional Application No. 60/403,249, filed August 12, 2002. SEVEN has provided no evidence to support its contention that the Asserted Claims of the '968 patent are entitled to claim priority back to these or any earlier filed application, and Apple therefore reserves the right to assert a later priority date based on any findings as to the priority date of the Asserted Claims by the Court, information learned through discovery, or otherwise

Apple reserves the right to challenge SEVEN's assertion that the '968 patent is entitled to claim the benefit of the filing dates of U.S. Provisional Application Nos. 60/346,881 and 60/403,249 to the extent that these provisional applications do not support the full scope of the Asserted Claims, for example, depending on scope of the Asserted Claims as properly construed. To the extent the provisional applications do not support the full scope of the Asserted Claims, the priority date of the '968 patent should be the filing date of the first non-provisional patent application to which the '968 patent claims priority, which is January 8, 2003. Additionally, to the extent the non-provisional patent applications to which the '968 patent claim priority do not support the full scope of the Asserted Claims, the priority date of the '968 patent should be the filing date of the patent application for the '968 patent, which is February 15, 2015.

The provisional application must "contain a written description of the invention and the manner and process of making and using it, in such full, clear, concise, and exact terms," 35 U.S.C. § 112, ¶ 1, to enable a POSITA to practice the invention claimed in the non-provisional application. *Id.*

a) The Asserted Claims of the ’968 patent cannot claim priority to the ’968 Provisionals or any patent application of which the ’968 Patent is a continuation

None of the Asserted Claims are entitled to the filing dates of U.S. Provisional Application Nos. 60/346,881 and/or 60/403,249 (“the ’968 Provisionals”) and/or the filing dates of U.S. Patent Application Nos. 10/339,368 and 11/470,802 (“the ’968 Continuing Applications”), because they do not have written description support in the ’968 Provisionals or in the ’968 Continuing Applications. *See Falko-Gunter Falkner v. Inglis*, 448 F.3d 1357 (Fed. Cir. 2006).

The Asserted Claims are not entitled to the ’968 Provisional or ’968 Continuing Application filing date(s) because neither the ’968 Provisionals nor the ’968 Continuing Applications actually or inherently disclose each and every claim element. *PowerOasis, Inc. v. T-Mobile USA, Inc.*, 522 F.3d 1299, 1306-07 (Fed. Cir. 2008).

Claims 1 and 20 recite features relating to receiving a first transaction from the first device ***in response to user input from the first device***—a feature found nowhere in the provisional applications or the continuing applications to which the ’968 patent claims priority. Nothing in the provisional applications or in the continuing applications shows the inventor possessed and enabled functionalities relating to receiving a first transaction from the first device ***in response to user input from the first device*** recited in Claims 1 and 20 (“receive a first transaction from the first device in response to user input at the first at the first device”), (“receiving a first transaction from the first device in response to user input at the first at the first device”).

Additionally, none of the Asserted Claims are disclosed in the ’968 Provisionals. The Asserted Claims use abstract terminology that does not exist in the ‘968 Provisionals. For example, the Asserted Claims recite the following terms: (1) “first device;” (2) “second device;”

(3) “third device;” (4) “first connection;” (5) “second connection;” (6) “third connection;” (7) “first transaction;” (8) “second transaction” and/or (9) “third transaction.”

SEVEN has failed to identify where these terms are found in the ’968 Provisionals. For example, SEVEN fails to explain in the ’968 Provisionals which devices referred to within them are the “first device” versus the “second device” or “third device,” which connections are the “first connection” versus the “second connection” or “third connection,” and which “transactions” are the first, second and/or third “transactions.” Apple sees no relevant disclosures of these terms and the distinctions between them in the ’968 Provisionals. The claims additionally define the relationship between these abstract terms, for example, requiring the authentication of the “first device” over the “first connection,” sending a “first transaction” where the “first connection” is maintained independently of the “first transaction,” and authenticating the “second device” over the “second connection,” and so on. Because Apple is not aware of how SEVEN maps the Asserted Claims to the ’968 Provisionals, Apple is unable to provide further rebuttal until SEVEN sets forth its theory with respect to each of limitation of the Asserted Claims.

Furthermore, the ’968 patent uses generic terminology that could refer to multiple different things within the ’968 Provisionals. For example, the claimed “processor” and “memory” could refer to components used in the Slingshot Connection Server, the chipset used in the User’s P.C., or the Slingshot Connection Client. Irrespective of which of these devices SEVEN maps to, however, the ’968 Provisionals do not disclose a “processor” or “memory” that satisfies the other steps of the claim.

For example, the ’968 Provisionals refer to the Slingshot system, but the Slingshot system does not support the claimed features. In some instances, such as with respect to the

limitations requiring the generation of a trigger for a second device based on the first transaction from the first device, wherein the trigger is pushed to the second device, or the limitation requiring that the trigger notify the second device of new data from the first transaction to be received by the second device from the server for display to a user, the disclosure concerning the Slingshot system does not provide the necessary level of detail to determine that this limitation is satisfied. In other instances, the disclosure of the Slingshot system teaches away from the claimed invention (*see, e.g.*, U.S. Provisional Application Nos. 60/346,881, SEVEN Slingshot Architecture Plan at p. 4-5 (referring to a single connection being used for multiple events, whereas the claim requires using different connections)). Elsewhere, the claims require "maintaining a connection," which the applicant stated during the file history was not HTML, presumably because HTML is a stateless protocol. Yet the '968 Provisionals disclose the use of HTML. *See, e.g.*, U.S. Provisional Application Nos. 60/346,881, System SEVEN Technical Overview at p. 10. Finally, as already discussed above, the Asserted Claims require "user input" at the first device, but the '968 Provisionals does not disclose the claimed "user input."

Consequently, neither the '968 Provisionals nor the '968 Continuing Applications actually or inherently disclose each and every element of the '968 patent claims. *Id.* The introduction of these features into the claims result in the '968 patent claims not being entitled to the filing date of the provisional applications or the continuing applications, and are, at most, entitled to the filing date of February 15, 2015—the filing date of the '968 application.

2. Anticipation

Some or all of the Asserted Claims of the '968 patent are invalid as anticipated under 35 U.S.C. § 102 in view of each of the prior art references identified above and in the claim charts included in **Exhibit 968-A**, which identify specific examples of where each limitation of the Asserted Claims is found in the prior art references. As explained above, the cited portions of

prior art references identified in the attached claim charts are exemplary only and representative of the content and teaching of the prior art references, and should be understood in the context of the reference as a whole and as they would be understood by a person of ordinary skill in the art.

Apple identifies the following references as anticipating one or more of the Asserted Claims of the '968 patent under 35 U.S.C. § 102. The below table of anticipating references is exemplary, and it does not constitute an admission that any reference anticipates only the listed claims. Further, Apple contends that any prior art reference in the attached charts that is charted for each limitation of any given claim, anticipates that claim, regardless of whether that prior art reference is listed in the following table.

Exhibit No.	Anticipating Prior Art	Claims
968-A01	Wireless Application Protocol ("WAP")	1, 3-9, 11-14, 16-19, 20, 22-29, 31, 33, 35-38
968-A02	U.S. Patent No. 6,138,158 to Boyle et al. ("Boyle")	1, 3-9, 11, 13-14, 16-19, 20, 22-29, 31, 33, 35-38
968-A03	U.S. Patent No. 8,326,940 to Yamamoto et al. ("Yamamoto")	1, 3-9, 11, 13-14, 16-19, 20, 22-29, 31, 33, 35-38
968-A04	U.S. Patent Application Publication No. 2002/0038371 to Spacey ("Spacey")	2-5, 9, 11, 16-19, 21-24, 29, 31, 35-38
968-A05	U.S. Patent No. 6,742,127 to Fox et al. ("Fox")	3-5, 6-8, 9-14, 16-19, 22, 24, 25-28, 29, 31, 33-38
968-A06	Blackberry RIM 857 System	1-9, 11-14, 16-19, 20-29, 31, 33, 35-38
968-A07	Microsoft Pocket PC System	1-9, 11-14, 16-19, 20-29, 31, 33, 35-38
968-A08	Nokia 6310 System	1-9, 11-14, 16-19, 20-29, 31, 33, 35-38
968-A09	U.S. Patent No. 9,077,673 ("Davies")	1-9, 11-14, 20-29, 31, 33
968-A10	U.S. Patent No. 7,805,489 ("Roberts")	2-7, 14, 16-19, 21-23, 33, 35-38

To the extent any item of prior art cited above is deemed not to disclose, explicitly or inherently, any limitation of an Asserted Claim of the '968 patent, Apple reserves the right to argue that any difference between that prior art and the corresponding patent claim would have been either inherent to the art, or obvious to a person of ordinary skill in the art, even if Apple

has not specifically denoted that the art is to be combined with the knowledge of a person of ordinary skill in the art.

3. Obviousness

To the extent any limitation is deemed not to be exactly met by an item of prior art listed above and in **Exhibit 968-A**, then any purported differences are such that the claimed subject matter as a whole would have been obvious to one skilled in the art at the time of the alleged invention, in view of the state of the art and knowledge of those skilled in the art. The item of prior art would, therefore, render the relevant claims invalid for obviousness under 35 U.S.C. § 103.

In addition, the references identified above render one or more Asserted Claims of the '968 patent obvious when the references are read in combination with each other, and/or when read in view of the state of the art and knowledge of those skilled in the art. Each and every reference identified is also relevant to the state of the art at the time of the alleged invention. Any of the references disclosed above may be combined with one another to render obvious (and therefore invalid) each of SEVEN's Asserted Claims. Apple may rely upon a subset of the above identified references or all of the references identified above, including all references in **Exhibits 968-A, 968-B, and C**, for purposes of obviousness depending on the Court's claim construction, positions taken by SEVEN during this litigation, and further investigation and discovery.

To the extent the foregoing references are found not to anticipate the Asserted Claims, the foregoing references render the Asserted Claims obvious either alone or in combination with one or more of the other references identified above pursuant to Patent Rule 3-3(a). It would have been obvious to a person of skill in the art at the time of the alleged invention of the

Asserted Claims of the ’968 patent to combine the various references cited herein so as to disclose the Asserted Claims of the ’968 patent.

In accordance with Patent Rule 3-3(b), prior art references rendering the Asserted Claims obvious, alone or in combination with other references, are outlined below and included in **Exhibits 968-A and 968-B,** which include exemplary claim charts for the Asserted Claims of the ’968 patent showing specifically where in each reference or combinations of references each Asserted Claim is found, and an explanation of why the prior art renders the Asserted Claim obvious. Where applicable, **Exhibits 968-A and 968-B** include the motivation to combine references.

Moreover, in addition to the information contained elsewhere in these contentions and in particular **Exhibit 968-B,** Apple has identified additional motivations and reasons to combine the various references cited herein. In particular, multiple teachings, suggestions, and/or reasons to modify any of the references and/or to combine any two or more of the references in **Exhibits 968-A and 968-B** come from many sources, including the prior art (specific and as a whole), common knowledge, common sense, predictability, expectations, industry trends, design incentives or need, market demand or pressure, market forces, obvious to try, the nature of the problem faced, and/or knowledge possessed by one of ordinary skill. In addition, it would have been obvious to try combining the prior art references identified above because there were only a finite number of predictable solutions and/or because known work in one field or endeavor prompted variations based on predictable design incentives and/or market forces either in the same field or a different one. The combination of prior art references identified in these contentions would have been obvious because the claimed combinations represent the known potential options with a reasonable expectation of success. Additionally, one of ordinary skill in

the art would have been motivated to create combinations identified in these contentions using: known methods to yield predictable results; known techniques in the same way; a simple substitution of one known, equivalent element for another to obtain predictable results; and/or teaching, suggestion, or motivation in the prior art generally. Also, market forces in the industry, and the desire to improve features and performance, would motivate the addition of features to systems as they become available, become less expensive, become more commonly used, provide better performance, reduce costs, size or weight, or predictably achieve other clearly desirable results.

While Apple reserves the right to rely on any combination of the references reflected in their charts or incorporated herein by reference, Apple provides the following exemplary and non-exhaustive references and/or combinations evidencing invalidity of the claims of the Asserted Patents. The combinations of prior art listed below render obvious the Asserted Claims under the proper construction of the claims and/or under Plaintiff's apparent interpretation of the claims as set forth by Plaintiff in their Complaint and Infringement Contentions. Each combination renders the identified claims obvious through the express and/or inherent disclosure in the combination of references themselves, as well as in view of the knowledge of a person of ordinary skill in the art.

Obviousness Combinations	**Claims**
U.S. Patent No. 6,138,158 ("Boyle") in view of one or more of U.S. Patent No. 8,326,940 ("Yamamoto"), U.S. Patent App. Pub. No. 2002/0038371 to Spacey ("Spacey"), U.S. Patent No. 6,742,127 to Fox et al. ("Fox"), U.S. Patent No. 6,473,609 ("Schwartz"), U.S. Patent No. 7,007,083 ("Chesley"), U.S. Patent No. 7,443,126 ("Gilmore"), U.S. Patent No. 7,509,379 ("Degraeve"), U.S. Patent App. Pub. No. 2002/0156921 to Dutta et al. ("Dutta"), RFC 793 - Transmission Control Protocol ("RFC 793"), Apache: The Definitive Guide 2nd Ed., ("Apache") U.S. Patent No. 7,392,254 ("Jenkins"), Wireless Application Protocol ("WAP"), HDTP Specification Ver. 1.1 ("HDTP Spec."),	Claims 1-9, 11-14, 16-29, 31, 33, 35-38

How to Set Up and Maintain a Website, 2nd Ed. by Lincoln D. Stein ("Stein")	
U.S. Patent No. 8,326,940 ("Yamamoto") in view of one or more of U.S. Patent No. 6,138,158 ("Boyle"), U.S. Patent App. Pub. No. 2002/0038371 to Spacey ("Spacey"), U.S. Patent No. 6,742,127 to Fox et al. ("Fox"), U.S. Patent No. 6,473,609 ("Schwartz"), U.S. Patent No. 7,007,083 ("Chesley"), U.S. Patent No. 7,443,126 ("Gilmore"), U.S. Patent No. 7,509,379 ("Degraeve"), U.S. Patent App. Pub. No. 2002/0156921 to Dutta et al. ("Dutta"), RFC 793 - Transmission Control Protocol ("RFC 793"), Apache: The Definitive Guide 2nd Ed., ("Apache") U.S. Patent No. 7,392,254 ("Jenkins"), Wireless Application Protocol ("WAP"), HDTP Specification Ver. 1.1 ("HDTP Spec."), How to Set Up and Maintain a Website, 2nd Ed. by Lincoln D. Stein ("Stein")	Claims 1-9, 11-14, 16-29, 31, 33, 35-38
U.S. Patent App. Pub. No. 2002/0038371 to Spacey ("Spacey") in view of one or more of U.S. Patent No. 6,138,158 ("Boyle") U.S. Patent No. 8,326,940 ("Yamamoto"), U.S. Patent No. 6,742,127 to Fox et al. ("Fox"), U.S. Patent No. 6,473,609 ("Schwartz"), U.S. Patent No. 7,007,083 ("Chesley"), U.S. Patent No. 7,443,126 ("Gilmore"), U.S. Patent No. 7,509,379 ("Degraeve"), U.S. Patent App. Pub. No. 2002/0156921 to Dutta et al. ("Dutta"), RFC 793 - Transmission Control Protocol ("RFC 793"), Apache: The Definitive Guide 2nd Ed., ("Apache") U.S. Patent No. 7,392,254 ("Jenkins"), Wireless Application Protocol ("WAP"), HDTP Specification Ver. 1.1 ("HDTP Spec."), How to Set Up and Maintain a Website, 2nd Ed. by Lincoln D. Stein ("Stein")	Claims 1-9, 11-14, 16-29, 31, 33, 35-38
U.S. Patent No. 6,742,127 to Fox et al. ("Fox") in view of one or more of U.S. Patent No. 6,138,158 ("Boyle"), U.S. Patent No. 8,326,940 ("Yamamoto"), U.S. Patent App. Pub. No. 2002/0038371 to Spacey ("Spacey"), U.S. Patent No. 6,473,609 ("Schwartz"), U.S. Patent No. 7,007,083 ("Chesley"), U.S. Patent No. 7,443,126 ("Gilmore"), U.S. Patent No. 7,509,379 ("Degraeve"), U.S. Patent App. Pub. No. 2002/0156921 to Dutta et al. ("Dutta"), RFC 793 - Transmission Control Protocol ("RFC 793"), Apache: The Definitive Guide 2nd Ed., ("Apache") U.S. Patent No. 7,392,254 ("Jenkins"), Wireless Application Protocol ("WAP"), HDTP Specification Ver. 1.1 ("HDTP Spec."), How to Set Up and Maintain a Website, 2nd Ed. by Lincoln D. Stein ("Stein")	Claims 1-9, 11-14, 16-29, 31, 33, 35-38
Wireless Application Protocol ("WAP") in view of one or more of U.S. Patent No. 6,138,158 ("Boyle"), U.S. Patent No. 8,326,940 ("Yamamoto"), U.S. Patent App. Pub. No. 2002/0038371 to Spacey ("Spacey"), U.S. Patent No. 6,742,127 to Fox et al. ("Fox"), U.S. Patent No. 6,473,609 ("Schwartz"), U.S. Patent No.	Claims 1-9, 11-14, 16-29, 31, 33, 35-38

7,007,083 (“Chesley”), U.S. Patent No. 7,443,126 (“Gilmore”), U.S. Patent No. 7,509,379 (“Degraeve”), U.S. Patent App. Pub. No. 2002/0156921 to Dutta et al. (“Dutta”), RFC 793 - Transmission Control Protocol (“RFC 793”), Apache: The Definitive Guide 2nd Ed., (“Apache”) U.S. Patent No. 7,392,254 (“Jenkins”), HDTP Specification Ver. 1.1 (“HDTP Spec.”), How to Set Up and Maintain a Website, 2nd Ed. by Lincoln D. Stein (“Stein”)	
U.S. Patent No. 9,077,673 (“Davies”) in view of one or more of U.S. Patent No. 7,805,489 (“Roberts”), U.S. Patent No. 6,138,158 (“Boyle”), U.S. Patent No. 8,326,940 (“Yamamoto”), U.S. Patent App. Pub. No. 2002/0038371 to Spacey (“Spacey”), U.S. Patent No. 6,742,127 to Fox et al. (“Fox”), U.S. Patent No. 6,473,609 (“Schwartz”), U.S. Patent No. 7,007,083 (“Chesley”), U.S. Patent No. 7,443,126 (“Gilmore”), U.S. Patent No. 7,509,379 (“Degraeve”), U.S. Patent App. Pub. No. 2002/0156921 to Dutta et al. (“Dutta”), RFC 793 - Transmission Control Protocol (“RFC 793”), Apache: The Definitive Guide 2nd Ed., (“Apache”) U.S. Patent No. 7,392,254 (“Jenkins”), Wireless Application Protocol (“WAP”), HDTP Specification Ver. 1.1 (“HDTP Spec.”), U.S. Patent App. Pub. No. 2012/0149342 (“Cohen”), U.S. Patent App. Pub. 2012/0150979 (“Monaco”), How to Set Up and Maintain a Website, 2nd Ed. by Lincoln D. Stein (“Stein”)	Claims 1-9, 11-14, 16-29, 31, 33, 35-38
U.S. Patent No. 7,805,489 (“Roberts”) in view of one or more of U.S. Patent No. 9,077,673 (“Davies”), U.S. Patent No. 6,138,158 (“Boyle”), U.S. Patent No. 8,326,940 (“Yamamoto”), U.S. Patent App. Pub. No. 2002/0038371 to Spacey (“Spacey”), U.S. Patent No. 6,742,127 to Fox et al. (“Fox”), U.S. Patent No. 6,473,609 (“Schwartz”), U.S. Patent No. 7,007,083 (“Chesley”), U.S. Patent No. 7,443,126 (“Gilmore”), U.S. Patent No. 7,509,379 (“Degraeve”), U.S. Patent App. Pub. No. 2002/0156921 to Dutta et al. (“Dutta”), RFC 793 - Transmission Control Protocol (“RFC 793”), Apache: The Definitive Guide 2nd Ed., (“Apache”), U.S. Patent App. Pub. 2012/0150979 (“Monaco”) U.S. Patent No. 7,392,254 (“Jenkins”), Wireless Application Protocol (“WAP”), HDTP Specification Ver. 1.1 (“HDTP Spec.”), U.S. Patent App. Pub. No. 2012/0149342 (“Cohen”), How to Set Up and Maintain a Website, 2nd Ed. by Lincoln D. Stein (“Stein”)	Claims 1-9, 11-14, 16-29, 31, 33, 35-38

In addition to the specific combinations of prior art and the specific combinations of groups of prior art disclosed above, Apple reserves the right to rely on any other combination of any prior art references disclosed herein. Apple further reserves the right to rely upon combinations disclosed within the prosecution history of the references cited herein. These

obviousness combinations reflect Apple's present understanding of the potential scope of the claims that SEVEN appears to be advocating and should not be seen as Apple's acquiescence to SEVEN's interpretation of the patent claims.

Apple also reserves the right to amend or supplement these contentions regarding anticipation or obviousness of the Asserted Claims, in view of further information from SEVEN, information discovered during discovery, or a claim construction ruling by the Court. SEVEN has not identified what elements or combinations it alleges were not known to one of ordinary skill in the art at the time. Therefore, for any claim limitation that SEVEN alleges is not disclosed in a particular prior art reference, Apple reserves the right to assert that any such limitation is either inherent in the disclosed reference or obvious to one of ordinary skill in the art at the time in light of the same, or that the limitation is disclosed in another of the references disclosed above and in combination would have rendered the Asserted Claim obvious.

C. Patent Rule 3-3(c): Charts Identifying Where Specifically in Each Alleged Item of Prior Art Each Asserted Claim Is Found

Pursuant to Patent Rule 3-3(c), charts identifying where specifically in each alleged item of prior art each limitation of each Asserted Claim is found, including for each limitation that Apple contends is governed by 35 U.S.C. § 112(6), the identity of the structure(s), act(s), or material(s) in each item of prior art that performs the claimed function, are attached in **Exhibits 968-A and 968-B.**

D. Patent Rule 3-3(d): Other Grounds for Invalidity

Apple identifies the following grounds for invalidity of the Asserted Claims of the '968 patent based on 35 U.S.C. §§ 101 and/or 112. Apple reserves the right to supplement these disclosures based on further investigation and discovery.

1. Invalidity Pursuant to 35 U.S.C. § 112

Apple further asserts that the Asserted Claims of the '968 patent are invalid under 35 U.S.C. § 112. The following are the grounds upon which Apple contends the Asserted Claims are invalid for failure to meet the requirements of 35 U.S.C. § 112, ¶ 1, ¶ 2, ¶ 4 and/or ¶ 6, based on Apple's investigation to date and currently-available information.

For each claim identified as invalid, any dependent claims of those invalid claims are also invalid under 35 U.S.C. § 112, ¶ 1, ¶ 2, ¶ 4, and/or ¶ 6. Apple reserves the right to supplement and amend these contentions based on further discovery and investigation including, in particular, the deposition of any of the named inventors of the Asserted Patent, the parties' claim construction positions, and further investigation of SEVEN's implied infringement positions.

a) Written Description and/or Enablement

At least in view of SEVEN's apparent construction of the claims in its Infringement Contentions, the Asserted Claims of the '968 patent are invalid because the specification as filed does not contain adequate written description of the claimed inventions sufficient to lead a person of ordinary skill in the art to understand that the named inventors had possession of the purported inventions as claimed as required by 35 U.S.C. § 112, ¶ 1. Likewise, the specification does not enable one of ordinary skill in the art to make or use the claimed inventions without undue experimentation. Based on Apple's present understanding of SEVEN's infringement contentions, Apple asserts that the Asserted Claims of the of the '968 patent are invalid for reciting at least the following claim terms/phrases/limitations:

Claims 1 and 20 of the '968 patent and their dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain an adequate written description and/or enabling disclosure of "receiv[ing] a first transaction from the first device in response to user input at the first device." To the extent the

claims require "user input at the first device," the full scope of the claimed subject matter is not described or enabled. The phrase "user input" is not used in the patent's specification, and the patent's disclosures do not describe or enable receiving a first transaction from the first device "in response to user input at the first device." Accordingly, the specification fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

Claim 1 of the '968 patent and its dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain adequate written descriptions and/or enabling disclosures of "a communication interface." To the extent the claims require "a communication interface," the full scope of the claimed subject matter is not described or enabled. The phrase "communication interface" is not used in the patent's specification, and the patent's disclosures do not describe or enable a server comprising "a communication interface." Rather, the patent's specification describes "[a] communication management system 16 *includes* at least one management server . . . ." '968 patent at 3:1-2; *see also id.* at Fig. 1; Fig. 2. Accordingly, the specification fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

Claims 1 and 20 of the '968 patent and their dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain adequate written descriptions and/or enabling disclosures of "authenticat[ing]" the first or second devices. To the extent the claims require "authenticat[ing]" the first and/or second devices, the full scope of the claimed subject matter is not described or enabled. The patent's

specification only describes authentication of a ***connection***. '968 patent at 3:37-39 ("[t]he personal client 40 initiates an outbound connection 25 which is then authenticated by the management server 28."); 4:29-30 ("the management server 28 authenticates mobile connections 23, 44, 45, and 46 initiated by the mobile device"). Accordingly, the specification fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

Claims 1 and 20 of the '968 patent and their dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain adequate written descriptions and/or enabling disclosures of "maintained independently." To the extent the claims require a connection to be "maintained independently," the full scope of the claimed subject matter is not described or enabled. The phrase "maintained independently" is not used in the patent's specification, and the patent's disclosures do not describe or enable a connection that is "maintained independently." Accordingly, the specification fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

Claims 1, 20, 11, and 31 of the '968 patent and any dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain adequate written descriptions and/or enabling disclosures of "generate" at trigger. To the extent the claims require a trigger to be "generate[d]," the full scope of the claimed subject matter is not described or enabled. The patent's disclosures do not describe or enable a trigger that is "generat[ed]" by the server of the claims. Accordingly, the specification fails to

reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

Claims 5 and 24 of the ’968 patent and any dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain adequate written descriptions and/or enabling disclosures of a server “receiving configuration information from the first device, wherein the configuration information comprises login data associated with a user of the first device.” To the extent the claims require the server to “receiv[e] configuration information from the first device, wherein the configuration information comprises login data associated with a user of the first device,” the full scope of the claimed subject matter is not described or enabled. The patent’s disclosures do not describe or enable a receipt by a server of configuration information from a first device, wherein the configuration information comprises login data associated with a user of the first device. Accordingly, the specification fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

Claims 16, 17, 18, 19, 35, 36, 37 and 38 of the ’968 patent are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain adequate written descriptions and/or enabling disclosures of a server “terminat[ing]” a first or second connection, or a server receiving a message from a first or second device wherein receipt of the message terminates a first or second connection. To the extent the claims require “terminat[ing]” a first or second connection, the full scope of the claimed subject matter is not described or enabled. The phrase “terminate” appears only once in the patent’s specification as

"[o]nce the connection 23 is terminated." '968 patent at 5:25-26. However, and the patent's disclosures do not describe or enable a server "terminat[ing]" a first or second connection, or a server receiving a message from a first or second device wherein receipt of the message terminates a first or second connection. Accordingly, the specification fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

Claims 7 and 17 of the '968 patent are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain adequate written descriptions and/or enabling disclosures of "maintain" a connection. To the extent the claims require a connection to be "maintain[ed]" the full scope of the claimed subject matter is not described or enabled. The term "maintain" is not used in the patent's specification, and the patent's disclosures do not describe or enable a connection that is "maintain[ed]." Accordingly, the specification fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

Claims 1 and 20 of the '968 patent and their dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain adequate written descriptions and/or enabling disclosures of "a server" at least to the extent that SEVEN contends this limitation is satisfied by Apple's products. Apple's accused products are not implemented using "a server." The feature that SEVEN identifies in its infringement contentions is not "a server." Thus, to the extent the claim is interpreted broadly enough to include features where there is not "a server," this limitation lacks support.

Claim 1 of the ’968 patent and its dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain adequate written descriptions and/or enabling disclosures of “a communication interface,” “a processor communicatively coupled to the communication interface,” and/or “a memory communicatively coupled to the processor, the memory containing instructions executable by the processor” at least to the extent that SEVEN contends this limitation is satisfied by Apple’s products. Apple’s accused products are not implemented using “a server” comprising “a communication interface,” “a processor,” or “a memory.” The feature that SEVEN identifies in its infringement contentions is not “a communication interface,” “a processor,” or “a memory.” Thus, to the extent the claim is interpreted broadly enough to include features where there is not “a communication interface,” “a processor,” or “a memory,” this limitation lacks support.

Claims 1 and 20 of the ’968 patent and their dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain adequate written descriptions and/or enabling disclosures of “authenticat[ing] a first device over the first connection” at least to the extent that SEVEN contends this limitation is satisfied by Apple’s products. In Apple’s accused products, authentication of the first device does not occur over the alleged first connection to the server that allegedly receives the alleged first connection from the first device. The feature that SEVEN identifies in its infringement contentions is not “authenticat[ing] a first device over the first connection.” Thus, to the extent the claim is interpreted broadly enough to include features where there is not an authentication of a first device over the first connection, this limitation lacks support.

Claims 1 and 20 of the ’968 patent and their dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not

contain adequate written descriptions and/or enabling disclosures of "authenticat[ing] the second device over the second connection" at least to the extent that SEVEN contends this limitation is satisfied by Apple's products. In Apple's accused products, authentication of the second device does not occur over the alleged second connection to the server that allegedly receives the alleged second connection from the second device. The feature that SEVEN identifies in its infringement contentions is not "authenticat[ing] the second device over the second connection." Thus, to the extent the claim is interpreted broadly enough to include features where there is not an authentication of the second device over the second connection, this limitation lacks support.

Claims 1 and 20 of the '968 patent and their dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain adequate written descriptions and/or enabling disclosures of "generat[ing] a trigger for a second device based on the first transaction from the first device [. . .] wherein the trigger is pushed to the second device" at least to the extent that SEVEN contends this limitation is satisfied by Apple's products. In Apple's accused products, neither the server that allegedly receives the alleged first connection, nor the server that allegedly receives the alleged second connection, generates a trigger for the second device or pushes the trigger to the second device. The feature that SEVEN identifies in its infringement contentions is not "generat[ing] a trigger for a second device based on the first transaction from the first device [. . .] wherein the trigger is pushed to the second device." Thus, to the extent the claim is interpreted broadly enough to include features where there is no generation of a trigger for a second device based on the first transaction from the first device wherein the trigger is pushed to the second device, this limitation lacks support.

Claims 1 and 20 of the '968 patent and their dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain adequate written descriptions and/or enabling disclosures of "wherein the trigger is pushed over a connection different from the second connection" at least to the extent that SEVEN contends this limitation is satisfied by Apple's products. Apple's accused products do not push a trigger over a "connection different from the second connection." The feature that SEVEN identifies in its infringement contentions is not a "connection different from the second connection." Thus, to the extent the claim is interpreted broadly enough to include features where the trigger is not pushed over a "connection different from the second connection," this limitation lacks support.

Claims 1 and 20 of the '968 patent and their dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain adequate written descriptions and/or enabling disclosures of "send[ing] a second transaction to the second device using the second connection" at least to the extent that SEVEN contends this limitation is satisfied by Apple's products. Apple's accused products do not send a second transaction to the second device using the alleged second connection which is different from the connection that the trigger is sent over. The feature that SEVEN identifies in its infringement contentions is not "send[ing] a second transaction to the second device using the second connection." Thus, to the extent the claim is interpreted broadly enough to include features where there is not a sending of a second transaction to the second device using the second connection, this limitation lacks support.

Claims 5 and 20 of the '968 patent are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain adequate written

descriptions and/or enabling disclosures of "receiv[ing] configuration information from the first device, wherein the configuration information comprises login data associated with a user of the first device " at least to the extent that SEVEN contends this limitation is satisfied by Apple's products. In Apple's accused products, the server that allegedly receives the alleged first connection from a first device does not receive configuration information from the first device "wherein the configuration information comprises login data associated with a user of the first device." The feature that SEVEN identifies in its infringement contentions is not a "receiv[ing] configuration information from the first device, wherein the configuration information comprises login data associated with a user of the first device." Thus, to the extent the claim is interpreted broadly enough to include features where there is not a receipt of configuration information comprising login data associated with a user of the first device, this limitation lacks support.

Claims 7 and 26 of the '968 patent are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain adequate written descriptions and/or enabling disclosures of "wherein the electronic messages comprise electronic mail (email) data" at least to the extent that SEVEN contends this limitation is satisfied by Apple's products. Apple's products as accused do not transmit in the alleged first transaction "electronic mail (email) data." The feature that SEVEN identifies in its infringement contentions is not "electronic mail (email) data." Thus, to the extent the claim is interpreted broadly enough to include features where no "electronic mail (email) data" is contained in the alleged first transaction, this limitation lacks support.

Claims 11 and 31 of the '968 patent are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain adequate written descriptions and/or enabling disclosures of "generate a third trigger for a third device based on

the first transaction" at least to the extent that SEVEN contends this limitation is satisfied by Apple's products. In Apple's accused products, neither the server that allegedly receives the alleged first connection, nor the server that allegedly receives the alleged second connection, generates a third trigger for a third device. The feature that SEVEN identifies in its infringement contentions is not "generate a third trigger for a third device based on the first transaction." Thus, to the extent the claim is interpreted broadly enough to include features where no third trigger is generated for a third device based on the first transaction by the server that allegedly receives the alleged first connection or by the server that allegedly receives the alleged second connection, this limitation lacks support.

Claims 9 and 29 of the '968 patent are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain adequate written descriptions and/or enabling disclosures of "the second connection is received in response to user input received at the second device" at least to the extent that SEVEN contends this limitation is satisfied by Apple's products. Apple's accused products do not receive the alleged second connection in response to user input received at the second device. The feature that SEVEN identifies in its infringement contentions is not a "the second connection is received in response to user input received at the second device." Thus, to the extent the claim is interpreted broadly enough to include features where no "second connection is received in response to user input received at the second device," this limitation lacks support.

Claims 17 and 36 of the '968 patent are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain adequate written descriptions and/or enabling disclosures of "receiv[ing] a message from the first device, wherein receipt of the message terminates the first connection" at least to the extent that SEVEN

contends this limitation is satisfied by Apple's products. Apple's accused products do not receive a message from the first device, wherein receipt of the message terminates the first connection. The feature that SEVEN identifies in its infringement contentions is not a "receiv[ing] a message from the first device, wherein receipt of the message terminates the first connection." Thus, to the extent the claim is interpreted broadly enough to include features where there is no "receiv[ing] a message from the first device, wherein receipt of the message terminates the first connection," this limitation lacks support.

Claims 19 and 38 of the '968 patent are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain adequate written descriptions and/or enabling disclosures of "receiv[ing] a message from the second device terminating the second connection" at least to the extent that SEVEN contends this limitation is satisfied by Apple's products. Apple's accused products do not receive a message from the second device terminating the second connection." The feature that SEVEN identifies in its infringement contentions is not "receiv[ing] a message from the second device terminating the second connection." Thus, to the extent the claim is interpreted broadly enough to include features where there is no "receiv[ing] a message from the second device terminating the second connection," this limitation lacks support.

b) Indefiniteness

At least in view of SEVEN's apparent construction of the claims in its Infringement Contentions, the Asserted Claims of the '968 patent are invalid because they fail to particularly point out and distinctly claim the subject matter which the applicant regards as his invention under 35 U.S.C. § 112, ¶¶ 2, 4, and/or 6. Based on Apple's present understanding of SEVEN's infringement contentions, Apple asserts that the Asserted Claims of the of the '968 patent are invalid for reciting at least the following claim terms/phrases/limitations:

- Claim 1 of the ’968 patent and its dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 2, ¶ 4, and/or ¶ 6 because the specification does not describe or otherwise inform one of ordinary skill about what constitutes “a communication interface.” Claim 1 requires a “server ***comprising***:” “a communication interface[.]” ’968 Patent at Claim 1 (emphasis added). However, the specification discloses that “[a]” communications management system 16 ***includes at least one management server*** 28 that manages the transactions between the mobile device 21 and the enterprise network 18.” ’968 Patent at 3:1-4 (emphasis added). *See also, id.* at Fig. 1. As such, one of ordinary skill would not understand the metes and bounds of the identified claims, rendering them indefinite under 35 U.S.C. § 112, ¶ 2. Therefore, the Asserted Claims, when read in light of the specification and the prosecution history, “fail to inform, with reasonable certainty, those skilled in the art about the scope of the invention.” *Nautilus, Inc. v. Biosig Instruments, Inc.*, 134 S. Ct. 2120, 2124 (2014).
- Claims 1, 20, 11 and 31 of the of the ’968 patent are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 2, ¶ 4, and/or ¶ 6 because neither the specification nor the claims describe or otherwise inform one of ordinary skill what constitutes the server of the claims “generat[ing]” a trigger as distinguished from the server merely sending through a trigger that it has received from the first device. As such, one of ordinary skill would not understand the metes and bounds of the identified claims, rendering them indefinite under 35 U.S.C. § 112, ¶ 2. Therefore, the Asserted Claims, when read in light of the specification and the

prosecution history, "fail to inform, with reasonable certainty, those skilled in the art about the scope of the invention." *Nautilus, Inc. v. Biosig Instruments, Inc.*, 134 S. Ct. 2120, 2124 (2014).

- Claims 11 and 31 of the of the '968 patent are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 2, ¶ 4, and/or ¶ 6 because neither the specification nor the claims describe or otherwise inform one of ordinary skill what constitutes a "third trigger" in the absence of any purported "second trigger" in the claims. As such, one of ordinary skill would not understand the metes and bounds of the identified claims, rendering them indefinite under 35 U.S.C. § 112, ¶ 2. Therefore, the Asserted Claims, when read in light of the specification and the prosecution history, "fail to inform, with reasonable certainty, those skilled in the art about the scope of the invention." *Nautilus, Inc. v. Biosig Instruments, Inc.*, 134 S. Ct. 2120, 2124 (2014).
- Claims 1, 20, 14 and 33 of the of the '968 patent and any of their dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 2, ¶ 4, and/or ¶ 6 because neither the specification nor the claims describe or explain how to distinguish or differentiate "wherein the second transaction contains the new data" in Claims 1 and 20, from "wherein the second transaction contains data from the first transaction" in Claims 14 and 33. A person of ordinary skill would understand a "second transaction contain[ing] the new data" to be the same as a "second transaction contain[ing] data from the first transaction" because the first transaction contains the new data. As such, one of ordinary skill would not understand the metes and bounds of the identified claims, rendering them

indefinite under 35 U.S.C. § 112, ¶ 2. Therefore, the Asserted Claims, when read in light of the specification and the prosecution history, "fail to inform, with reasonable certainty, those skilled in the art about the scope of the invention." *Nautilus, Inc. v. Biosig Instruments, Inc*., 134 S. Ct. 2120, 2124 (2014).

- Claims 20 and 27 of the of the '968 patent, and any of their dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 2, ¶ 4, and/or ¶ 6 because neither the specification nor the claims describe or explain how to distinguish or differentiate "wherein the trigger notifies the second device of new data . . . to be received by the second device from the server" in Claim element 20(d), from "wherein the trigger notifies the second device of new data to be received by the second device from the server" in Claim 27. As such, one of ordinary skill would not understand the metes and bounds of the identified claims, rendering them indefinite under 35 U.S.C. § 112, ¶ 2. Therefore, the Asserted Claims, when read in light of the specification and the prosecution history, "fail to inform, with reasonable certainty, those skilled in the art about the scope of the invention." *Nautilus, Inc. v. Biosig Instruments, Inc*., 134 S. Ct. 2120, 2124 (2014).
- Claims 1 and 20 of the of the '968 patent and their dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 2, ¶ 4, and/or ¶ 6 because neither the specification nor the claims describe or otherwise inform one of ordinary skill what constitutes a "receiving" a connection. As such, one of ordinary skill would not understand the metes and bounds of the identified claims, rendering them indefinite under 35 U.S.C. § 112, ¶ 2. Therefore, the Asserted

Claims, when read in light of the specification and the prosecution history, "fail to inform, with reasonable certainty, those skilled in the art about the scope of the invention." *Nautilus, Inc. v. Biosig Instruments, Inc*., 134 S. Ct. 2120, 2124 (2014).

- Claims 1, 20, 11 and 31 of the of the '968 patent and any of their dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 2, ¶ 4, and/or ¶ 6 because neither the specification nor the claims describe or otherwise inform one of ordinary skill what constitutes a "generat[ing]" a trigger. As such, one of ordinary skill would not understand the metes and bounds of the identified claims, rendering them indefinite under 35 U.S.C. § 112, ¶ 2. Therefore, the Asserted Claims, when read in light of the specification and the prosecution history, "fail to inform, with reasonable certainty, those skilled in the art about the scope of the invention." *Nautilus, Inc. v. Biosig Instruments, Inc*., 134 S. Ct. 2120, 2124 (2014).

2. Other Grounds for Invalidity

In addition to the preceding invalidity contentions, Apple further contends that each of the Asserted Claims of the '968 patent is drawn to subject matter that is not patentable under 35 U.S.C. § 101. The '968 patent Asserted Claims are invalid under 35 U.S.C. § 101 for failure to recite patent eligible subject matter. Specifically, all claims of the '968 patent are fatally abstract under the U.S. Supreme Court's decision in *Alice Corp. v. CLS Bank Int'l*, 134 S. Ct. 2345 (2014) and progeny. The ideas presented in the claims are generally directed to the concept of sending information from one place to another, via an intermediary. Under *Alice* Step 1, those ideas are abstract, as they relate to a fundamental long prevalent practice. *See Intellectual Ventures I LLC v. Symantec Corp*., 838 F.3d 1307, 1314 (Fed. Cir. 2016). Limiting the invention

to a particular technological environment, e.g. generic computer hardware, "do[es] not render an otherwise abstract concept any less abstract." *Intellectual Ventures I LLC v. Capital One Fin. Corp.*, 850 F.3d 1332, 1340 (Fed Cir. 2017). Furthermore, because the patent relates to transmission of information, it is likewise abstract, as "information is … an intangible." *Electric Power Group, LLC v. Alstom S.A.*, 830 F.3d 1350, 1353 (Fed. Cir. 2016). Furthermore, under *Alice* Step 2 the '968 patent does not contain any inventive concept. The '968 patent Asserted Claims employs well-known components or functionality, as shown in Apple's invalidity contentions involving anticipation and/or obviousness in this case, which is not enough to impart patent eligibility of an abstract idea. *See, e.g., Alice*, 134 S. Ct. at 2359 (holding that limitations describing "'well-understood, routine, conventional activit[ies]' previously known to the industry" were insufficient to supply an inventive concept (quoting *Mayo*, 132 S. Ct. at 1294)). Further detail regarding Apple's contentions that the Asserted Claims of the '968 patent do not qualify as patent-eligible subject matter are contained in **Exhibit 968-D**.

Apple reserves the right to assert that the asserted patents are invalid under 35 U.S.C. §102(f) and/or (g) in the event Apple obtains evidence that the named inventors of the '968 patent did not invent (either alone or in conjunction with other parties) the subject matter claimed in the '968 patent. Should Apple obtain such evidence, it will provide the name of the person(s) from whom and the circumstances under which the invention or any part of it was derived, and/or the circumstances surrounding the making of the invention before the patent application.

Apple reserves the right to supplement these disclosures based on further investigation and discovery.

VII. THE ’557 PATENT

A. Patent Rule 3-3(a): Identification of Prior Art

At this time, Apple contends that at least each of the prior art references described and charted in **Exhibits 557-A and 557-B** anticipates or renders obvious, either alone or in combination, one or more of the Asserted Claims of the ’557 patent.

Additional prior art that has not been charted, but is still relevant to the invalidity of the ’557 patent is listed in **Exhibit C**, including without limitation as evidence of the state of the art at the alleged time of invention. Apple reserves the right to amend these invalidity contentions to assert these references depending on the claim construction and infringement positions SEVEN may take as the case proceeds. Moreover, Apple reserves the right to use these references in combination with other references to render the claims of the ’557 patent obvious in the event SEVEN takes the position that certain claim limitations are missing from the references charted in **Exhibits 557-A and 557-B**.

B. Patent Rule 3-3(b): Whether Each Item Anticipates or Renders Obvious the Asserted Claims

SEVEN asserts claims 1-28 of the ’557 patent against Apple in this lawsuit. These claims are invalid because the ’557 patent fails to meet one or more of the requirements for patentability. The individual bases for invalidity are provided below and in the claim charts attached as **Exhibits 557-A and 557-B**. Each of the foregoing listed prior art documents, the underlying work, and/or the underlying apparatus or method qualifies as prior art under one or more sections of 35 U.S.C. §§ 102 and/or 103.

Although Apple has identified at least one citation per limitation for each reference, each and every disclosure of the same limitation in the same reference is not necessarily identified. Rather, in an effort to focus the issues, Apple has cited representative portions of identified

references, even where a reference may contain additional support for a particular claim element. In addition, persons of ordinary skill in the art generally read a prior art reference as a whole and in the context of other publications and literature. Thus, to understand and interpret any specific statement or disclosure within a prior art reference, such persons would rely on other information within the reference, along with other publications and their general scientific knowledge. Apple may rely upon uncited portions of the prior art references and on other publications and expert testimony to provide context, and as aids to understanding and interpreting the portions that are cited. Apple may also rely on uncited portions of the prior art references, other disclosed publications, and the testimony of experts to establish that a person of ordinary skill in the art would have been motivated to modify or combine certain of the cited references so as to render the claims obvious.

1. Priority

SEVEN's Patent Rule 3-1(e) disclosures provide that the Asserted Claims of the '557 patent are entitled to a priority date of November 1, 2006, which is the filing date of U.S. Provisional Application No. 60/863,931 ("the '931 provisional"). SEVEN has provided no evidence to support its contention that the Asserted Claims of the '557 patent are entitled to claim priority back to these or any earlier filed application, and Apple therefore reserves the right to assert a later priority date based on any findings as to the priority date of the Asserted Claims by the Court, information learned through discovery, or otherwise. To the extent the provisional application does not support the full scope of the Asserted Claims, the priority date of the '557 patent should be the filing date of U.S. Patent Application Ser. Nos. 13/929/066 and 13/929,376 to which the '557 patent incorporates by reference, which is October 30, 2007. Apple further contends that the incorporation by reference of these applications was improper and that the Asserted Claims of the '557 patent are entitled to the filing date of the '557 patent.

The provisional and non-provisional applications to which SEVEN claims priority must "contain a written description of the invention and the manner and process of making and using it, in such full, clear, concise, and exact terms," 35 U.S.C. § 112 ¶ 1, to enable a POSITA to practice the invention claimed in the non-provisional application. *Id.*

a) The Asserted Claims of the '550 Patent Cannot Claim Priority to the '931 Provisional

The Asserted Claims are not entitled to the filing date of the '931 Provisional because claims 1 and 14 and their dependents do not have written description support in the '931 Provisional. *See Falko-Gunter Falkner v. Inglis*, 448 F.3d 1357 (Fed. Cir. 2006).

Claims 1 and 14 and their dependents are not entitled to the '931 Provisional filing date because the '931 Provisional does not actually or inherently disclose each and every claim element. *PowerOasis, Inc. v. T-Mobile USA, Inc.*, 522 F.3d 1299, 1306-07 (Fed. Cir. 2008). By way of example, claims 1 and 14 and their dependents recite a user settings, including a "roaming rule," "connectivity rule," and "application profile," in addition to the transmission of application requests for certain types of applications occurring over WIFI networks and cellular networks at the same time—features found nowhere in the provisional application to which the '557 patent claims priority. Nothing in the provisional application shows the inventor possessed or enabled these claimed features.

2. Anticipation

Some or all of the Asserted Claims of the '557 patent are invalid as anticipated under 35 U.S.C. § 102 in view of each of the prior art references identified above and in the claim charts included in **Exhibit 557-A**, which identify specific examples of where each limitation of the Asserted Claims is found in the prior art references. As explained above, the cited portions of prior art references identified in the attached claim charts are exemplary only and representative

of the content and teaching of the prior art references, and should be understood in the context of the reference as a whole and as they would be understood by a person of ordinary skill in the art.

Apple identifies the following references as anticipating one or more of the Asserted Claims of the ’557 patent under 35 U.S.C. § 102. The below table of anticipating references is exemplary, and it does not constitute an admission that any reference anticipates only the listed claims. Further, Apple contends that any prior art reference in the attached charts that is charted for each limitation of any given claim, anticipates that claim, regardless of whether that prior art reference is listed in the following table.

Anticipating Prior Art	Claims
U.S. Patent No. 7,539,175 to White et al. (“White”)	1-5, 10, 12, 13, 14, 15, 16, 17, 18, 23-28
U.S. Patent No. 7,620,065 to Falardeau (“Falardeau”)	1-5, 8-10, 12, 13, 14, 15, 16, 17, 18, 20-23, 25, 26, 27, 28
Nokia 6136 UMA/GAN enabled mobile phone (“Nokia 6138”)	All Asserted Claims
Samsung T709 UMA/GAN enabled mobile phone (“Samsung T709”)	All Asserted Claims

To the extent any item of prior art cited above is deemed not to disclose, explicitly or inherently, any limitation of an Asserted Claim of the ’557 patent, Apple reserves the right to argue that any difference between that prior art and the corresponding patent claim would have been either inherent to the art, or obvious to a person of ordinary skill in the art, even if Apple has not specifically denoted that the art is to be combined with the knowledge of a person of ordinary skill in the art.

3. Obviousness

To the extent any limitation is deemed not to be exactly met by an item of prior art listed above and in **Exhibit 557-A**, then any purported differences are such that the claimed subject matter as a whole would have been obvious to one skilled in the art at the time of the alleged

invention, in view of the state of the art and knowledge of those skilled in the art. The item of prior art would, therefore, render the relevant claims invalid for obviousness under 35 U.S.C. § 103.

In addition, the references identified above render one or more Asserted Claims of the '557 patent obvious when the references are read in combination with each other, and/or when read in view of the state of the art and knowledge of those skilled in the art. Each and every reference identified is also relevant to the state of the art at the time of the alleged invention. Any of the references disclosed above may be combined with one another to render obvious (and therefore invalid) each of SEVEN's Asserted Claims. Apple may rely upon a subset of the above identified references or all of the references identified above, including all references in **Exhibits 557-A, 557-B, and C**, for purposes of obviousness depending on the Court's claim construction, positions taken by SEVEN during this litigation, and further investigation and discovery.

To the extent the foregoing references are found not to anticipate the Asserted Claims, the foregoing references render the Asserted Claims obvious either alone or in combination with one or more of the other references identified above pursuant to Patent Rule 3-3(a). It would have been obvious to a person of skill in the art at the time of the alleged invention of the Asserted Claims of the '557 patent to combine the various references cited herein so as to disclose the Asserted Claims of the '557 patent.

In accordance with Patent Rule 3-3(b), prior art references rendering the Asserted Claims obvious, alone or in combination with other references, are outlined below and included in **Exhibits 557-A and 557-B**, which include exemplary claim charts for the Asserted Claims of the '557 patent showing specifically where in each reference or combinations of references each

Asserted Claim is found, and an explanation of why the prior art renders the Asserted Claim obvious. Where applicable, **Exhibits 557-A and 557-B** include the motivation to combine references.

Moreover, in addition to the information contained elsewhere in these contentions and in particular **Exhibit 557-B**, Apple has identified additional motivations and reasons to combine the various references cited herein. In particular, multiple teachings, suggestions, and/or reasons to modify any of the references and/or to combine any two or more of the references in **Exhibits 557-A and 557-B** come from many sources, including the prior art (specific and as a whole), common knowledge, common sense, predictability, expectations, industry trends, design incentives or need, market demand or pressure, market forces, obvious to try, the nature of the problem faced, and/or knowledge possessed by one of ordinary skill. In addition, it would have been obvious to try combining the prior art references identified above because there were only a finite number of predictable solutions and/or because known work in one field or endeavor prompted variations based on predictable design incentives and/or market forces either in the same field or a different one. The combination of prior art references identified in these contentions would have been obvious because the claimed combinations represent the known potential options with a reasonable expectation of success. Additionally, one of ordinary skill in the art would have been motivated to create combinations identified in these contentions using: known methods to yield predictable results; known techniques in the same way; a simple substitution of one known, equivalent element for another to obtain predictable results; and/or teaching, suggestion, or motivation in the prior art generally. Also, market forces in the industry, and the desire to improve features and performance, would motivate the addition of features to systems as they become available, become less expensive, become more commonly used,

provide better performance, reduce costs, size or weight, or predictably achieve other clearly desirable results.

While Apple reserves the right to rely on any combination of the references reflected in their charts or incorporated herein by reference, Apple provides the following exemplary and non-exhaustive references and/or combinations evidencing invalidity of the claims of the Asserted Patents. The combinations of prior art listed below render obvious the Asserted Claims under the proper construction of the claims and/or under Plaintiff's apparent interpretation of the claims as set forth by Plaintiff in their Complaint and Infringement Contentions. Each combination renders the identified claims obvious through the express and/or inherent disclosure in the combination of references themselves, as well as in view of the knowledge of a person of ordinary skill in the art.

Obviousness Combinations	**Claims**
White in view of Falardeau	1-28
Falardeau in view of White and in further view of U.S. Patent No. 8,917,699 to Sachs et al. ("Sachs") Sachs	1-28
Falardeau in view of Sachs and in further view of Myhre	1-28
White in view of Sachs and in further view of Myhre	1-28
Nokia 6136 in view of Sachs	1-28
Nokia 6136 in view of Falardeau	1-28
Nokia 6136 in view of White	1-28
Samsung T709 in view of Sachs	1-28
Samsung T709 in view of Falardeau	1-28
Samsung T709 in view of White	1-28
White in view of U.S. Patent No. 7,843,900 to Gallagher et al. ("Gallagher") in further view of Myhre in further view of Falardeau	1-28
White in view of U.S. Patent No. 8,036,664 to Khetawat et al. ("Khetawat") in further view of Samsung T709 in further view of Falardeau	1-28
White in view of U.S. Patent No. 7,574,510 to Kalofonos et al. ("Kalofonos") in further view of Nokia 6136 in further view of Falardeau	1-28

White in view of U.S. Patent No. 7,656,835 to Joutsenvirta et al. (“Joutsenvirta”) in further view of Samsung T709 in further view of Falardeau	1-28
White in view of U.S. Patent No. 7,177,628 to Sommers et al. (“Sommers”) in further view of Myhre in further view of Falardeau	1-28
White in view of U.S. Patent Pub. No. 2004/0192312 to Li et al. (“Li”) in further view of Samsung T709 in further view of Falardeau	1-28
White in view of U.S. Patent No. 8,670,406 to Lee et al. (“Lee”) in further view of Samsung T709 in further view of Falardeau	1-28
White in view of U.S. Patent Pub. No. 2007/0191014 to Zheng et al. (“Zheng”) in further view of Sachs in further view of Falardeau	1-28
White in view of U.S. Patent Pub. No. 2008/0037473 to Brown et al. (“Brown”) in further view of Nokia 6136 in further view of Falardeau	1-28
White in view of U.S. Patent Pub. No. 2008/0096560 to Felske et al. (“Felske”) in further view of Samsung T709 in further view of Falardeau	1-28
White in view of U.S. Patent Pub. No. 2003/0083080 to Fournier et al. (“Fournier”) in further view of Sachs in further view of Falardeau	1-28
White in view of U.S. Patent No. 7,733,831 to Samuel et al. (“Samuel”) in further view of Sachs in further view of Falardeau	1-28
White in view of U.S. Patent No. 8,811,991 to Jain et al. (“Jain”) in further view of Samsung T709 in further view of Falardeau	1-28
White in view of U.S. Patent No. 7,613,171 to Zehavi et al. (“Zehavi”) in further view of Nokia 6136 in further view of Falardeau	1-28
White in view of U.S. Patent No. 7,983,711 to Juneja et al. (“Juneja”) in further view of Sachs in further view of Falardeau	1-28
White in view of U.S. Patent Pub. No. 2008/0043726 to Herrero-Veron et al. (“Herrero-Veron”) in further view of Sachs in further view of Falardeau	1-28

White in view of U.S. Patent No. 7,835,743 to Zhang et al. ("Zhang") in further view of Samsung T709 in further view of Falardeau	1-28
White in view of U.S. Patent Pub. No. 20014/0293986 to Drennan ("Drenna") in further view of Nokia 6136 in further view of Falardeau	1-28
White in view of U.S. Patent No. 7,409,219 to Levitan. ("Levitan") in further view of Nokia 6136 in further view of Falardeau	1-28
White in view of U.S. Patent No. 8,520,645 to Saarela ("Saarela") in further view of Samsung T709 in further view of Falardeau	1-28
White in view of U.S. Patent No. 8,888,047 to Konicek et al. ("Konicek") in further view of Sachs in further view of Falardeau	1-28
Samsung T709 in view of Konicek in further view of Zhang in further view of Falardeau	1-28
Samsung T709 in view of Konicek in further view of Zehavi in further view of White	1-28
Nokia 6136 in view of Konicek in further view of Zhang in further view of Falardeau	1-28
Nokia 6136 in view of Konicek in further view of Zehavi in further view of White	1-28

In addition to the specific combinations of prior art and the specific combinations of groups of prior art disclosed above, Apple reserves the right to rely on any other combination of any prior art references disclosed herein. Apple further reserves the right to rely upon combinations disclosed within the prosecution history of the references cited herein. These obviousness combinations reflect Apple's present understanding of the potential scope of the claims that SEVEN appears to be advocating and should not be seen as Apple's acquiescence to SEVEN's interpretation of the patent claims.

Apple also reserves the right to amend or supplement these contentions regarding anticipation or obviousness of the Asserted Claims, in view of further information from SEVEN, information discovered during discovery, or a claim construction ruling by the Court. SEVEN has not identified what elements or combinations it alleges were not known to one of ordinary

skill in the art at the time. Therefore, for any claim limitation that SEVEN alleges is not disclosed in a particular prior art reference, Apple reserves the right to assert that any such limitation is either inherent in the disclosed reference or obvious to one of ordinary skill in the art at the time in light of the same, or that the limitation is disclosed in another of the references disclosed above and in combination would have rendered the Asserted Claim obvious.

C. Patent Rule 3-3(c): Charts Identifying Where Specifically in Each Alleged Item of Prior Art Each Asserted Claim Is Found

Pursuant to Patent Rule 3-3(c), charts identifying where specifically in each alleged item of prior art each limitation of each Asserted Claim is found, including for each limitation that Apple contends is governed by 35 U.S.C. § 112(6), the identity of the structure(s), act(s), or material(s) in each item of prior art that performs the claimed function, are attached in **Exhibits 557-A and 557-B**.

D. Patent Rule 3-3(d): Other Grounds for Invalidity

Apple identifies the following grounds for invalidity of the Asserted Claims of the '557 patent based on 35 U.S.C. §§ 101 and/or 112. Apple reserves the right to supplement these disclosures based on further investigation and discovery.

1. Invalidity Pursuant to 35 U.S.C. § 112

Apple further asserts that the Asserted Claims of the '557 patent are invalid under 35 U.S.C. § 112. The following are the grounds upon which Apple contends the Asserted Claims are invalid for failure to meet the requirements of 35 U.S.C. § 112, ¶ 1, ¶ 2, ¶ 4 and/or ¶ 6, based on Apple's investigation to date and currently-available information.

For each claim identified as invalid, any dependent claims of those invalid claims are also invalid under 35 U.S.C. § 112, ¶ 1, ¶ 2, ¶ 4, and/or ¶ 6. Apple reserves the right to supplement and amend these contentions based on further discovery and investigation including, in

particular, the deposition of any of the named inventors of the Asserted Patent, the parties' claim construction positions, and further investigation of SEVEN's implied infringement positions.

a) Written Description and/or Enablement

At least in view of SEVEN's apparent construction of the claims in its Infringement Contentions, the Asserted Claims of the '557 patent are invalid because the specification as filed does not contain adequate written description of the claimed inventions sufficient to lead a person of ordinary skill in the art to understand that the named inventors had possession of the purported inventions as claimed as required by 35 U.S.C. § 112, ¶ 1. Likewise, the specification does not enable one of ordinary skill in the art to make or use the claimed inventions without undue experimentation. Based on Apple's present understanding of SEVEN's infringement contentions, Apple asserts that the Asserted Claims of the of the '557 patent are invalid for reciting at least the following claim terms/phrases/limitations:

- Claims 1 and 14 of the '557 patent and their dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain an adequate written description and/or enabling disclosure of "roaming rules." The phrase "roaming rule" is not used in the patent's specification, and the patent's disclosures do not otherwise describe or enable the "roaming rule" limitation. Accordingly, the specification fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.
- Claims 1 and 14 of the '557 patent and their dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the

specification as filed does not contain an adequate written description and/or enabling disclosure of "connectivity rules." The phrase "connectivity rule" is not used in the patent's specification, and the patent's disclosures do not otherwise describe or enable the "connectivity rule" limitation. Accordingly, the specification fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

- Claims 1 and 14 of the '557 patent and their dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain an adequate written description and/or enabling disclosure of "displaying an indication of availability." The phrase "displaying an indication of availability" is not used in the patent's specification, and the patent's disclosures do not otherwise describe or enable the "displaying an indication of availability" limitation. Moreover, the word "display" fails to appear outside of the claims. Accordingly, the specification fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.
- Claims 1 and 14 of the '557 patent and their dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain an adequate written description and/or enabling disclosure of "time responsiveness." The phrase "time responsiveness" is not used in the patent's specification, and the patent's disclosures do not

otherwise describe or enable the "time responsiveness" limitation. Moreover, the words "responsiveness" or "responsive" fail to appear outside of the claims. Accordingly, the specification fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

- Claims 1 and 14 of the '557 patent and their dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain an adequate written description and/or enabling disclosure of "application profile." The phrase "application profile" is not used in the patent's specification, and the patent's disclosures do not otherwise describe or enable the "application profile" limitation. Accordingly, the specification fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.
- Claims 1 and 14 of the '557 patent and their dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain an adequate written description and/or enabling disclosure of "evaluating user settings." The phrase "user settings" is not used in the patent's specification, and the patent's disclosures do not otherwise describe or enable the "evaluating user settings" limitation. Accordingly, the specification fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

- Claims 1 and 14 of the ’557 patent and their dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain an adequate written description and/or enabling disclosure of a “network interface operable to . . .” perform the claimed “displaying . . . ,” “detecting . . .,” “evaluating . . . ,” and/or “determining . . .” functions. The phrase “network interface” is not used in the patent’s specification, and the patent’s disclosures do not otherwise describe or enable a “network interface operable” to perform each of the functions the claimed network interface is required to be operable to perform. Accordingly, the specification fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.
- Claims 1 and 14 of the ’557 patent and their dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain an adequate written description and/or enabling disclosure of “wherein requests from another application executing on the mobile device continue to access data through the WIFI network” limitations. The phrases “continue to access data,” “another application,” and “mobile device” are not used in the patent’s specification, and the patent’s disclosures do not otherwise describe or enable the “wherein requests from another application executing on the mobile device continue to access data through the WIFI network” limitations. Accordingly, the specification fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the

invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

- Claims 2 and 15 of the ’557 patent are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain an adequate written description and/or enabling disclosure of “send[ing] requests to the cellular network on an application-by-application basis.” The phrase “application-by-application” is not used in the patent’s specification, and the patent’s disclosures do not otherwise describe or enable the sending requests to the cellular network on an “application-by-application basis” limitation. Accordingly, the specification fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.
- Claims 3 and 16 of the ’557 patent are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain an adequate written description and/or enabling disclosure of “evaluating a network preference.” The phrase “network preference” is not used in the patent’s specification, and the patent’s disclosures do not otherwise describe or enable the “evaluating a network preference” limitation. Accordingly, the specification fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.
- Claims 6 and 19 of the ’557 patent are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not

contain an adequate written description and/or enabling disclosure of each of the WIFI network and the cellular network "are operating in a respective TCP session" limitation. The phrase "TCP session" is not used in the patent's specification, and the patent's disclosures do not otherwise describe or enable the "TCP session" limitation. Accordingly, the specification fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

- Claims 13 and 27 of the '557 patent are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain an adequate written description and/or enabling disclosure of "requests from the another application executing on the mobile device are not sent to the cellular network" limitation. The phrases "another application" and "not sent to the cellular network" are not used in the patent's specification, and the patent's disclosures do not otherwise describe or enable the "requests from the another application executing on the mobile device are not sent to the cellular network" limitation. Accordingly, the specification fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

b) Indefiniteness

At least in view of SEVEN's apparent construction of the claims in its Infringement Contentions, the Asserted Claims of the '557 patent are invalid because they fail to particularly point out and distinctly claim the subject matter which the applicant regards as his invention

under 35 U.S.C. § 112, ¶¶ 2, 4, and/or 6. Based on Apple's present understanding of SEVEN's infringement contentions, Apple asserts that the Asserted Claims of the of the '557 patent are invalid for reciting at least the following claim terms/phrases/limitations:

- Claims 1 and 14 of the '557 patent and their dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 2, ¶ 4, and/or ¶ 6 because the specification does not describe or otherwise inform one of ordinary skill about what constitutes a "connectivity rule." The '557 patent does not describe or explain how to distinguish any "rule" from a "connectivity rule." As such, one of ordinary skill would not understand the metes and bounds of the identified claims, rendering them indefinite under 35 U.S.C. § 112, ¶ 2. Therefore, the Asserted Claims, when read in light of the specification and the prosecution history, "fail to inform, with reasonable certainty, those skilled in the art about the scope of the invention." *Nautilus, Inc. v. Biosig Instruments, Inc*., 134 S. Ct. 2120, 2124 (2014).
- Claims 1 and 14 of the '557 patent and their dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 2, ¶ 4, and/or ¶ 6 because the specification does not describe or otherwise inform one of ordinary skill about what constitutes a "roaming rule." The '557 patent does not describe or explain how to distinguish any "rule" from a "roaming rule." As such, one of ordinary skill would not understand the metes and bounds of the identified claims, rendering them indefinite under 35 U.S.C. § 112, ¶ 2. Therefore, the Asserted Claims, when read in light of the specification and the prosecution history, "fail to inform, with reasonable certainty, those skilled in the art about the scope of the

invention." *Nautilus, Inc. v. Biosig Instruments, Inc.*, 134 S. Ct. 2120, 2124 (2014).

2. Other Grounds for Invalidity

In addition to the preceding invalidity contentions, Apple further contends that each of the Asserted Claims of the '557 patent is drawn to subject matter that is not patentable under 35 U.S.C. § 101. The '557 patent Asserted Claims are invalid under 35 U.S.C. § 101 for failure to recite patent-eligible subject matter. Specifically, all claims of the '557 patent are fatally abstract under the U.S. Supreme Court's decision in *Alice Corp. v. CLS Bank Int'l*, 134 S. Ct. 2345 (2014) and progeny. The claims of the '557 patent as whole relate to collecting and analyzing information before choosing a WIFI or cellular network for completing a connection. At the most basic level, the claims of the '557 patent are directed to connection routing, which is a long prevalent human activity. Under *Alice* Step 1, those ideas are abstract, as they relate to a fundamental long prevalent practice. *See Intellectual Ventures I LLC v. Symantec Corp*., 838 F.3d 1307, 1314 (Fed. Cir. 2016). A claim is drawn to an abstract idea when "humans have always performed [the claimed] functions." *Content Extraction & Transmission LLC v. Wells Fargo Bank, NA*, 776 F.3d 1343, 1347 (Fed. Cir. 2014). Limiting the invention to a particular technological environment, e.g. generic computer hardware, "do[es] not render an otherwise abstract concept any less abstract." *Intellectual Ventures I LLC v. Capital One Fin. Corp*., 850 F.3d 1332, 1340 (Fed Cir. 2017). Furthermore, because the patent relates to transmission of information, it is likewise abstract, as "information is . . . an intangible." *Electric Power Group, LLC v. Alstom S.A.*, 830 F.3d 1350, 1353 (Fed. Cir. 2016). Furthermore, under *Alice* Step 2 the '557 patent does not contain any inventive concept. "It is well-settled that mere recitation of concrete, tangible components is insufficient to confer patent eligibility to an otherwise abstract idea" where those components simply perform their "well-understood, routine, conventional"

functions. *In re TLI Commc'ns LLC Patent Litig.,* 823 F.3d 607 (Fed. Cir. 2016). The '557 patent's Asserted Claims employ well-known components or functionality, as shown in Apple's invalidity contentions involving anticipation and/or obviousness in this case, which is not enough to impart patent eligibility of an abstract idea. *See, e.g., Alice*, 134 S. Ct. at 2359 (holding that limitations describing "'well-understood, routine, conventional activit[ies]' previously known to the industry" were insufficient to supply an inventive concept (quoting *Mayo*, 132 S. Ct. at 1294)). Further detail regarding Apple's contentions that the Asserted Claims of the '557 patent do not qualify as patent-eligible subject matter are contained in **Exhibit 557-D**.

Apple reserves the right to assert that the asserted patents are invalid under 35 U.S.C. §102(f) and/or (g) in the event Apple obtains evidence that the named inventors of the '557 patent did not invent (either alone or in conjunction with other parties) the subject matter claimed in the '557 patent. Should Apple obtain such evidence, it will provide the name of the person(s) from whom and the circumstances under which the invention or any part of it was derived, and/or the circumstances surrounding the making of the invention before the patent application.

Apple reserves the right to supplement these disclosures based on further investigation and discovery.

VIII. THE '476 PATENT

A. Patent Rule 3-3(a): Identification of Prior Art

At this time, Apple contends that at least each of the prior art references described and charted in **Exhibits 476-A and 476-B** anticipates or renders obvious, either alone or in combination, one or more of the Asserted Claims of the '476 patent.

Additional prior art that has not been charted, but is still relevant to the invalidity of the '476 patent is listed in **Exhibit C**, including without limitation as evidence of the state of the art at the alleged time of invention. Apple reserves the right to amend these invalidity contentions

to assert these references depending on the claim construction and infringement positions SEVEN may take as the case proceeds. Moreover, Apple reserves the right to use these references in combination with other references to render the claims of the '476 patent obvious in the event SEVEN takes the position that certain claim limitations are missing from the references charted in **Exhibits 476-A and 476-B.**

B. Patent Rule 3-3(b): Whether Each Item Anticipates or Renders Obvious the Asserted Claims

SEVEN asserts claims 1-44 of the '476 patent against Apple in this lawsuit. These claims are invalid because the '476 patent fails to meet one or more of the requirements for patentability. The individual bases for invalidity are provided below and in the claim charts attached as **Exhibits 476-A and 476-B**. Each of the foregoing listed prior art documents, the underlying work, and/or the underlying apparatus or method qualifies as prior art under one or more sections of 35 U.S.C. §§ 102 and/or 103.

Although Apple has identified at least one citation per limitation for each reference, each and every disclosure of the same limitation in the same reference is not necessarily identified. Rather, in an effort to focus the issues, Apple has cited representative portions of identified references, even where a reference may contain additional support for a particular claim element. In addition, persons of ordinary skill in the art generally read a prior art reference as a whole and in the context of other publications and literature. Thus, to understand and interpret any specific statement or disclosure within a prior art reference, such persons would rely on other information within the reference, along with other publications and their general scientific knowledge. Apple may rely upon uncited portions of the prior art references and on other publications and expert testimony to provide context, and as aids to understanding and interpreting the portions that are cited. Apple may also rely on uncited portions of the prior art references, other disclosed

publications, and the testimony of experts to establish that a person of ordinary skill in the art would have been motivated to modify or combine certain of the cited references so as to render the claims obvious.

1. Priority

SEVEN's Patent Rule 3-1(e) disclosures provide that the Asserted Claims of the '476 patent are entitled to a priority date of January 8, 2002, which is the filing date of U.S. Provisional Application No. 60/346,881. SEVEN has provided no evidence to support its contention that the Asserted Claims of the '476 patent are entitled to claim priority back to this or any earlier filed application, and Apple therefore reserves the right to assert a later priority date based on any findings as to the priority date of the Asserted Claims by the Court, information learned through discovery, or otherwise.

The '476 patent claims priority to two provisional applications: (1) Provisional Application No. 60/403,249 (the '249 application) filed on August 12, 2002 and (2) Provisional Application No. 60/346,881 (the '881 application) filed on January 8, 2002. Apple reserves the right to challenge SEVEN's assertion that the '476 patent is entitled to claim the benefit of either of these provisional applications' filing dates to the extent that the provisional applications do not support the full scope of the Asserted Claims, for example, depending on scope of the Asserted Claims as properly construed. To the extent the provisional applications do not support the full scope of the Asserted Claims, the priority date of the '476 patent should be the filing date of patent application No. 10/339,369 to which the '476 patent is a continuation, which is January 8, 2003.

None of the Asserted Claims are entitled to the filing date of either the '249 or the '881 applications because each and every claim does not have written description support from the provisional applications. *See Falko-Gunter Falkner v. Inglis*, 448 F.3d 1357 (Fed. Cir. 2006).

Each and every asserted claim is not entitled to either the ’249 or the ’881 application filing dates because those applications do not actually or inherently disclose each and every claim element. *PowerOasis, Inc. v. T-Mobile USA, Inc*., 522 F.3d 1299, 1306-07 (Fed. Cir. 2008).

For example, the claims recite the features relating to “issue a token for the first computer after authenticating the username and the password, wherein a first point-to-point security association is negotiated with the first computer and a second point-to-point security association is negotiated with a second computer,” “receive a transaction message from the second computer, the transaction message comprising control data and payload data, wherein the control data includes information that provides authentication of a source of the transaction and transaction routing information, wherein the information includes the token,” “transmit the control data to the intermediary server, wherein the control data includes a token associated with the intermediary server and the token provides transaction routing information,” “encrypt second data of a second data path using a second security association, wherein the second data path is distinct from the intermediary server,” “ transmit the payload data through the second data path,” and variations of those limitations. Nothing in the ’249 or the ’881 provisional applications shows that the inventors possessed and enabled functionalities relating to these limitations as recited in the Asserted Claims. The ’249 and ’881 provisional applications are merely user guides that do not disclose the limitations by which a token is used to dictate any routing information, for example. Additionally, the ’249 and ’881 provisional applications do not disclose the use of a second data path distinct from an intermediary server, or by which the payload data is transferred along that second data path, for example. The ’249 and ’881 provisional applications, which are merely user guides, are high level descriptions of a product and do not disclose these limitations or their variations.

Consequently the ’249 and ’881 provisional applications do not actually or inherently disclose each and every element of the ’476 patent claims and therefore the ’476 patent claims do not deserve either filing date of the provisional applications from which the ’476 patent claims priority.

2. Anticipation

Some or all of the Asserted Claims of the ’476 patent are invalid as anticipated under 35 U.S.C. § 102 in view of each of the prior art references identified above and in the claim charts included in **Exhibit 476-A**, which identify specific examples of where each limitation of the Asserted Claims is found in the prior art references. As explained above, the cited portions of prior art references identified in the attached claim charts are exemplary only and representative of the content and teaching of the prior art references, and should be understood in the context of the reference as a whole and as they would be understood by a person of ordinary skill in the art.

Apple identifies the following references as anticipating one or more of the Asserted Claims of the ’476 patent under 35 U.S.C. § 102. The below table of anticipating references is exemplary, and it does not constitute an admission that any reference anticipates only the listed claims. Further, Apple contends that any prior art reference in the attached charts that is charted for each limitation of any given claim, anticipates that claim, regardless of whether that prior art reference is listed in the following table.

Exhibit	Anticipating Prior Art	Claims
476-A01	U.S. Patent Appl. No. 2002/0178370 to Gurevich et al.	1, 2, 3, 4, 7, 8, 9, 10, 11, 12, 13, 14, 15, 17, 18, 19, 20, 21, 22, 23, 24, 25, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 38, 39, 40, 41, 42, 43, 44, 45
476-A02	U.S. Patent No. 7,747,856 to Favazza et al.	1, 2, 3, 4, 7, 8, 9, 10, 11, 12, 13, 14, 15, 17, 18, 19, 20, 21, 22, 23, 24, 25, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 38, 39, 40, 41, 42, 43, 44
476-A03	U.S. Patent No. 6,167,513 to Inoue et al.	1, 2, 4, 6, 7, 8, 9, 10, 11, 12, 13, 14, 17, 18, 19, 20, 21, 22, 23, 24, 27, 28, 29, 30, 31, 32, 33, 34, 36, 38, 39, 40, 41, 42, 43, 44

Exhibit	Anticipating Prior Art	Claims
476-A04	U.S. Patent No. 9,941,951 to Felsher et al.	1, 2, 3, 4, 9, 10, 11, 12, 13, 14, 15, 17, 22, 23, 24, 25, 27, 32, 33, 34, 35, 36, 41, 42, 43, 44
476-A05	U.S. Patent No. 7,814,208 to Stephenson et al.	1, 9, 10, 13, 17, 23, 26, 33, 40, 41
476-A06	The UGuard System	1, 2, 3, 4, 33, 34, 35, 36

To the extent any item of prior art cited above is deemed not to disclose, explicitly or inherently, any limitation of an Asserted Claim of the ’476 patent, Apple reserves the right to argue that any difference between that prior art and the corresponding patent claim would have been either inherent to the art, or obvious to a person of ordinary skill in the art, even if Apple has not specifically denoted that the art is to be combined with the knowledge of a person of ordinary skill in the art.

3. Obviousness

To the extent any limitation is deemed not to be exactly met by an item of prior art listed above and in **Exhibits 476-A**, then any purported differences are such that the claimed subject matter as a whole would have been obvious to one skilled in the art at the time of the alleged invention, in view of the state of the art and knowledge of those skilled in the art. The item of prior art would, therefore, render the relevant claims invalid for obviousness under 35 U.S.C. § 103.

In addition, the references identified above render one or more Asserted Claims of the ’476 patent obvious when the references are read in combination with each other, and/or when read in view of the state of the art and knowledge of those skilled in the art. Each and every reference identified is also relevant to the state of the art at the time of the alleged invention. Any of the references disclosed above may be combined with one another to render obvious (and therefore invalid) each of SEVEN’s Asserted Claims. Apple may rely upon a subset of the above identified references or all of the references identified above, including all references in

Exhibits 476-A, 476-B, and C, for purposes of obviousness depending on the Court's claim construction, positions taken by SEVEN during this litigation, and further investigation and discovery.

To the extent the foregoing references are found not to anticipate the Asserted Claims, the foregoing references render the Asserted Claims obvious either alone or in combination with one or more of the other references identified above pursuant to Patent Rule 3-3(a). It would have been obvious to a person of skill in the art at the time of the alleged invention of the Asserted Claims of the '476 patent to combine the various references cited herein so as to disclose the Asserted Claims of the '476 patent.

In accordance with Patent Rule 3-3(b), prior art references rendering the Asserted Claims obvious, alone or in combination with other references, are outlined below and included in **Exhibits 476-A and 476-B**, which include exemplary claim charts for the Asserted Claims of the '476 patent showing specifically where in each reference or combinations of references each Asserted Claim is found, and an explanation of why the prior art renders the Asserted Claim obvious. Where applicable, **Exhibits 476-A and 476-B** include the motivation to combine references.

Moreover, in addition to the information contained elsewhere in these contentions and in particular **Exhibit 476-B**, Apple has identified additional motivations and reasons to combine the various references cited herein. In particular, multiple teachings, suggestions, and/or reasons to modify any of the references and/or to combine any two or more of the references in **Exhibits 476-A and 476-B** come from many sources, including the prior art (specific and as a whole), common knowledge, common sense, predictability, expectations, industry trends, design incentives or need, market demand or pressure, market forces, obvious to try, the nature of the

problem faced, and/or knowledge possessed by one of ordinary skill. In addition, it would have been obvious to try combining the prior art references identified above because there were only a finite number of predictable solutions and/or because known work in one field or endeavor prompted variations based on predictable design incentives and/or market forces either in the same field or a different one. The combination of prior art references identified in these contentions would have been obvious because the claimed combinations represent the known potential options with a reasonable expectation of success. Additionally, one of ordinary skill in the art would have been motivated to create combinations identified in these contentions using: known methods to yield predictable results; known techniques in the same way; a simple substitution of one known, equivalent element for another to obtain predictable results; and/or teaching, suggestion, or motivation in the prior art generally. Also, market forces in the industry, and the desire to improve features and performance, would motivate the addition of features to systems as they become available, become less expensive, become more commonly used, provide better performance, reduce costs, size or weight, or predictably achieve other clearly desirable results.

While Apple reserves the right to rely on any combination of the references reflected in their charts or incorporated herein by reference, Apple provides the following exemplary and non-exhaustive references and/or combinations evidencing invalidity of the claims of the Asserted Patents. The combinations of prior art listed below render obvious the Asserted Claims under the proper construction of the claims and/or under Plaintiff's apparent interpretation of the claims as set forth by Plaintiff in their Complaint and Infringement Contentions. Each combination renders the identified claims obvious through the express and/or inherent disclosure

in the combination of references themselves, as well as in view of the knowledge of a person of ordinary skill in the art.

Obviousness Combinations	Claims
U.S. Patent App. No. 2002/0178370 ("Gurevich") in view of U.S. Patent No. 9,419,951 ("Felsher"), U.S. Patent No. 7,814,208 to Stephenson et al. ("Stephenson"), U.S. Patent No. 6,167,513 to Inoue ("Inoue"), The U-Guard System at https://web.archive.org/web/*/http://uguard.com (UGuard), U.S. Patent No. 7,747,856 ("Favazza"), Int. Pat. App. WO 97/45981 ("Johnston"), U.S. Patent No. 8,090,951 ("Erlingsson"), U.S. Patent App. No. 2002/0019932 ("Toh"), U.S. Patent No. 5,479,514 (Klonowski), and/or U.S. Patent No. 8,543,644 ("Gage")	All Asserted Claims
Gurevich in view of Felsher, and/or one or more of Johnston, Erlingsson, Toh, and/or Gage	All Asserted Claims
Gurevich in view of Stephenson, and/or one or more of Johnston, Erlingsson, Toh, and/or Gage	All Asserted Claims
Gurevich in view of Inoue, and/or one or more of Johnston, Erlingsson, Toh, and/or Gage	All Asserted Claims
Gurevich in view of U-Guard, and/or one or more of Johnston, Erlingsson, Toh, and/or Gage	All Asserted Claims
Gurevich in view of Favazza, and/or one or more of Johnston, Erlingsson, Toh, and/or Gage	All Asserted Claims
Gurevich in view of Klonowski, and/or one or more of Johnston, Erlingsson, Toh, and/or Gage	All Asserted Claims
Gurevich in view of Felsher, Stephenson, Inoue, U-Guard, Klonowski, and/or Favazza	All Asserted Claims
Felsher in view of Gurevich, and/or one or more of Johnston, Erlingsson, Toh, and/or Gage	All Asserted Claims
Felsher in view of Stephenson, and/or one or more of Johnston, Erlingsson, Toh, and/or Gage	All Asserted Claims
Felsher in view of Inoue, and/or one or more of Johnston, Erlingsson, Toh, and/or Gage	All Asserted Claims
Felsher in view of U-Guard, and/or one or more of Johnston, Erlingsson, Toh, and/or Gage	All Asserted Claims
Felsher in view of Favazza, and/or one or more of Johnston, Erlingsson, Toh, and/or Gage	All Asserted Claims
Felsher in view of Klonowski, and/or one or more of Johnston, Erlingsson, Toh, and/or Gage	All Asserted Claims
Felsher in view of Gurevich, Stephenson, Inoue, U-Guard, Klonowski, and/or Favazza	All Asserted Claims
Felsher in view of Gurevich, Stephenson, Inoue, U-Guard, Favazza, Johnston, Erlingsson, Toh, Klonowski, and/or Gage	All Asserted Claims
Stephenson in view of Felsher, and/or one or more of Johnston, Erlingsson, Toh, and/or Gage	All Asserted Claims

Obviousness Combinations	Claims
Stephenson in view of Gurevich, and/or one or more of Johnston, Erlingsson, Toh, and/or Gage	All Asserted Claims
Stephenson in view of Inoue, and/or one or more of Johnston, Erlingsson, Toh, and/or Gage	All Asserted Claims
Stephenson in view of U-Guard, and/or one or more of Johnston, Erlingsson, Toh, and/or Gage	All Asserted Claims
Stephenson in view of Favazza, and/or one or more of Johnston, Erlingsson, Toh, and/or Gage	All Asserted Claims
Stephenson in view of Klonowski, and/or one or more of Johnston, Erlingsson, Toh, and/or Gage	All Asserted Claims
Stephenson in view of Felsher, Gurevich, Inoue, U-Guard, Klonowski, and/or Favazza	All Asserted Claims
Stephenson in view of Felsher, Gurevich, Inoue, U-Guard, Favazza, Johnston, Erlingsson, Toh, Klonowski, and/or Gage	All Asserted Claims
Inoue in view of Gurevich, and/or one or more of Johnston, Erlingsson, Toh, and/or Gage	All Asserted Claims
Inoue in view of Stephenson, and/or one or more of Johnston, Erlingsson, Toh, and/or Gage	All Asserted Claims
Inoue in view of Felsher, and/or one or more of Johnston, Erlingsson, Toh, and/or Gage	All Asserted Claims
Inoue in view of U-Guard, and/or one or more of Johnston, Erlingsson, Toh, and/or Gage	All Asserted Claims
Inoue in view of Favazza, and/or one or more of Johnston, Erlingsson, Toh, and/or Gage	All Asserted Claims
Inoue in view of Klonowski, and/or one or more of Johnston, Erlingsson, Toh, and/or Gage	All Asserted Claims
Inoue in view of Gurevich, Stephenson, Felsher, U-Guard, Klonowski, and/or Favazza	All Asserted Claims
Inoue in view of Felsher, Stephenson, Gurevich, U-Guard, Favazza, Johnston, Erlingsson, Toh, Klonowski, and/or Gage	All Asserted Claims
Favazza in view of Felsher, and/or one or more of Johnston, Erlingsson, Toh, and/or Gage	All Asserted Claims
Favazza in view of Stephenson, and/or one or more of Johnston, Erlingsson, Toh, and/or Gage	All Asserted Claims
Favazza in view of Inoue, and/or one or more of Johnston, Erlingsson, Toh, and/or Gage	All Asserted Claims
Favazza in view of U-Guard, and/or one or more of Johnston, Erlingsson, Toh, and/or Gage	All Asserted Claims
Favazza in view of Gurevich, and/or one or more of Johnston, Erlingsson, Toh, and/or Gage	All Asserted Claims
Favazza in view of Klonowski, and/or one or more of Johnston, Erlingsson, Toh, and/or Gage	All Asserted Claims
Favazza in view of Felsher, Stephenson, Inoue, U-Guard, Klonowski, and/or Gurevich	All Asserted Claims

Obviousness Combinations	Claims
Favazza in view of Felsher, Stephenson, Inoue, U-Guard, Gurevich, Johnston, Erlingsson, Toh, Klonowski and/or Gage	All Asserted Claims
U-Guard in view of Gurevich, and/or one or more of Johnston, Erlingsson, Toh, and/or Gage	All Asserted Claims
U-Guard in view of Stephenson, and/or one or more of Johnston, Erlingsson, Toh, and/or Gage	All Asserted Claims
U-Guard in view of Inoue, and/or one or more of Johnston, Erlingsson, Toh, and/or Gage	All Asserted Claims
U-Guard in view of Felsher, and/or one or more of Johnston, Erlingsson, Toh, and/or Gage	All Asserted Claims
U-Guard in view of Favazza, and/or one or more of Johnston, Erlingsson, Toh, and/or Gage	All Asserted Claims
U-Guard in view of Klonowski, and/or one or more of Johnston, Erlingsson, Toh, and/or Gage	All Asserted Claims
U-Guard in view of Felsher, Gurevich, Stephenson, Inoue, Klonowski, and/or Favazza	All Asserted Claims
U-Guard in view of Felsher, Stephenson, Inoue, Gurevich, Favazza, Johnston, Erlingsson, Toh, Klonowski, and/or Gage	All Asserted Claims
Klonowski in view of Gurevich, and/or one or more of Johnston, Erlingsson, Toh, and/or Gage	All Asserted Claims
Klonowski in view of Stephenson, and/or one or more of Johnston, Erlingsson, Toh, and/or Gage	All Asserted Claims
Klonowski in view of Felsher, and/or one or more of Johnston, Erlingsson, Toh, and/or Gage	All Asserted Claims
Klonowski in view of U-Guard, and/or one or more of Johnston, Erlingsson, Toh, and/or Gage	All Asserted Claims
Klonowski in view of Favazza, and/or one or more of Johnston, Erlingsson, Toh, and/or Gage	All Asserted Claims
Klonowski in view of Inoue, and/or one or more of Johnston, Erlingsson, Toh, and/or Gage	All Asserted Claims
Klonowski in view of Gurevich, Stephenson, Felsher, U-Guard, Inoue, and/or Favazza	All Asserted Claims
Klonowski in view of Felsher, Stephenson, Gurevich, U-Guard, Favazza, Johnston, Erlingsson, Toh, Inoue, and/or Gage	All Asserted Claims

In addition to the specific combinations of prior art and the specific combinations of groups of prior art disclosed above, Apple reserves the right to rely on any other combination of any prior art references disclosed herein. Apple further reserves the right to rely upon combinations disclosed within the prosecution history of the references cited herein. These obviousness combinations reflect Apple's present understanding of the potential scope of the

claims that SEVEN appears to be advocating and should not be seen as Apple's acquiescence to SEVEN's interpretation of the patent claims.

Apple also reserves the right to amend or supplement these contentions regarding anticipation or obviousness of the Asserted Claims, in view of further information from SEVEN, information discovered during discovery, or a claim construction ruling by the Court. SEVEN has not identified what elements or combinations it alleges were not known to one of ordinary skill in the art at the time. Therefore, for any claim limitation that SEVEN alleges is not disclosed in a particular prior art reference, Apple reserves the right to assert that any such limitation is either inherent in the disclosed reference or obvious to one of ordinary skill in the art at the time in light of the same, or that the limitation is disclosed in another of the references disclosed above and in combination would have rendered the Asserted Claim obvious.

C. Patent Rule 3-3(c): Charts Identifying Where Specifically in Each Alleged Item of Prior Art Each Asserted Claim Is Found

Pursuant to Patent Rule 3-3(c), charts identifying where specifically in each alleged item of prior art each limitation of each Asserted Claim is found, including for each limitation that Apple contends is governed by 35 U.S.C. § 112(6), the identity of the structure(s), act(s), or material(s) in each item of prior art that performs the claimed function, are attached in **Exhibits 476-A and 476-B**.

D. Patent Rule 3-3(d): Other Grounds for Invalidity

Apple identifies the following grounds for invalidity of the Asserted Claims of the '476 patent based on 35 U.S.C. §§ 101 and/or 112. Apple reserves the right to supplement these disclosures based on further investigation and discovery.

1. Invalidity Pursuant to 35 U.S.C. § 112

Apple further asserts that the Asserted Claims of the '476 patent are invalid under 35 U.S.C. § 112. The following are the grounds upon which Apple contends the Asserted Claims are invalid for failure to meet the requirements of 35 U.S.C. § 112, ¶ 1, ¶ 2, ¶ 4 and/or ¶ 6, based on Apple's investigation to date and currently-available information.

For each claim identified as invalid, any dependent claims of those invalid claims are also invalid under 35 U.S.C. § 112, ¶ 1, ¶ 2, ¶ 4, and/or ¶ 6. Apple reserves the right to supplement and amend these contentions based on further discovery and investigation including, in particular, the deposition of any of the named inventors of the Asserted Patent, the parties' claim construction positions, and further investigation of SEVEN's implied infringement positions.

a) Written Description and/or Enablement

At least in view of SEVEN's apparent construction of the claims in its Infringement Contentions, the Asserted Claims of the '476 patent are invalid because the specification as filed does not contain adequate written description of the claimed inventions sufficient to lead a person of ordinary skill in the art to understand that the named inventors had possession of the purported inventions as claimed as required by 35 U.S.C. § 112, ¶ 1. Likewise, the specification does not enable one of ordinary skill in the art to make or use the claimed inventions without undue experimentation. Based on Apple's present understanding of SEVEN's infringement contentions, Apple asserts that the Asserted Claims of the of the '476 patent are invalid for reciting at least the following claim terms/phrases/limitations:

Claims 1 and 33 of the '476 patent and its dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain an adequate written description and/or enabling disclosure of "transmitting the payload data through the second data path." The phrase "transmitting the payload data through the

second data path" is not used in the patent's specification and the specification does not otherwise describe or enable the "transmitting the payload data through the second data path" limitation. Accordingly, the specification fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

Claims 1, 13, 23, and 33 of the '476 patent and their dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification does not contain an adequate written description and/or enabling disclosure of "intermediary server" as used in claims 1, 13, and 33 of the '476 patent or "server" as used in claim 23 of the '476 patent. To the extent the term "intermediary server" or "server" is construed to mean more than a specific set of computers acting as a single server as identified in the '476 patent specification, the full scope of the claimed subject matter is not described or enabled. Accordingly, the specification fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

b) Indefiniteness

At least in view of SEVEN's apparent construction of the claims in its Infringement Contentions, the Asserted Claims of the '476 patent are invalid because they fail to particularly point out and distinctly claim the subject matter which the applicant regards as his invention under 35 U.S.C. § 112, ¶¶ 2, 4, and/or 6. Based on Apple's present understanding of SEVEN's infringement contentions, Apple asserts that the Asserted Claims of the of the '476 patent are invalid for reciting at least the following claim terms/phrases/limitations:

- Claims 1, 13, 26, and 33 of the '476 patent and its dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 2, ¶ 4, and/or ¶ 6

because the specification does not describe or otherwise inform one of ordinary skill about what constitutes "an intermediary server" or "a server." The '476 patent does not describe or explain how to distinguish connectivity using an intermediary server as it is boundless. As such, one of ordinary skill would not understand the metes and bounds of the identified claims, rendering them indefinite under 35 U.S.C. § 112, ¶ 2. Therefore, the Asserted Claims, when read in light of the specification and the prosecution history, "fail to inform, with reasonable certainty, those skilled in the art about the scope of the invention." *Nautilus, Inc. v. Biosig Instruments, Inc.*, 134 S. Ct. 2120, 2124 (2014).

- Claims 1 and 33 of the '476 patent and its dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 2, ¶ 4, and/or ¶ 6 because "the specification does not describe or otherwise inform one of ordinary skill about what constitutes being "distinct from the intermediary server." The '476 patent does not describe or explain what it means to be distinct from an intermediary server. As such, one of ordinary skill would not understand the metes and bounds of the identified claims, rendering them indefinite under 35 U.S.C. § 112, ¶ 2. Therefore, the Asserted Claims, when read in light of the specification and the prosecution history, "fail to inform, with reasonable certainty, those skilled in the art about the scope of the invention." *Nautilus, Inc. v. Biosig Instruments, Inc.*, 134 S. Ct. 2120, 2124 (2014).

2. Other Grounds for Invalidity

In addition to the preceding invalidity contentions, Apple further contends that each of the Asserted Claims of the '476 patent is drawn to subject matter that is not patentable under 35 U.S.C. § 101. The '476 patent Asserted Claims are invalid under 35 U.S.C. § 101 for failure to

recite patent eligible subject matter. Specifically, all claims of the '476 patent are fatally abstract under the U.S. Supreme Court's decision in *Alice Corp. v. CLS Bank Int'l*, 134 S. Ct. 2345 (2014) and progeny. The ideas presented in the claims are generally directed to concepts of splitting a message in half, passing half a message through one path, and half a message through another path so that only the recipient can understand the full message. Under *Alice* Step 1, those ideas are abstract, as they relate to a fundamental long prevalent practice. *See Intellectual Ventures I LLC v. Symantec Corp.*, 838 F.3d 1307, 1314 (Fed. Cir. 2016). Limiting the invention to a particular technological environment, *e.g.*, generic computer hardware, "do[es] not render an otherwise abstract concept any less abstract." *Intellectual Ventures I LLC v. Capital One Fin. Corp.*, 850 F.3d 1332, 1340 (Fed Cir. 2017). Furthermore, because the patent relates to the secure transmission of information, it is likewise abstract, as "information is … an intangible." *Electric Power Group, LLC v. Alstom S.A.*, 830 F.3d 1350, 1353 (Fed. Cir. 2016). Furthermore, under *Alice* Step 2 the '476 patent does not contain any inventive concept. The '476 patent's Asserted Claims employ well-known components or functionality, as shown in Apple's invalidity contentions involving anticipation and/or obviousness in this case, which is not enough to impart patent eligibility of an abstract idea. *See, e.g., Alice*, 134 S. Ct. at 2359 (holding that limitations describing "'well-understood, routine, conventional activit[ies]' previously known to the industry" were insufficient to supply an inventive concept (*quoting Mayo*, 132 S. Ct. at 1294)). Further detail regarding Apple's contentions that the Asserted Claims of the '476 patent do not qualify as patent-eligible subject matter are contained in **Exhibit 476-D**.

Apple reserves the right to assert that the asserted patents are invalid under 35 U.S.C. §102(f) and/or (g) in the event Apple obtains evidence that the named inventors of the '476 patent did not invent (either alone or in conjunction with other parties) the subject matter claimed

in the ’476 patent. Should Apple obtain such evidence, it will provide the name of the person(s) from whom and the circumstances under which the invention or any part of it was derived, and/or the circumstances surrounding the making of the invention before the patent application.

Apple reserves the right to supplement these disclosures based on further investigation and discovery.

IX. THE ’986 PATENT

A. Patent Rule 3-3(a): Identification of Prior Art

At this time, Apple contends that at least each of the prior art references described and charted in **Exhibits 986-A and 986-B** anticipates or renders obvious, either alone or in combination, one or more of the Asserted Claims of the ’986 patent.

Additional prior art that has not been charted, but is still relevant to the invalidity of the ’986 patent is listed in **Exhibit C**, including without limitation as evidence of the state of the art at the alleged time of invention. Apple reserves the right to amend these invalidity contentions to assert these references depending on the claim construction and infringement positions SEVEN may take as the case proceeds. Moreover, Apple reserves the right to use these references in combination with other references to render the claims of the ’986 patent obvious in the event SEVEN takes the position that certain claim limitations are missing from the references charted in **Exhibits 986-A and 986-B**.

B. Patent Rule 3-3(b): Whether Each Item Anticipates or Renders Obvious the Asserted Claims

SEVEN asserts 1–29 of the ’986 patent against Apple in this lawsuit. These claims are invalid because the ’986 patent fails to meet one or more of the requirements for patentability. The individual bases for invalidity are provided below and in the claim charts attached as **Exhibits 986-A and 986-B**. Each of the foregoing listed prior art documents, the underlying

work, and/or the underlying apparatus or method qualifies as prior art under one or more sections of 35 U.S.C. §§ 102 and/or 103.

Although Apple has identified at least one citation per limitation for each reference, each and every disclosure of the same limitation in the same reference is not necessarily identified. Rather, in an effort to focus the issues, Apple has cited representative portions of identified references, even where a reference may contain additional support for a particular claim element. In addition, persons of ordinary skill in the art generally read a prior art reference as a whole and in the context of other publications and literature. Thus, to understand and interpret any specific statement or disclosure within a prior art reference, such persons would rely on other information within the reference, along with other publications and their general scientific knowledge. Apple may rely upon uncited portions of the prior art references and on other publications and expert testimony to provide context, and as aids to understanding and interpreting the portions that are cited. Apple may also rely on uncited portions of the prior art references, other disclosed publications, and the testimony of experts to establish that a person of ordinary skill in the art would have been motivated to modify or combine certain of the cited references so as to render the claims obvious.

1. Priority

SEVEN's Patent Rule 3-1(e) disclosures provide that the Asserted Claims of the '986 patent are entitled to a priority date of Jan. 11, 2008, which is the filing date of U.S. Provisional Application No. 12/008,710. SEVEN has provided no evidence to support its contention that the Asserted Claims of the '986 patent are entitled to claim priority back to this or any earlier filed application, and Apple therefore reserves the right to assert a later priority date based on any findings as to the priority date of the Asserted Claims by the Court, information learned through discovery, or otherwise.

The ’986 patent claims priority to a provisional application filed on January 11, 2008. Apple reserves the right to challenge SEVEN’s assertion that the ’986 patent is entitled to claim the benefit of that provisional application’s filing date to the extent that the provisional application does not support the full scope of the Asserted Claims, for example, depending on scope of the Asserted Claims as properly construed. To the extent the provisional application does not support the full scope of the Asserted Claims, the priority date of the ’986 patent should be the filing date of the patent application of which the ’914 patent is a continuation, which is March 22, 2012.

a) The Asserted Claims of the ’986 Patent Cannot Claim Priority to the ’641 Provisional

None of the Asserted Claims are entitled to the filing date of U.S. Provisional No. 2009/0181641 (“the ’641 Provisional”) because claims 1 do not have written description support in the ’641 Provisional. *See Falko-Gunter Falkner v. Inglis*, 448 F.3d 1357 (Fed. Cir. 2006).

Claims 1, 12, and 23 are not entitled to the ’641 Provisional filing date because the ’641 Provisional does not actually or inherently disclose each and every claim element. *PowerOasis, Inc. v. T-Mobile USA, Inc.*, 522 F.3d 1299, 1306-07 (Fed. Cir. 2008).

Claims 1, 12, and 23 recite features relating to authentication of two or more associated devices—features found nowhere in the Provisional to which the ’986 patent claims priority. Nothing in the Provisional shows that the inventor possessed and enabled functionalities relating to authenticating multiple devices associated with a user that are capable of sharing and transmitting representations of content, as recited in claims 1, 12, 23 (“transmitting a representation of the accessed content to an application at a second device associated with the user, wherein the second device is authenticated over a mobile network”), (“receiving the accessed content in response to a selection at the second device, wherein the selection identifies

accessed content at the first device to be transmitted"), ("transmitting a representation of the content to an application at a second device that is communicatively coupled to the first device and is associated with the user, wherein the second device is authenticated over a mobile network").

Importantly, while the '641 Provisional does make references to a "unique authentication token," it does not provide any description of how a system might operate to accommodate multiple devices and multiple forms of authentication, including over the mobile network, or authentication between devices. The '641 Provisional never mentions authenticating multiple devices or how a server might understand two more devices to be associated based on multiple authentication tokens as recited in the '986 patent claims. In terms of authenticating multiple devices, the '641 Provisional never discusses the use of more than one authentication token, and never discusses using two forms of authentication associate devices before content is transferred or shared. Further, as to claims 1, 12, and 23, the '641 Provisional fails to disclose "wherein the application at the first device and the application at the second device are branded by a same entity," and "wherein the same entity is other than a provider that operates the mobile network." Consequently, the '641 Provisional does not actually or inherently disclose each and every element of the '986 patent claims. The introduction of these features into the claims resulted in the '986 patent claims not being entitled to the filing date of the Provisional, and are, at most, entitled to the filing date of March 22, 2012—the filing date of the '986 patent.

2. Anticipation

Some or all of the Asserted Claims of the '986 patent are invalid as anticipated under 35 U.S.C. § 102 in view of each of the prior art references identified above and in the claim charts included in **Exhibit 986-A**, which identify specific examples of where each limitation of the Asserted Claims is found in the prior art references. As explained above, the cited portions of

prior art references identified in the attached claim charts are exemplary only and representative of the content and teaching of the prior art references, and should be understood in the context of the reference as a whole and as they would be understood by a person of ordinary skill in the art.

Apple identifies the following references as anticipating one or more of the Asserted Claims of the '986 patent under 35 U.S.C. § 102. The below table of anticipating references is exemplary, and it does not constitute an admission that any reference anticipates only the listed claims. Further, Apple contends that any prior art reference in the attached charts that is charted for each limitation of any given claim, anticipates that claim, regardless of whether that prior art reference is listed in the following table.

Ex. No.	Anticipating Prior Art	Claims
Ex. 986-A1	U.S. Patent 8,001,612 to James Wieder ("Wieder")	All Asserted Claims except 6 and 17
Ex. 986-A2	U.S. Patent No. 7,792,756 to Plastina et al. ("Plastina")	All Asserted Claims except 6 and 17
Ex. 986-A3	U.S. Patent No. 8,028,323 to Martin Weel ("Weel")	All Asserted Claims except 10 and 21
Ex. 986-A4	U.S. Patent Application No. 2006/0190413 to Gregory W. Harper ("Harper")	All Asserted Claims except 4, 10, 15, 21
Ex. 986-A5	Microsoft Zune	All Asserted Claims
Ex. 986-A6	iTunes 4.0	All Asserted Claims
Ex. 986-A7	U.S. patent No. 8,880,714 to Todd Collart ("Collart")	All Asserted Claims except 6, 7, 9, 17, 18, and 20
Ex. 986-A8	U.S. Patent Application No. 2002/0068558 A1 to Craig Janik ("Janik")	All Asserted Claims except 4, 9, 10, 11, 15, 19, 21, and 22

To the extent any item of prior art cited above is deemed not to disclose, explicitly or inherently, any limitation of an Asserted Claim of the '986 patent, Apple reserves the right to argue that any difference between that prior art and the corresponding patent claim would have been either inherent to the art, or obvious to a person of ordinary skill in the art, even if Apple

has not specifically denoted that the art is to be combined with the knowledge of a person of ordinary skill in the art.

3. Obviousness

To the extent any limitation is deemed not to be exactly met by an item of prior art listed above and in **Exhibit 986-A**, then any purported differences are such that the claimed subject matter as a whole would have been obvious to one skilled in the art at the time of the alleged invention, in view of the state of the art and knowledge of those skilled in the art. The item of prior art would, therefore, render the relevant claims invalid for obviousness under 35 U.S.C. § 103.

In addition, the references identified above render one or more Asserted Claims of the '986 patent obvious when the references are read in combination with each other, and/or when read in view of the state of the art and knowledge of those skilled in the art. Each and every reference identified is also relevant to the state of the art at the time of the alleged invention. Any of the references disclosed above may be combined with one another to render obvious (and therefore invalid) each of SEVEN's Asserted Claims. Apple may rely upon a subset of the above identified references or all of the references identified above, including all references in **Exhibits 986-A, 986-B, and C** for purposes of obviousness depending on the Court's claim construction, positions taken by SEVEN during this litigation, and further investigation and discovery.

To the extent the foregoing references are found not to anticipate the Asserted Claims, the foregoing references render the Asserted Claims obvious either alone or in combination with one or more of the other references identified above pursuant to Patent Rule 3-3(a). It would have been obvious to a person of skill in the art at the time of the alleged invention of the

Asserted Claims of the ’986 patent to combine the various references cited herein so as to disclose the Asserted Claims of the ’986 patent.

In accordance with Patent Rule 3-3(b), prior art references rendering the Asserted Claims obvious, alone or in combination with other references, are outlined below and included in **Exhibits 986-A and 986-B**, which include exemplary claim charts for the Asserted Claims of the ’986 patent showing specifically where in each reference or combinations of references each Asserted Claim is found, and an explanation of why the prior art renders the Asserted Claim obvious. Where applicable, **Exhibits 986-A and 986-B** include the motivation to combine references.

Moreover, in addition to the information contained elsewhere in these contentions and in particular **Exhibit 986-B**, Apple has identified additional motivations and reasons to combine the various references cited herein. In particular, multiple teachings, suggestions, and/or reasons to modify any of the references and/or to combine any two or more of the references in **Exhibits 986-A and 986-B** come from many sources, including the prior art (specific and as a whole), common knowledge, common sense, predictability, expectations, industry trends, design incentives or need, market demand or pressure, market forces, obvious to try, the nature of the problem faced, and/or knowledge possessed by one of ordinary skill. In addition, it would have been obvious to try combining the prior art references identified above because there were only a finite number of predictable solutions and/or because known work in one field or endeavor prompted variations based on predictable design incentives and/or market forces either in the same field or a different one. The combination of prior art references identified in these contentions would have been obvious because the claimed combinations represent the known potential options with a reasonable expectation of success. Additionally, one of ordinary skill in

the art would have been motivated to create combinations identified in these contentions using: known methods to yield predictable results; known techniques in the same way; a simple substitution of one known, equivalent element for another to obtain predictable results; and/or teaching, suggestion, or motivation in the prior art generally. Also, market forces in the industry, and the desire to improve features and performance, would motivate the addition of features to systems as they become available, become less expensive, become more commonly used, provide better performance, reduce costs, size or weight, or predictably achieve other clearly desirable results.

While Apple reserves the right to rely on any combination of the references reflected in their charts or incorporated herein by reference, Apple provides the following exemplary and non-exhaustive references and/or combinations evidencing invalidity of the claims of the Asserted Patents. The combinations of prior art listed below render obvious the Asserted Claims under the proper construction of the claims and/or under Plaintiff's apparent interpretation of the claims as set forth by Plaintiff in their Complaint and Infringement Contentions. Each combination renders the identified claims obvious through the express and/or inherent disclosure in the combination of references themselves, as well as in view of the knowledge of a person of ordinary skill in the art.

Obviousness Combinations	**Claims**
Wieder in view of one or more of US 8,880,714 B2 to Todd Collart et al., ("Collart") and/or Sprint's Open Application Developer Program Press Release (Dec. 12, 2007) ("Sprint")	Claims 1-29
Plastina in view of one or more of Collart, Varshavsky, Scannell, et al., "Amigo: Proximity-Based Authentication of Mobile Devices," UbiComp 2007, LNCS 4717, pp. 253–270, 2007 ("Amigo"), and/or Sprint	Claims 1-29
Plastina in view of one or more of Wieder, Amigo, and/or Sprint	Claims 1-29
Plastina in view of one or more of Harper, Collart, Amigo, and/or Sprint	Claims 1-29
Weel in view of one or more of Weider, and/or Sprint	Claims 1-29

Obviousness Combinations	Claims
Weel in view of one or more of Wieder, Amigo, and/or Sprint	Claims 1-29
Weel in view of one or more of Collart, Amigo, and/or Sprint	Claims 1-29
Weel in view of one or more of Plastina, Collart, Amigo, and/or Sprint	Claims 1-29
US Patent Application No. 2006/0190413 to Gregory Harper ("Harper") in view of one or more of Collart, and/or Sprint	Claims 1-29
Harper in view of one or more of Wieder, Amigo, and/or Sprint	Claims 1-29
Harper in view of one or more of Collart, Wieder, Amigo, and/or Sprint	Claims 1-29
Harper in view of one or more of Janik, Wieder, Collart, Amigo, and/or Sprint	Claims 1-29
Harper in view of one or more of Plastina, Wieder, Collart, U.S. 2002/0068558 A1 to Craig Janik ("Janik"), Amigo, and/or Sprint	Claims 1-19
Janik in view of one or more of Collart, Varshavsky, Scannell, et al., "Amigo: Proximity-Based Authentication of Mobile Devices," UbiComp 2007, LNCS 4717, pp. 253–270, 2007 ("Amigo"), and/or Sprint	Claims 1-29
Janik in view of one or more of Wieder, Amigo, and/or Sprint	Claims 1-29
Janik in view of one or more of Wieder, Collart, Amigo, and/or Sprint	Claims 1-29
Janik in view of one or more of Harper, Wieder, Collart, Amigo, and/or Sprint	Claims 1-29
Janik in view of one or more of Plastina, Harper, Wieder, Collart, Amigo, and/or Sprint	
The Microsoft Zune System in view of one or more of Collart, Amigo, and/or Sprint	Claims 1-29
The Microsoft Zune System in view of one or more of Wieder, Amigo, and/or Sprint	Claims 1-29
The Microsoft Zune System in view of one or more of Plastina, Collart, Wieder, Amigo, and/or Sprint	Claims 1-29
The Microsoft Zune System in view of one or more of Harper, Wieder, Collart, Amigo, and/or Sprint	Claims 1-29
The Microsoft Zune System in view of one or more of Janik, Collart, Wieder, Plastina, Amigo, and/or Sprint	Claims 1-29
The iTunes 4.0 System ("iTunes 4.0") in view of one or more of Collart and Amigo	Claims 1-29
iTunes 4.0 in view of one or more of Collart, Amigo, and/or Sprint	Claims 1-29
iTunes 4.0 in view of one or more of Wieder, Amigo, and/or Sprint	Claims 1-29
iTunes 4.0 in view of one or more of Plastina, Collart, Wieder, Amigo, and/or Sprint	Claims 1-29
iTunes 4.0 in view of one or more of Harper, Wieder, Collart, Amigo, and/or Sprint	Claims 1-29
iTunes 4.0 in view of one or more of Janik, Collart, Wieder, Plastina, Amigo, and/or Sprint	Claims 1-29

Obviousness Combinations	Claims
Wieder in view of one or more of Collart, Plastina, Harper, Janik, the Microsoft Zune System, Amigo, Sprint, U.S. Patent No. 8,171,531 to Buer ("Buer"), U.S. Patent No. 7,487,537 to Giles et al. ("Giles"), U.S. 7,660, 420 B1 to Anand Narayan et al. ("Narayan"), and/or U.K. Patent Pub. No. 2,434,724 to Lin ("Line")	Claims 1-29
Plastina in view of one or more of Wieder, Collart, Harper, Janik, the Microsoft Zune System, Amigo, Sprint, Buer, Giles, Narayan, and/or Lin	Claims 1-29
Weel in view of one or more of Wieder, Collart, Harper, Janik, the Microsoft Zune System, Amigo, Sprint, Buer, Giles, Narayan, and/or Lin	Claims 1-29
Harper in view of one or more of Wieder, Collart, Plastina, Janik, the Microsoft Zune System, Amigo, Sprint, Buer, Giles, Narayan, and/or Lin	Claims 1-29
Janik in view of one or more of Wieder, Collart, Plastina, Harper, the Microsoft Zune System, Amigo, Sprint, Buer, Giles, Narayan, and/or Lin	Claims 1-29
The Microsoft Zune in view of one or more of Wieder, Collart, Plastina, Harper, Janik, Amigo, Sprint, Buer, Giles, Narayan, and/or Lin	Claims 1-29
iTunes 4.0 in view of one or more of Wieder, Collart, Plastina, Harper, Janik, Amigo, Sprint, Buer, Giles, Narayan, and/or Lin	Claims 1-29
Collart in view of one or more of Wieder, Plastina, Harper, Janik, the Microsoft Zune System, Amigo, Sprint, Buer, Giles, Narayan and/or Lin	Claims 1-29

In addition to the specific combinations of prior art and the specific combinations of groups of prior art disclosed above, Apple reserves the right to rely on any other combination of any prior art references disclosed herein. Apple further reserves the right to rely upon combinations disclosed within the prosecution history of the references cited herein. These obviousness combinations reflect Apple's present understanding of the potential scope of the claims that SEVEN appears to be advocating and should not be seen as Apple's acquiescence to SEVEN's interpretation of the patent claims.

Apple also reserves the right to amend or supplement these contentions regarding anticipation or obviousness of the Asserted Claims, in view of further information from SEVEN, information discovered during discovery, or a claim construction ruling by the Court. SEVEN has not identified what elements or combinations it alleges were not known to one of ordinary skill in the art at the time. Therefore, for any claim limitation that SEVEN alleges is not disclosed in a particular prior art reference, Apple reserves the right to assert that any such limitation is either inherent in the disclosed reference or obvious to one of ordinary skill in the art at the time in light of the same, or that the limitation is disclosed in another of the references disclosed above and in combination would have rendered the Asserted Claim obvious.

C. Patent Rule 3-3(c): Charts Identifying Where Specifically in Each Alleged Item of Prior Art Each Asserted Claim Is Found

Pursuant to Patent Rule 3-3(c), charts identifying where specifically in each alleged item of prior art each limitation of each Asserted Claim is found, including for each limitation that Apple contends is governed by 35 U.S.C. § 112(6), the identity of the structure(s), act(s), or material(s) in each item of prior art that performs the claimed function, are attached in **Exhibits 986-A and 986-B**.

D. Patent Rule 3-3(d): Other Grounds for Invalidity

Apple identifies the following grounds for invalidity of the Asserted Claims of the ’986 patent based on 35 U.S.C. §§ 101 and/or 112. Apple reserves the right to supplement these disclosures based on further investigation and discovery.

1. Invalidity Pursuant to 35 U.S.C. § 112

Apple further asserts that the Asserted Claims of the ’986 patent are invalid under 35 U.S.C. § 112. The following are the grounds upon which Apple contends the Asserted Claims

are invalid for failure to meet the requirements of 35 U.S.C. § 112, ¶¶ 1, 2, 4 and/or 6, based on Apple's investigation to date and currently-available information.

For each claim identified as invalid, any dependent claims of those invalid claims are also invalid under 35 U.S.C. § 112, ¶ 1, ¶ 2, ¶ 4, and/or ¶ 6. Apple reserves the right to supplement and amend these contentions based on further discovery and investigation including, in particular, the deposition of any of the named inventors of the Asserted Patent, the parties' claim construction positions, and further investigation of SEVEN's implied infringement positions.

a) Written Description and/or Enablement

At least in view of SEVEN's apparent construction of the claims in its Infringement Contentions, the Asserted Claims of the '986 patent are invalid because the specification as filed does not contain adequate written description of the claimed inventions sufficient to lead a person of ordinary skill in the art to understand that the named inventors had possession of the purported inventions as claimed as required by 35 U.S.C. § 112, ¶ 1. Likewise, the specification does not enable one of ordinary skill in the art to make or use the claimed inventions without undue experimentation. Based on Apple's present understanding of SEVEN's infringement contentions, Apple asserts that the Asserted Claims of the of the '986 patent are invalid for reciting at least the following claim terms/phrases/limitations:

Claims 1, 12, and 23 of the '986 patent and its dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain an adequate written description and/or enabling disclosure of the authentication—"subsequent to the second device authenticating over the mobile network, the second device is authenticated with the first device." (*See, e.g.*, '986 Patent at 20:25-36). To the extent the term "authenticated" is construed to mean more than "an identifying element included in the user's account record," as identified in the '986 patent specification, the full scope of the claimed

subject matter is not described or enabled. The phrases "authenticating over the mobile network" or "second device is authenticated with the first" is not used in the patent's specification, and the patent's disclosures do not otherwise describe or enable the two different authentication requirements limitation. Accordingly, the specification fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

Claims 1, 12, and 23 of the '986 patent and its dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain an adequate written description and/or enabling disclosure for the two-device architecture embodied in the claims. These claims discuss the distribution of content between a "first device" and a "second device." However, the words "first device" and "second device" never appear in the specification, nor do the images depict a system that embodies two devices. While the specification discusses distribution content to a device, there are issues specific to content distribution across multiple devices that the specification does not adequately describe or disclose. For example, and as discussed in further detail below, the specification describes a system of authenticating a user device. However, the specification does not describe how authentication occurs across or between multiple devices. The specification describes a system for automatically transmitting content to a device, but does not describe how content is transmitted to a "first device" and then "automatically transmitted" to the "second device." Furthermore, the specification does not describe the relationship, if any, between authentication and content distribution across a first device and a second device. Accordingly, the specification fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject

matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

Claims 1, 12, and 23 of the ’986 patent and its dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain an adequate written description and/or enabling disclosure of “transmitting a representation of the accessed content.” (*See, e.g.*, ’986 Patent at 20:25-32). To the extent the term “transmitting a representation of the content” is construed to mean more than “digital audio data files, mobile device ring-tones, e-book data files, picture data files, video data files, e-mail data files, voice message data files, SMS data files, document files, and software applications,” as identified in the ’986 patent specification, the full scope of the claimed subject matter is not described or enabled. (*See, e.g.*, ’986 Patent at 9:11-17). Accordingly, the specification fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

Claims 1, 12, and 23 of the ’986 Patent and its dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain an adequate written description and/or enabling disclosure of the element “wherein the application at the first device and application at the second device are branded by the same entity,” and “the same entity is other than a provider that operates the mobile network.” (*See, e.g.*, ’986 Patent at 20:37-41). To the extent the terms “branded by the same entity,” and “the same entity is other than a provider that operates the mobile network,” are construed to mean more than “one or more services . . . may be branded by the mobile virtual network operator as a separate entity from the mobile network service provider,” (’986 Patent at 4:33-36), and “the

service may be branded by an entity other than the operator of the mobile network. For example the service may be branded by an MVNO" ('986 Patent at 15:6-12), as identified in the '986 patent specification, the full scope of the claimed subject matter is not described or enabled. Accordingly, the specification fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

Claims 4, 8, 15, 19, of the '986 patent are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain an adequate written description and/or enabling disclosure of "a notification." The phrase "a notification of available content" is not used in the patent's specification, and the patent's disclosures do not otherwise describe or enable any form of notification or notice to the user describing the availability of content for download. Accordingly, the specification fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

Claim 23 of the '986 Patent is invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain an adequate written description and/or enabling disclosure of "communicatively coupled." The phrase 'directly communicatively connected' is not defined, used, or described in the patent's specification, and the patent's disclosures do not otherwise describe or enable the 'directly communicatively connected' limitation." Furthermore, the specification fails to describe how the devices are indirectly communicatively connected to one another rather than directly communicatively connected. Accordingly, the specification fails to reasonably convey to one of ordinary skill that

the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

Finally, claims 1, 12, and 23 of the '986 patent are invalid for including the limitation requiring "transmitting a representation of the accessed content to an application at a second device associated with the user, wherein the second device is authenticated over a mobile network." This limitation lacks written description support and/or is not enabled, at least to the extent that SEVEN contends this limitation is satisfied by Apple's products. Apple's accused products do not "transmit[] a representation of the accessed content." Thus, to the extent the claim is interpreted broad enough to encompass differently or more than "transmitting a representation of the accessed content," this limitations lacks 112 support.

b) Indefiniteness

At least in view of SEVEN's apparent construction of the claims in its Infringement Contentions, the Asserted Claims of the '986 patent are invalid because they fail to particularly point out and distinctly claim the subject matter which the applicant regards as his invention under 35 U.S.C. § 112, ¶¶ 2, 4, and/or 6. Based on Apple's present understanding of SEVEN's infringement contentions, Apple asserts that the Asserted Claims of the of the '986 patent are invalid for reciting at least the following claim terms/phrases/limitations:

- Claim 1, 12, and 23 of the '986 patent and its dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 2, ¶ 4, and/or ¶ 6 because "the specification does not describe or otherwise inform one of ordinary skill about what constitutes "authentication over the mobile network" and "subsequent to the second device authenticating over the mobile network, the second device is authenticated with the first device." The '986 patent does not describe or explain how to distinguish 'authentication over the mobile network' from

'authenticat[ion] with the first device.' As such, one of ordinary skill would not understand the metes and bounds of the identified claims, rendering them indefinite under 35 U.S.C. § 112, ¶ 2.] Therefore, the Asserted Claims, when read in light of the specification and the prosecution history, "fail to inform, with reasonable certainty, those skilled in the art about the scope of the invention." *Nautilus, Inc. v. Biosig Instruments, Inc.*, 134 S. Ct. 2120, 2124 (2014).

- Claim 1, 12, and 23 of the '986 patent and its dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 2, ¶ 4, and/or ¶ 6 because the specification does not describe or otherwise inform one of ordinary skill about what constitutes "wherein the application at the first device and application at the second device are branded by the same entity," and "the same entity is other than a provider that operates the mobile network." The '986 patent specification explains that "the one or more services may be associated with the unique authentication token, and may be branded by the mobile virtual network operator as a separate entity from the mobile network service provider," ('986 Patent at 4:33-36), and "the service may be branded by an entity other than the operator of the mobile network. For example the service may be branded by an MVNO" ('986 Patent at 15:6-12). However, the '986 patent does not describe or explain the types of entities or services that may be "branded by the same entity," outside of this MVNO network services and mobile operator context. As such, one of ordinary skill would not understand the metes and bounds of the identified claims, rendering them indefinite under 35 U.S.C. § 112, ¶ 2.] Therefore, the Asserted Claims, when read in light of the specification and the prosecution history, "fail to

inform, with reasonable certainty, those skilled in the art about the scope of the invention." *Nautilus, Inc. v. Biosig Instruments, Inc*., 134 S. Ct. 2120, 2124 (2014).

2. Other Grounds for Invalidity

In addition to the preceding invalidity contentions, Apple further contends that each of the Asserted Claims of the '986 patent is drawn to subject matter that is not patentable under 35 U.S.C. § 101. The '986 patent Asserted Claims are invalid under 35 U.S.C. § 101 for failure to recite patent eligible subject matter. Specifically, all claims of the '986 patent are fatally abstract under the U.S. Supreme Court's decision in *Alice Corp. v. CLS Bank Int'l*, 134 S. Ct. 2345 (2014) and progeny. The ideas presented in the claims are generally directed to concepts of receiving information, analyzing it, selecting content, and transmitting that content. Under *Alice* Step 1, those ideas are abstract, as they relate to a fundamental long prevalent practice. *See Intellectual Ventures I LLC v. Symantec Corp*., 838 F.3d 1307, 1314 (Fed. Cir. 2016). Limiting the invention to a particular technological environment, e.g. generic computer hardware, "do[es] not render an otherwise abstract concept any less abstract." *Intellectual Ventures I LLC v. Capital One Fin. Corp*., 850 F.3d 1332, 1340 (Fed Cir. 2017). Furthermore, because the patent relates to transmission of information, it is likewise abstract, as "information is … an intangible." *Electric Power Group, LLC v. Alstom S.A.*, 830 F.3d 1350, 1353 (Fed. Cir. 2016). Furthermore, under *Alice* Step 2 the '986 patent does not contain any inventive concept. The '986 patent Asserted Claims employs well-known components or functionality, as shown in Apple's invalidity contentions involving anticipation and/or obviousness in this case, which is not enough to impart patent eligibility of an abstract idea. *See, e.g., Alice,* 134 S. Ct. at 2359 (holding that limitations describing "'well-understood, routine, conventional activit[ies]' previously known to

the industry" were insufficient to supply an inventive concept (quoting *Mayo*, 132 S. Ct. at 1294)). Further detail regarding Apple's contentions that the Asserted Claims of the '986 patent do not qualify as patent-eligible subject matter are contained in **Exhibit 986-D**.

Apple reserves the right to assert that the asserted patents are invalid under 35 U.S.C. §102(f) and/or (g) in the event Apple obtains evidence that the named inventors of the '986 patent did not invent (either alone or in conjunction with other parties) the subject matter claimed in the '986 patent. Should Apple obtain such evidence, it will provide the name of the person(s) from whom and the circumstances under which the invention or any part of it was derived, and/or the circumstances surrounding the making of the invention before the patent application.

Apple reserves the right to supplement these disclosures based on further investigation and discovery.

X. THE '176 PATENT

A. Patent Rule 3-3(a): Identification of Prior Art

At this time, Apple contends that at least each of the prior art references described and charted in **Exhibits 176-A and 176-B** anticipates or renders obvious, either alone or in combination, one or more of the Asserted Claims of the '176 patent.

Additional prior art that has not been charted, but is still relevant to the invalidity of the '176 patent is listed in **Exhibit C**, including without limitation as evidence of the state of the art at the alleged time of invention. Apple reserves the right to amend these invalidity contentions to assert these references depending on the claim construction and infringement positions SEVEN may take as the case proceeds. Moreover, Apple reserves the right to use these references in combination with other references to render the claims of the '176 patent obvious in the event SEVEN takes the position that certain claim limitations are missing from the references charted in **Exhibits 176-A and 176-B**.

B. Patent Rule 3-3(b): Whether Each Item Anticipates or Renders Obvious the Asserted Claims

SEVEN asserts claims 1–26 the ’176 patent against Apple in this lawsuit. These claims are invalid because the ’176 patent fails to meet one or more of the requirements for patentability. The individual bases for invalidity are provided below and in the claim charts attached as **Exhibits 176-A and 176-B**. Each of the foregoing listed prior art documents, the underlying work, and/or the underlying apparatus or method qualifies as prior art under one or more sections of 35 U.S.C. §§ 102 and/or 103.

Although Apple has identified at least one citation per limitation for each reference, each and every disclosure of the same limitation in the same reference is not necessarily identified. Rather, in an effort to focus the issues, Apple has cited representative portions of identified references, even where a reference may contain additional support for a particular claim element. In addition, persons of ordinary skill in the art generally read a prior art reference as a whole and in the context of other publications and literature. Thus, to understand and interpret any specific statement or disclosure within a prior art reference, such persons would rely on other information within the reference, along with other publications and their general scientific knowledge. Apple may rely upon uncited portions of the prior art references and on other publications and expert testimony to provide context, and as aids to understanding and interpreting the portions that are cited. Apple may also rely on uncited portions of the prior art references, other disclosed publications, and the testimony of experts to establish that a person of ordinary skill in the art would have been motivated to modify or combine certain of the cited references so as to render the claims obvious.

1. Priority

SEVEN's Patent Rule 3-1(e) disclosures provide that the Asserted Claims of the '176 patent are entitled to a priority date of April 21, 2005, which is the filing date of parent U.S. Application No. 11/112,690 ("the '690 application"), which issued as U.S. Patent No. 7,796,742. The '176 patent also claims priority to U.S. Application No. 11/640,629 ("the '629 application"), which issued as U.S. Patent No. 8,438,633. The '629 application is a continuation-in-part of the '690 application. Apple reserves the right to challenge SEVEN's assertion that the '176 patent is entitled to claim the benefit of the application filing date of the '690 application to the extent that it does not support the full scope of the Asserted Claims, for example, depending on scope of the Asserted Claims as properly construed. To the extent the '690 application does not support the full scope of the Asserted Claims, the priority date of the '176 patent should be the filing date of the '629 application, December 18, 2006.

SEVEN has provided no evidence to support its contention that the Asserted Claims of the '176 patent are entitled to claim priority back to the '690 application or any earlier filed application, and Apple therefore reserves the right to assert a later priority date based on any findings as to the priority date of the Asserted Claims by the Court, information learned through discovery, or otherwise.

a) The Asserted Claims of the '176 Patent Cannot Claim Priority to the '690 Application

None of the Asserted Claims are entitled to the filing date of U.S. Application No. 11/112,690 ("the '690 application"), issued as U.S. Patent No. 7,796,742 because the '176 patent claims 1, 14, and dependent claims thereof, as well as claims 7, 8, 10, 11, 13, 20, 21, 23, 24, and 26 do not have written description support in the '690 application. *See PowerOasis, Inc. v. T-Mobile USA, Inc.*, 522 F.3d 1299, 1306-07 (Fed. Cir. 2008).

Claims 1 and 14 are not entitled to the ’690 application filing date because the ’690 application does not actually or inherently disclose each and every claim element. *PowerOasis*, 522 F.3d at 1306-07. Claims 1 and 14 recite features relating to a server sending messages to a client device which find no support in the parent application to which the ’176 patent claims priority, the ’690 application. Nothing in the ’690 application shows the inventor(s) possessed and enabled functionalities relating to “sending a first message indicative of new information at the data store,” “transmitting a second message to the client device in response to receipt of the first message,” and “wherein additional information associated with the first message is sent from the data store to the client device upon receipt of the second message by the client device,” as recited in claims 1 and 14.

Importantly, the ’690 application never uses the terms “first message,” “second message,” “indicative of new information,” or “additional information,” or otherwise discloses the concepts. The ’690 application does make one reference to sending a “text message,” but such text message is not “indicative of new information at the data store” or sent “in response to a first message.” ’690 application ¶ [0038] (“In order to associate the unique identifier to the device 102 for recognition during future contact with the server 106, a text message, for example, can be sent to the device 102 with the unique identifier.”). The ’690 application never mentions sending messages or additional information in the context and based on the factors recited in the ’176 patent claims. Thus, the ’690 application does not adequately provide written description support for sending a first message, sending a second message, or providing additional information in response to the sending of the messages.

As to claims 7 and 15, the ’690 application fails to disclose “the first message is limited in data size.” As noted above, the ’690 application never uses the term “first message” and does

not disclose sending any communication "indicative of new information at the data store." Additionally, it does not disclose any message that is limited in data size, let alone one that is a "first message." Thus, the '690 application does not adequately provide written description support for limiting the first message in data size.

As to claims 8 and 16, the '690 application fails to disclose "wherein the first message is received when the first message matches a predefined characteristic set by the data store." As noted above, the '690 application never uses the term "first message" and does not disclose sending any communication "indicative of new information at the data store." Additionally, it does not disclose sending any such first message based on predefined characteristics. The '690 application does not use the term "predefined characteristics" or otherwise disclose the concept. Thus, the '690 application does not adequately provide written description support for sending a first message when the first message matches a predefined characteristic set by the data store.

As to claims 10 and 23, the '690 application fails to disclose "wherein the server is configured to direct the client device to delete content thereon in response to an indication that the client device is misappropriated." The '690 application does not use the term "misappropriated," "delete" or "indication" or otherwise disclose the concepts. Thus, the '690 application does not adequately provide written description support for "wherein the server is configured to direct the client device to delete content thereon in response to an indication that the client device is misappropriated."

As to claims 11 and 24, the '690 application fails to disclose "wherein the additional information is sent over a subsequently established connection that is independent of the server." As noted above, the '690 application never uses the term "additional information" and does not disclose sending any "additional information" upon receipt of the second message, and in

addition, does not disclose sending any such additional information over a subsequently established connection that is independent of the server. The '690 application does not use the term "subsequent connection" or "independent connection" or otherwise disclose the concepts. Thus, the '690 application does not adequately provide written description support for "wherein the additional information is sent over a subsequently established connection that is independent of the server."

As to claims 13 and 25, the '690 application fails to disclose "wherein an IP connection is established between the client device and the data store in response to transmission of the second message to the client device by the server for sending of the additional information." As noted above, the '690 application never uses the term "additional information" and does not disclose sending any "additional information" upon receipt of the second message, and in addition, does not disclose establishing an IP connection between the client device and the data store for sending such additional information. The '690 application does not use the term "IP connection" or otherwise disclose the concept. Thus, the '690 application does not adequately provide written description support for "wherein an IP connection is established between the client device and the data store in response to transmission of the second message to the client device by the server for sending of the additional information."

Consequently, the '690 application does not actually or inherently disclose each and every element of the '176 patent claims. *PowerOasis*, 522 F.3d at 1306-07. The introduction of these features into the claims resulted in the '176 patent claims not being entitled to the filing date of the '690 application, and are, at most, entitled to the filing date of December 18, 2006—the filing date of the '629 application.

2. Anticipation

Some or all of the Asserted Claims of the ’176 patent are invalid as anticipated under 35 U.S.C. § 102 in view of each of the prior art references identified above and in the claim charts included in **Exhibit 176-A**, which identify specific examples of where each limitation of the Asserted Claims is found in the prior art references. As explained above, the cited portions of prior art references identified in the attached claim charts are exemplary only and representative of the content and teaching of the prior art references, and should be understood in the context of the reference as a whole and as they would be understood by a person of ordinary skill in the art.

Apple identifies the following references as anticipating one or more of the Asserted Claims of the ’176 patent under 35 U.S.C. § 102. The below table of anticipating references is exemplary, and it does not constitute an admission that any reference anticipates only the listed claims. Further, Apple contends that any prior art reference in the attached charts that is charted for each limitation of any given claim, anticipates that claim, regardless of whether that prior art reference is listed in the following table.

Exhibit No.	Anticipating Prior Art	Claims
176-A1	U.S. Patent No. 7,191,218 to Innes [“Innes”]	1–9, 11–23, 24–26
176-A2	U.S. Patent Application Publication No. 2002/0046299 to Lefeber et al. [“Lefeber”]	1–9, 11–23, 24–26

To the extent any item of prior art cited above is deemed not to disclose, explicitly or inherently, any limitation of an Asserted Claim of the ’176 patent, Apple reserves the right to argue that any difference between that prior art and the corresponding patent claim would have been either inherent to the art, or obvious to a person of ordinary skill in the art, even if Apple has not specifically denoted that the art is to be combined with the knowledge of a person of ordinary skill in the art.

3. Obviousness

To the extent any limitation is deemed not to be exactly met by an item of prior art listed above and in **Exhibit 176-A**, then any purported differences are such that the claimed subject matter as a whole would have been obvious to one skilled in the art at the time of the alleged invention, in view of the state of the art and knowledge of those skilled in the art. The item of prior art would, therefore, render the relevant claims invalid for obviousness under 35 U.S.C. § 103.

In addition, the references identified above render one or more Asserted Claims of the '176 patent obvious when the references are read in combination with each other, and/or when read in view of the state of the art and knowledge of those skilled in the art. Each and every reference identified is also relevant to the state of the art at the time of the alleged invention. Any of the references disclosed above may be combined with one another to render obvious (and therefore invalid) each of SEVEN's Asserted Claims. Apple may rely upon a subset of the above identified references or all of the references identified above, including all references in **Exhibits 176-A, 176-B, and C**, for purposes of obviousness depending on the Court's claim construction, positions taken by SEVEN during this litigation, and further investigation and discovery.

To the extent the foregoing references are found not to anticipate the Asserted Claims, the foregoing references render the Asserted Claims obvious either alone or in combination with one or more of the other references identified above pursuant to Patent Rule 3-3(a). It would have been obvious to a person of skill in the art at the time of the alleged invention of the Asserted Claims of the '176 patent to combine the various references cited herein so as to disclose the Asserted Claims of the '176 patent.

In accordance with Patent Rule 3-3(b), prior art references rendering the Asserted Claims obvious, alone or in combination with other references, are outlined below and included in **Exhibits 176-A and 176-B**, which include exemplary claim charts for the Asserted Claims of the '176 patent showing specifically where in each reference or combinations of references each Asserted Claim is found, and an explanation of why the prior art renders the Asserted Claim obvious. Where applicable, **Exhibits 176-A and 176-B** include the motivation to combine references.

Moreover, in addition to the information contained elsewhere in these contentions and in particular **Exhibit 176-B**, Apple has identified additional motivations and reasons to combine the various references cited herein. In particular, multiple teachings, suggestions, and/or reasons to modify any of the references and/or to combine any two or more of the references in **Exhibits 176-A and 176-B** come from many sources, including the prior art (specific and as a whole), common knowledge, common sense, predictability, expectations, industry trends, design incentives or need, market demand or pressure, market forces, obvious to try, the nature of the problem faced, and/or knowledge possessed by one of ordinary skill. In addition, it would have been obvious to try combining the prior art references identified above because there were only a finite number of predictable solutions and/or because known work in one field or endeavor prompted variations based on predictable design incentives and/or market forces either in the same field or a different one. The combination of prior art references identified in these contentions would have been obvious because the claimed combinations represent the known potential options with a reasonable expectation of success. Additionally, one of ordinary skill in the art would have been motivated to create combinations identified in these contentions using: known methods to yield predictable results; known techniques in the same way; a simple

substitution of one known, equivalent element for another to obtain predictable results; and/or teaching, suggestion, or motivation in the prior art generally. Also, market forces in the industry, and the desire to improve features and performance, would motivate the addition of features to systems as they become available, become less expensive, become more commonly used, provide better performance, reduce costs, size or weight, or predictably achieve other clearly desirable results.

While Apple reserves the right to rely on any combination of the references reflected in their charts or incorporated herein by reference, Apple provides the following exemplary and non-exhaustive references and/or combinations evidencing invalidity of the claims of the Asserted Patents. The combinations of prior art listed below render obvious the Asserted Claims under the proper construction of the claims and/or under Plaintiff's apparent interpretation of the claims as set forth by Plaintiff in their Complaint and Infringement Contentions. Each combination renders the identified claims obvious through the express and/or inherent disclosure in the combination of references themselves, as well as in view of the knowledge of a person of ordinary skill in the art.

Obviousness Combinations	**Claims**
U.S. Patent Application Publication No. 2003/0149781 to Yared et al. ["Yared"] in view of U.S. Patent No. 8,326,9409 to Yamamoto et al. ["Yamamoto"] and/or one of U.S. Patent No. 5,898,783 to Rohrbach ["Rohrbach"], U.S. Patent No. 7,054,624 to Cocita ["Cocita"], or U.S. Patent No. 7,181,252 to Komsi ["Komsi]	1–26
Yared in view of Innes and/or one of Rohrbach, Cocita, or Komsi	1–26
Yared in view of Lefeber and/or one of Rohrbach, Cocita, or Komsi	1–26
Lefeber in view of Yared and/or one of Rohrbach, Cocita, or Komsi	1–26
Lefeber in view of International Pat. App. WO 00/65424 to Barrett et al. ["Barrett"] and/or Yared and/or one of Rohrbach, Cocita, or Komsi	1–26
Lefeber in view of one of Rohrbach, Cocita, or Komsi	1–26
Lefeber in view of Barrett and/or Innes and/or one of Rohrbach, Cocita, or Komsi	1–26
Lefeber in view of Barrett and/or International Patent Pub. WO 03/073242 to Barriga et al. ["Barriga"]and/or one of Rohrbach, Cocita, or Komsi	1–26
Lefeber in view of Barriga and/or one of Rohrbach, Cocita, or Komsi	1–26
Lefeber in view of Innes and/or one of Rohrbach, Cocita, or Komsi	1–26

Obviousness Combinations	Claims
Barrett in view of Yared and/or one of Rohrbach, Cocita, or Komsi	1–26
Barrett in view of Innes and/or one of Rohrbach, Cocita, or Komsi	1–26
Barrett in view of Lefeber and/or Innes and/or one of Rohrbach, Cocita, or Komsi	1–26
Barriga in view of Lefeber and/or one of Rohrbach, Cocita, or Komsi	1–26
Barriga in view of Innes and/or one of Rohrbach, Cocita, or Komsi	1–26
Innes in view of one of Rohrbach, Cocita, or Komsi	1–26
Innes in view of Barriga and/or one of Rohrbach, Cocita, or Komsi	1–26
Innes in view of Barrett and/or one of Rohrbach, Cocita, or Komsi	1–26
Yamamoto in view of Innes and/or one of Rohrbach, Cocita, or Komsi	1–26
Yamamoto in view of Barrett and/or one of Rohrbach, Cocita, or Komsi	1–26
Yamamoto in view of Yared and/or one of Rohrbach, Cocita, or Komsi	1–26
The Microsoft .Net Passport and .Net Alert System and/or one of Rohrbach, Cocita, or Komsi	1–26

In addition to the specific combinations of prior art and the specific combinations of groups of prior art disclosed above, Apple reserves the right to rely on any other combination of any prior art references disclosed herein. Apple further reserves the right to rely upon combinations disclosed within the prosecution history of the references cited herein. These obviousness combinations reflect Apple's present understanding of the potential scope of the claims that SEVEN appears to be advocating and should not be seen as Apple's acquiescence to SEVEN's interpretation of the patent claims.

Apple also reserves the right to amend or supplement these contentions regarding anticipation or obviousness of the Asserted Claims, in view of further information from SEVEN, information discovered during discovery, or a claim construction ruling by the Court. SEVEN has not identified what elements or combinations it alleges were not known to one of ordinary skill in the art at the time. Therefore, for any claim limitation that SEVEN alleges is not disclosed in a particular prior art reference, Apple reserves the right to assert that any such limitation is either inherent in the disclosed reference or obvious to one of ordinary skill in the art at the time in light of the same, or that the limitation is disclosed in another of the references disclosed above and in combination would have rendered the Asserted Claim obvious.

C. Patent Rule 3-3(c): Charts Identifying Where Specifically in Each Alleged Item of Prior Art Each Asserted Claim Is Found

Pursuant to Patent Rule 3-3(c), charts identifying where specifically in each alleged item of prior art each limitation of each Asserted Claim is found, including for each limitation that Apple contends is governed by 35 U.S.C. § 112(6), the identity of the structure(s), act(s), or material(s) in each item of prior art that performs the claimed function, are attached in **Exhibits 176-A and 176-B**.

D. Patent Rule 3-3(d): Other Grounds for Invalidity

Apple identifies the following grounds for invalidity of the Asserted Claims of the '176 patent based on 35 U.S.C. §§ 101 and/or 112. Apple reserves the right to supplement these disclosures based on further investigation and discovery.

1. Invalidity Pursuant to 35 U.S.C. § 112

Apple further asserts that the Asserted Claims of the '176 patent are invalid under 35 U.S.C. § 112. The following are the grounds upon which Apple contends the Asserted Claims are invalid for failure to meet the requirements of 35 U.S.C. § 112, ¶ 1, ¶ 2, ¶ 4 and/or ¶ 6, based on Apple's investigation to date and currently-available information.

For each claim identified as invalid, any dependent claims of those invalid claims are also invalid under 35 U.S.C. § 112, ¶ 1, ¶ 2, ¶ 4, and/or ¶ 6. Apple reserves the right to supplement and amend these contentions based on further discovery and investigation including, in particular, the deposition of any of the named inventors of the Asserted Patent, the parties' claim construction positions, and further investigation of SEVEN's implied infringement positions.

a) Written Description and/or Enablement

At least in view of SEVEN's apparent construction of the claims in its Infringement Contentions, the Asserted Claims of the '176 patent are invalid because the specification as filed

does not contain adequate written description of the claimed inventions sufficient to lead a person of ordinary skill in the art to understand that the named inventors had possession of the purported inventions as claimed as required by 35 U.S.C. § 112, ¶ 1. Likewise, the specification does not enable one of ordinary skill in the art to make or use the claimed inventions without undue experimentation. Based on Apple's present understanding of SEVEN's infringement contentions, Apple asserts that the Asserted Claims of the of the '176 patent are invalid for reciting at least the following claim terms/phrases/limitations:

Claim 1 of the '176 patent and its dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification does not contain an adequate written description and/or enabling disclosure of "configure a service to receive data from the data store on behalf of the client device, wherein the service is based on the second identifier." The phrases "second identifier" and "configure a service" are not used in the patent's specification, and the patent's disclosures do not otherwise describe or enable the "second identifier" or "configure a service" limitation. Accordingly, the specification fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed. The similar limitation in claim 14, "configuring a service to receive data from the data store on behalf of the client device, wherein the service is based on the second identifier," lacks written description and/or enabling disclosure for the same reasons.

Claims 10 and 23 of the '176 patent are invalid for failure to satisfy the requirements of 35 U.S.C. 112, ¶ 1 because the specification does not contain an adequate written description and/or enabling disclosure of "directing the client device to delete content thereon in response to an indication that the client device is misappropriated." The term "misappropriated" is not used

in the specification, nor is there any disclosure of the conditions or communications which might indicate that a device has been misappropriated. Although the specification does address "data obliteration" operations, there is no enabling disclosure of how "the sever" may direct the device to accomplish such a data obliteration. The only disclosure is of unspecified "client software" and an unspecified user-initiated command. '176 patent, 17:60–18:4. The only other discussion of deletion of data appears in the context of discussing conditions under which data may be deleted from the mail server, not the mobile device. *See, e.g.*, '176 patent, 14:30–37 (discussing the conditions under which e-mail may be deleted in POP and IMAP protocols). There is no other disclosure of deleting content on a mobile device or the means by which such deletion might be accomplished. Accordingly, the specification fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

Claims 1 and 14 and their dependent claims also lack written description support and/or are not enabled, at least to the extent that SEVEN contends the "a server" or "the server" limitations are satisfied by Apple's products. To the extent the term "a server" is construed to mean more than a specific set of computers acting as a single server, as identified in the '176 patent specification, the full scope of the claimed subject matter is not described or enabled. Accordingly, the specification fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

b) Indefiniteness

At least in view of SEVEN's apparent construction of the claims in its Infringement Contentions, the Asserted Claims of the '176 patent are invalid because they fail to particularly point out and distinctly claim the subject matter which the applicant regards as his invention

under 35 U.S.C. § 112, ¶¶ 2, 4, and/or 6. Based on Apple's present understanding of SEVEN's infringement contentions, Apple asserts that the Asserted Claims of the of the '176 patent are invalid for reciting at least the following claim terms/phrases/limitations:

Independent claims 1 and 14 of the '176 patent and their dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 2, ¶ 4, and/or ¶ 6 because the specification does not describe or otherwise inform one of ordinary skill about what constitutes "a subsequent connection with the server." The '176 patent does not describe or explain how to distinguish a "subsequent connection" from any other connection, including the conditions and or timing of a "subsequent connection." Moreover, the '176 patent does not describe or explain how such a "subsequent connection" may "include a first identifier." As such, one of ordinary skill would not understand the metes and bounds of the identified claims, rendering them indefinite under 35 U.S.C. § 112, ¶ 2. Therefore, the Asserted Claims, when read in light of the specification and the prosecution history, "fail to inform, with reasonable certainty, those skilled in the art about the scope of the invention." *Nautilus, Inc. v. Biosig Instruments, Inc*., 134 S. Ct. 2120, 2124 (2014).

Dependent claims 7 and 20 of the '176 patent are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 2, ¶ 4, and/or ¶ 6 because the specification does not describe or otherwise inform one of ordinary skill about what constitutes "wherein the first identifier is limited in data size." The '176 patent does not describe or explain how to distinguish a "first message [] limited in data size" from any other message. As such, one of ordinary skill would not understand the metes and bounds of the identified claims, rendering them indefinite under 35 U.S.C. § 112, ¶ 2. Therefore, the Asserted Claims, when read in light of the specification and the

prosecution history, "fail to inform, with reasonable certainty, those skilled in the art about the scope of the invention." *Nautilus, Inc. v. Biosig Instruments, Inc.*, 134 S. Ct. 2120, 2124 (2014).

Claims 1 and 14 of the '176 patent and their dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 2, ¶ 4, and/or ¶ 6 because the specification does not describe or otherwise inform one of ordinary skill about what constitutes "a server." The '176 patent does not describe or explain how to limit a server. According to SEVEN, a server has no bounds, including based on the amount of physical servers involved or the type of server involved, such that SEVEN would consider all servers to be one server. As such, one of ordinary skill would not understand the metes and bounds of the identified claims, rendering them indefinite under 35 U.S.C. § 112, ¶ 2. Therefore, the Asserted Claims, when read in light of the specification and the prosecution history, "fail to inform, with reasonable certainty, those skilled in the art about the scope of the invention." *Nautilus, Inc. v. Biosig Instruments, Inc.*, 134 S. Ct. 2120, 2124 (2014).

2. Other Grounds for Invalidity

Apple reserves the right to assert that the asserted patents are invalid under 35 U.S.C. §102(f) and/or (g) in the event Apple obtains evidence that the named inventors of the '176 patent did not invent (either alone or in conjunction with other parties) the subject matter claimed in the '176 patent. For example, although the '962 patent purports to be a continuation of the '176 patent and the two patents share the same specification and their claims share many of the same limitations and a terminal disclaimer to the same patent, the named inventors the differ: the '176 patent identifies Parvinder Sawhney and five others as inventors whereas the '962 patent identifies Parvinder Sawhney and one other (who was not an inventor on the '176 patent) as '962 patent inventors. During prosecution, the application leading to the '176 patent was initially filed on November 28, 2016, naming Ari Backholm and Parvinder Sawhney as

inventors. On April 19, 2017, the applicant filed a Request Under Rule 48 to Correct Inventorship, removing Ari Backholm as an inventor, and designating an additional five inventors. The Request to Correct Inventorship was accepted on April 24, 2017 without comment or explanation. SEVEN has identified no evidence from which it may be determined that inventorship is correct as to the '962 and '176 patent. Should Apple obtain further such evidence, it will provide the name of the person(s) from whom and the circumstances under which the invention or any part of it was derived, and/or the circumstances surrounding the making of the invention before the patent application.

Apple reserves the right to supplement these disclosures based on further investigation and discovery.

XI. THE '619 PATENT

A. Patent Rule 3-3(a): Identification of Prior Art

At this time, Apple contends that at least each of the prior art references described and charted in **Exhibits 619-A and 619-B** anticipates or renders obvious, either alone or in combination, one or more of the Asserted Claims of the '619 patent.

Additional prior art that has not been charted, but is still relevant to the invalidity of the '619 patent is listed in **Exhibit C**, including without limitation as evidence of the state of the art at the alleged time of invention. Apple reserves the right to amend these invalidity contentions to assert these references depending on the claim construction and infringement positions SEVEN may take as the case proceeds. Moreover, Apple reserves the right to use these references in combination with other references to render the claims of the '619 patent obvious in the event SEVEN takes the position that certain claim limitations are missing from the references charted in **Exhibits 619-A and 619-B**.

B. Patent Rule 3-3(b): Whether Each Item Anticipates or Renders Obvious the Asserted Claims

SEVEN asserts claims 22-28, 32, 33, 36-42, 46, and 50-52 of the '619 patent against Apple in this lawsuit. These claims are invalid because the '619 patent fails to meet one or more of the requirements for patentability. The individual bases for invalidity are provided below and in the claim charts attached as **Exhibits 619-A and 619-B**. Each of the foregoing listed prior art documents, the underlying work, and/or the underlying apparatus or method qualifies as prior art under one or more sections of 35 U.S.C. §§ 102 and/or 103.

Although Apple has identified at least one citation per limitation for each reference, each and every disclosure of the same limitation in the same reference is not necessarily identified. Rather, in an effort to focus the issues, Apple has cited representative portions of identified references, even where a reference may contain additional support for a particular claim element. In addition, persons of ordinary skill in the art generally read a prior art reference as a whole and in the context of other publications and literature. Thus, to understand and interpret any specific statement or disclosure within a prior art reference, such persons would rely on other information within the reference, along with other publications and their general scientific knowledge. Apple may rely upon uncited portions of the prior art references and on other publications and expert testimony to provide context, and as aids to understanding and interpreting the portions that are cited. Apple may also rely on uncited portions of the prior art references, other disclosed publications, and the testimony of experts to establish that a person of ordinary skill in the art would have been motivated to modify or combine certain of the cited references so as to render the claims obvious.

1. Priority

SEVEN's Patent Rule 3-1(e) disclosures provide that the Asserted Claims of the '619 patent are entitled to a priority date of November 22, 2004, which is the filing date of Finnish Patent Application number 20045451. SEVEN has provided no evidence to support its contention that the Asserted Claims of the '619 patent are entitled to claim priority back to this or any earlier filed application, and Apple therefore reserves the right to assert a later priority date based on any findings as to the priority date of the Asserted Claims by the Court, information learned through discovery, or otherwise.

The '619 patent claims priority to a Finnish Patent Application number 20045451 filed on November 22, 2004. Apple reserves the right to challenge SEVEN's assertion that the '619 patent is entitled to claim the benefit of that provisional application's filing date to the extent that the provisional application does not support the full scope of the Asserted Claims, for example, depending on the scope of the Asserted Claims as properly construed.

None of the Asserted Claims are entitled to the filing date of the Finnish application because every claim does not have written description support from the Finnish application. *See Falko-Gunter Falkner v. Inglis*, 448 F.3d 1357 (Fed. Cir. 2006). Each and every asserted claim is not entitled to the Finnish application filing date because the Finnish application does not actually or inherently disclose each and every claim element. *PowerOasis, Inc. v. T-Mobile USA, Inc.*, 522 F.3d 1299, 1306-07 (Fed. Cir. 2008).

For example, the Asserted Claims recite features relating to "optically receiv[ing] information including a displayed service activation code from a remote device" and "register[ing] the remote device for access to a messaging account using the service activation code," and variations of those limitations for other claims. Nothing in the Finnish application

shows that the inventors possessed and enabled functionalities relating to these limitations as recited in the Asserted Claims.

Consequently, the Finnish application does not actually or inherently disclose each and every element of the ’619 patent claims and therefore does not deserve the February 22, 2004 priority date claimed.

2. Anticipation

Some or all of the Asserted Claims of the ’619 patent are invalid as anticipated under 35 U.S.C. § 102 in view of each of the prior art references identified above and in the claim charts included in **Exhibit 619-A**, which identify specific examples of where each limitation of the Asserted Claims is found in the prior art references. As explained above, the cited portions of prior art references identified in the attached claim charts are exemplary only and representative of the content and teaching of the prior art references, and should be understood in the context of the reference as a whole and as they would be understood by a person of ordinary skill in the art.

Apple identifies the following references as anticipating one or more of the Asserted Claims of the ’619 patent under 35 U.S.C. § 102. The below table of anticipating references is exemplary, and it does not constitute an admission that any reference anticipates only the listed claims. Further, Apple contends that any prior art reference in the attached charts that is charted for each limitation of any given claim, anticipates that claim, regardless of whether that prior art reference is listed in the following table.

Anticipating Prior Art	Claims
WO 01/29731 to Thompson et al.	Claims 22-28, 32, 33, 36-42, 46, and 50-52
US 7,984,488 to Cross et al.	Claims 22-27, 32, 33, 36-42, 46, and 50-52

To the extent any item of prior art cited above is deemed not to disclose, explicitly or inherently, any limitation of an Asserted Claim of the ’619 patent, Apple reserves the right to

argue that any difference between that prior art and the corresponding patent claim would have been either inherent to the art, or obvious to a person of ordinary skill in the art, even if Apple has not specifically denoted that the art is to be combined with the knowledge of a person of ordinary skill in the art.

3. Obviousness

To the extent any limitation is deemed not to be exactly met by an item of prior art listed above and in **Exhibit 619-A**, then any purported differences are such that the claimed subject matter as a whole would have been obvious to one skilled in the art at the time of the alleged invention, in view of the state of the art and knowledge of those skilled in the art. The item of prior art would, therefore, render the relevant claims invalid for obviousness under 35 U.S.C. § 103.

In addition, the references identified above render one or more Asserted Claims of the '619 patent obvious when the references are read in combination with each other, and/or when read in view of the state of the art and knowledge of those skilled in the art. Each and every reference identified is also relevant to the state of the art at the time of the alleged invention. Any of the references disclosed above may be combined with one another to render obvious (and therefore invalid) each of SEVEN's Asserted Claims. Apple may rely upon a subset of the above identified references or all of the references identified above, including all references in **Exhibits 619-A, 619-B, and C**, for purposes of obviousness depending on the Court's claim construction, positions taken by SEVEN during this litigation, and further investigation and discovery.

To the extent the foregoing references are found not to anticipate the Asserted Claims, the foregoing references render the Asserted Claims obvious either alone or in combination with one or more of the other references identified above pursuant to Patent Rule 3-3(a). It would

have been obvious to a person of skill in the art at the time of the alleged invention of the Asserted Claims of the ’619 patent to combine the various references cited herein so as to disclose the Asserted Claims of the ’619 patent.

In accordance with Patent Rule 3-3(b), prior art references rendering the Asserted Claims obvious, alone or in combination with other references, are outlined below and included in **Exhibits 619-A and 619-B**, which include exemplary claim charts for the Asserted Claims of the ’619 patent showing specifically where in each reference or combinations of references each Asserted Claim is found, and an explanation of why the prior art renders the Asserted Claim obvious. Where applicable, **Exhibits 619-A and 619-B** include the motivation to combine references.

Moreover, in addition to the information contained elsewhere in these contentions and in particular **Exhibits 619-B**, Apple has identified additional motivations and reasons to combine the various references cited herein. In particular, multiple teachings, suggestions, and/or reasons to modify any of the references and/or to combine any two or more of the references in **Exhibits 619-A and 619-B** come from many sources, including the prior art (specific and as a whole), common knowledge, common sense, predictability, expectations, industry trends, design incentives or need, market demand or pressure, market forces, obvious to try, the nature of the problem faced, and/or knowledge possessed by one of ordinary skill. In addition, it would have been obvious to try combining the prior art references identified above because there were only a finite number of predictable solutions and/or because known work in one field or endeavor prompted variations based on predictable design incentives and/or market forces either in the same field or a different one. The combination of prior art references identified in these contentions would have been obvious because the claimed combinations represent the known

potential options with a reasonable expectation of success. Additionally, one of ordinary skill in the art would have been motivated to create combinations identified in these contentions using: known methods to yield predictable results; known techniques in the same way; a simple substitution of one known, equivalent element for another to obtain predictable results; and/or teaching, suggestion, or motivation in the prior art generally. Also, market forces in the industry, and the desire to improve features and performance, would motivate the addition of features to systems as they become available, become less expensive, become more commonly used, provide better performance, reduce costs, size or weight, or predictably achieve other clearly desirable results.

While Apple reserves the right to rely on any combination of the references reflected in their charts or incorporated herein by reference, Apple provides the following exemplary and non-exhaustive references and/or combinations evidencing invalidity of the claims of the Asserted Patents. The combinations of prior art listed below render obvious the Asserted Claims under the proper construction of the claims and/or under Plaintiff's apparent interpretation of the claims as set forth by Plaintiff in their Complaint and Infringement Contentions. Each combination renders the identified claims obvious through the express and/or inherent disclosure in the combination of references themselves, as well as in view of the knowledge of a person of ordinary skill in the art.

Obviousness Combinations	**Claims**
International Patent Application No. WO 01/29731 to Thompson et al. ("Thompson") in view of Int. Patent. App. WO 02/25890 ("Hind"), U.S. Patent No. 7,603,556 to Brown et al. ("Brown"), U.S. Patent No. 7,849,313 to Klassen et al. ("Klassen"), U.S. Patent No. 8,831,576 to Munje et al. ("Munje"), U.S. Patent No. 7,012,503 to Nielsen et al. ("Nielsen"), U.S. Patent No. 7,984,488 to Cross et al. ("Cross"), Int. Patent App. WO 2005/002174 ("Braley"), U.S. Patent App. No. 2006/0135064 ("Cho"), U.S. Patent App. No. 2004/0255034 ("Choi"), European Patent EP 1 578 093 ("Ekdahl"), U.S. Patent No. 7,921,209	All Asserted Claims

Obviousness Combinations	Claims
("Hammell"), U.S. Patent No. 7,562,218 ("Kirkup"), U.S. Patent App. No. 2004/0205248 to Little et al. ("Little"), U.S. Patent App. No. 2006/0031913 ("Pulitzer"), U.S. Patent Pub. No. 2005/0060551 ("Barchi"), U.S. Patent Pub. No. 2003/0101343 ("Eaton"), U.S. Patent Pub. No. 2004/0186884 ("Dutordoir"), and/or U.S. Patent No. 9,020,854 ("Giobbi")	
Thompson in view of Cross, and/or one or more of Pulitzer, Hammel, Kirkup, Barchi, Dutordoir, and/or Eaton	All Asserted Claims
Thompson in view of Hind, and/or one or more of Pulitzer, Hammel, Kirkup, Barchi, Dutordoir, and/or Eaton	All Asserted Claims
Thompson in view of Klassen, and/or one or more of Pulitzer, Hammel, Kirkup, Barchi, Dutordoir, and/or Eaton	All Asserted Claims
Thompson in view of Munje, and/or one or more of Pulitzer, Hammel, Kirkup, Barchi, Dutordoir, and/or Eaton	All Asserted Claims
Thompson in view of Brown, and/or one or more of Pulitzer, Hammel, Kirkup, Barchi, Dutordoir, and/or Eaton	All Asserted Claims
Thompson in view of Little, and/or one or more of Pulitzer, Hammel, Kirkup, Barchi, Dutordoir, and/or Eaton	All Asserted Claims
Little in view of U.S. Patent No. 7,124,953 ("Antilla"), U.S. Patent App. No. 2002/0147918 ("Osthoff"), U.S. patent No. 7,289,792 ("Turunen")	All Asserted Claims except 24, 25, 26, 36, 39, 40, 50, 52
Cross in view of Thompson, and/or one or more of Pulitzer, Hammel, Kirkup, Barchi, Dutordoir, and/or Eaton	All Asserted Claims
Cross in view of Hind, and/or one or more of Pulitzer, Hammel, Kirkup, Barchi, Dutordoir, and/or Eaton	All Asserted Claims
Cross in view of Klassen, and/or one or more of Pulitzer, Hammel, Kirkup, Barchi, Dutordoir, and/or Eaton	All Asserted Claims
Cross in view of Munje, and/or one or more of Pulitzer, Hammel, Kirkup, Barchi, Dutordoir, and/or Eaton	All Asserted Claims
Cross in view of Brown, and/or one or more of Pulitzer, Hammel, Kirkup, Barchi, Dutordoir, and/or Eaton	All Asserted Claims
Cross in view of Little, and/or one or more of Pulitzer, Hammel, Kirkup, Barchi, Dutordoir, and/or Eaton	All Asserted Claims
Cross in view of Brown, Klassen, Munje, Thompson, Hind, Little, and/or one or more of Nielsen, Braley, Cho, Choi, Ekdahl, Hammell, Kirkup, Choi, Pulitzer, Barchi, Eaton, and/or Giobbi.	All Asserted Claims
Hind in view of Cross, and/or one or more of Pulitzer, Hammel, Kirkup, Barchi, Dutordoir, and/or Eaton	All Asserted Claims
Hind in view of Thompson, and/or one or more of Pulitzer, Hammel, Kirkup, Barchi, Dutordoir, and/or Eaton	All Asserted Claims
Hind in view of Klassen, and/or one or more of Pulitzer, Hammel, Kirkup, Barchi, Dutordoir, and/or Eaton	All Asserted Claims
Hind in view of Munje, and/or one or more of Pulitzer, Hammel, Kirkup, Barchi, Dutordoir, and/or Eaton	All Asserted Claims

Obviousness Combinations	Claims
Hind in view of Brown, and/or one or more of Pulitzer, Hammel, Kirkup, Barchi, Dutordoir, and/or Eaton	All Asserted Claims
Hind in view of Little, and/or one or more of Pulitzer, Hammel, Kirkup, Barchi, Dutordoir, and/or Eaton	All Asserted Claims
Hind in view of Brown, Klassen, Munje, Cross, Thompson, Little, and/or one or more of Nielsen, Braley, Cho, Choi, Ekdahl, Hammell, Kirkup, Choi, Pulitzer, Barchi, Eaton, and/or Giobbi	All Asserted Claims
Klassen in view of Cross, and/or one or more of Pulitzer, Hammel, Kirkup, Barchi, Dutordoir, and/or Eaton	All Asserted Claims
Klassen in view of Hind, and/or one or more of Pulitzer, Hammel, Kirkup, Barchi, Dutordoir, and/or Eaton	All Asserted Claims
Klassen in view of Thompson, and/or one or more of Pulitzer, Hammel, Kirkup, Barchi, Dutordoir, and/or Eaton	All Asserted Claims
Klassen in view of Munje, and/or one or more of Pulitzer, Hammel, Kirkup, Barchi, Dutordoir, and/or Eaton	All Asserted Claims
Klassen in view of Brown, and/or one or more of Pulitzer, Hammel, Kirkup, Barchi, Dutordoir, and/or Eaton	All Asserted Claims
Klassen in view of Little, and/or one or more of Pulitzer, Hammel, Kirkup, Barchi, Dutordoir, and/or Eaton	All Asserted Claims
Klassen in view of Brown, Thompson, Munje, Cross, Hind, Little, and/or one or more of Nielsen, Braley, Cho, Choi, Ekdahl, Hammell, Kirkup, Choi, Pulitzer, Barchi, Eaton, and/or Giobbi	All Asserted Claims
Munje in view of Cross, and/or one or more of Pulitzer, Hammel, Kirkup, Barchi, Dutordoir, and/or Eaton	All Asserted Claims
Munje in view of Hind, and/or one or more of Pulitzer, Hammel, Kirkup, Barchi, Dutordoir, and/or Eaton	All Asserted Claims
Munje in view of Klassen, and/or one or more of Pulitzer, Hammel, Kirkup, Barchi, Dutordoir, and/or Eaton	All Asserted Claims
Munje in view of Thompson, and/or one or more of Pulitzer, Hammel, Kirkup, Barchi, Dutordoir, and/or Eaton	All Asserted Claims
Munje in view of Brown, and/or one or more of Pulitzer, Hammel, Kirkup, Barchi, Dutordoir, and/or Eaton	All Asserted Claims
Munje in view of Little, and/or one or more of Pulitzer, Hammel, Kirkup, Barchi, Dutordoir, and/or Eaton	All Asserted Claims
Munje in view of Brown, Klassen, Thompson, Cross, Hind, Little, and/or one or more of Nielsen, Braley, Cho, Choi, Ekdahl, Hammell, Kirkup, Choi, Pulitzer, Barchi, Eaton, and/or Giobbi.	All Asserted Claims
Brown in view of Cross, and/or one or more of Pulitzer, Hammel, Kirkup, Barchi, Dutordoir, and/or Eaton	All Asserted Claims
Brown in view of Hind, and/or one or more of Pulitzer, Hammel, Kirkup, Barchi, Dutordoir, and/or Eaton	All Asserted Claims
Brown in view of Klassen, and/or one or more of Pulitzer, Hammel, Kirkup, Barchi, Dutordoir, and/or Eaton	All Asserted Claims
Brown in view of Munje, and/or one or more of Pulitzer, Hammel, Kirkup, Barchi, Dutordoir, and/or Eaton	All Asserted Claims

Obviousness Combinations	Claims
Brown in view of Thompson, and/or one or more of Pulitzer, Hammel, Kirkup, Barchi, Dutordoir, and/or Eaton	All Asserted Claims
Brown in view of Little, and/or one or more of Pulitzer, Hammel, Kirkup, Barchi, Dutordoir, and/or Eaton	All Asserted Claims
Brown in view of Thompson, Klassen, Munje, Cross, Hind, Little and/or one or more of Nielsen, Braley, Cho, Choi, Ekdahl, Hammell, Kirkup, Choi, Pulitzer, Barchi, Eaton, and/or Giobbi	All Asserted Claims
Little in view of Cross, and/or one or more of Pulitzer, Hammel, Kirkup, Barchi, Dutordoir, and/or Eaton	All Asserted Claims
Little in view of Hind, and/or one or more of Pulitzer, Hammel, Kirkup, Barchi, Dutordoir, and/or Eaton	All Asserted Claims
Little in view of Klassen, and/or one or more of Pulitzer, Hammel, Kirkup, Barchi, Dutordoir, and/or Eaton	All Asserted Claims
Little in view of Munje, and/or one or more of Pulitzer, Hammel, Kirkup, Barchi, Dutordoir, and/or Eaton	All Asserted Claims
Little in view of Brown, and/or one or more of Pulitzer, Hammel, Kirkup, Barchi, Dutordoir, and/or Eaton	All Asserted Claims
Little in view of Thompson, and/or one or more of Pulitzer, Hammel, Kirkup, Barchi, Dutordoir, and/or Eaton	All Asserted Claims
Little in view of Brown, Klassen, Munje, Cross, Hind, Thompson and/or one or more of Nielsen, Braley, Cho, Choi, Ekdahl, Hammell, Kirkup, Choi, Pulitzer, Barchi, Eaton, and/or Giobbi	All Asserted Claims

In addition to the specific combinations of prior art and the specific combinations of groups of prior art disclosed above, Apple reserves the right to rely on any other combination of any prior art references disclosed herein. Apple further reserves the right to rely upon combinations disclosed within the prosecution history of the references cited herein. These obviousness combinations reflect Apple's present understanding of the potential scope of the claims that SEVEN appears to be advocating and should not be seen as Apple's acquiescence to SEVEN's interpretation of the patent claims.

Apple also reserves the right to amend or supplement these contentions regarding anticipation or obviousness of the Asserted Claims, in view of further information from SEVEN, information discovered during discovery, or a claim construction ruling by the Court. SEVEN has not identified what elements or combinations it alleges were not known to one of ordinary

skill in the art at the time. Therefore, for any claim limitation that SEVEN alleges is not disclosed in a particular prior art reference, Apple reserves the right to assert that any such limitation is either inherent in the disclosed reference or obvious to one of ordinary skill in the art at the time in light of the same, or that the limitation is disclosed in another of the references disclosed above and in combination would have rendered the Asserted Claim obvious.

C. Patent Rule 3-3(c): Charts Identifying Where Specifically in Each Alleged Item of Prior Art Each Asserted Claim Is Found

Pursuant to Patent Rule 3-3(c), charts identifying where specifically in each alleged item of prior art each limitation of each Asserted Claim is found, including for each limitation that Apple contends is governed by 35 U.S.C. § 112(6), the identity of the structure(s), act(s), or material(s) in each item of prior art that performs the claimed function, are attached in **Exhibits 619-A and 619-B**.

D. Patent Rule 3-3(d): Other Grounds for Invalidity

Apple identifies the following grounds for invalidity of the Asserted Claims of the '619 patent based on 35 U.S.C. §112. Apple reserves the right to supplement these disclosures based on further investigation and discovery.

1. Invalidity Pursuant to 35 U.S.C. § 112

Apple further asserts that the Asserted Claims of the '619 patent are invalid under 35 U.S.C. § 112. The following are the grounds upon which Apple contends the Asserted Claims are invalid for failure to meet the requirements of 35 U.S.C. § 112, ¶ 1, ¶ 2, ¶ 4 and/or ¶ 6, based on Apple's investigation to date and currently-available information.

For each claim identified as invalid, any dependent claims of those invalid claims are also invalid under 35 U.S.C. § 112, ¶ 1, ¶ 2, ¶ 4, and/or ¶ 6. Apple reserves the right to supplement and amend these contentions based on further discovery and investigation including, in

particular, the deposition of any of the named inventors of the Asserted Patent, the parties' claim construction positions, and further investigation of SEVEN's implied infringement positions.

a) Written Description and/or Enablement

At least in view of SEVEN's apparent construction of the claims in its Infringement Contentions, the Asserted Claims of the '619 patent are invalid because the specification as filed does not contain adequate written description of the claimed inventions sufficient to lead a person of ordinary skill in the art to understand that the named inventors had possession of the purported inventions as claimed as required by 35 U.S.C. § 112, ¶ 1. Likewise, the specification does not enable one of ordinary skill in the art to make or use the claimed inventions without undue experimentation. Based on Apple's present understanding of SEVEN's infringement contentions, Apple asserts that the Asserted Claims of the of the '619 patent are invalid for reciting at least the following claim terms/phrases/limitations:

Every Asserted Claim of the '619 patent and its dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain an adequate written description and/or enabling disclosure. Every Asserted Claim of the '619 patent a device comprising a (i) radio and a (ii) processor and memory operable to perform several recited functions, e.g., sending a message from the claimed device to a remote device. The only disclosures in the specification describe a "host system" (e.g., "a normal office computer" or "server") that sends email messages to a "mobile terminal," described as a "pocket or laptop computer with a radio interface, a smart cellular telephone, or the like." Thus, the claimed "device" may only find written description support in the "host system" described in the specification. However, Plaintiff's infringement allegations suggest Plaintiff is interpreting the "device" and "remote device" claimed in the Asserted Claims as mobile phones and smartwatches, respectively. Accordingly, Plaintiff's infringement allegations extend the scope

of the claimed invention beyond the disclosures of the '619 patent's written description. Thus, to the extent the claimed "device" is broad enough to encompass the accused instrumentalities (which Apple denies), the specification fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

Claims 22, 37, and 51 of the '619 patent and its dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain an adequate written description and/or enabling disclosure of "optically receive information including a displayed service activation code from a remote device." The specification does not disclose any support for the optical receipt of a displayed code from a remote device using a camera. In particular, the specification does not support the use of a camera to optically receive a service activation code. The phrase "optically receive information including a displayed service activation code from a remote device" is not used in the patent's specification, and the patent's disclosures do not otherwise describe or enable the "optically receive information including a displayed service activation code from a remote device" limitation. Accordingly, the specification fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

b) Indefiniteness

At least in view of SEVEN's apparent construction of the claims in its Infringement Contentions, the Asserted Claims of the '619 patent are invalid because they fail to particularly point out and distinctly claim the subject matter which the applicant regards as his invention under 35 U.S.C. § 112, ¶¶ 2, 4, and/or 6. Based on Apple's present understanding of SEVEN's

infringement contentions, Apple asserts that the Asserted Claims of the of the '619 patent are invalid for reciting at least the following claim terms/phrases/limitations:

- Dependent claims 24, 25, 26, 39, and 40 of the '619 patent are indefinite and therefore invalid under 35 U.S.C. § 112, ¶ 4 for failing to place a further limitation on independent claims 22 and 37 from which they depend. Rather than specifying a further limitation on the independent claims, as the statute requires, the dependent claims instead purport to add limitations that are already included within the independent claim. Specifically, the '619 patent defines "optically receiving" as narrower than "off-line communication," meaning the "off-line communication" limitation does not place a further limitation on the respective independent claims. Therefore, the Asserted Claims, when read in light of the specification and the prosecution history, "fail to inform, with reasonable certainty, those skilled in the art about the scope of the invention." *Nautilus, Inc. v. Biosig Instruments, Inc.*, 134 S. Ct. 2120, 2124 (2014).
- Claims 27, 28, 41, and 42 of the '619 patent and its dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 2, ¶ 4, and/or ¶ 6 because the terms "the authentication of the device" and "the authentication of the messaging account" lack antecedent basis. Further, the specification does not describe or otherwise inform one of ordinary skill about what constitutes "the authentication of the device" or "the authentication of the messaging account." The '619 patent does not describe or explain how the authentication of a device is tied to the authentication of a messaging account, or as here, what the terms are referring to. Therefore, the Asserted Claims, when read in light of the

specification and the prosecution history, "fail to inform, with reasonable certainty, those skilled in the art about the scope of the invention." *Nautilus, Inc. v. Biosig Instruments, Inc.*, 134 S. Ct. 2120, 2124 (2014).

- Claims 32 and 46 of the '619 patent and its dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 2, ¶ 4, and/or ¶ 6 because the term "closely related" is a term of degree, and the specification provides no objective indication by which to guide how related something must be in order to be "closely related." As such, one of ordinary skill would not understand the metes and bounds of the identified claims, rendering them indefinite under 35 U.S.C. § 112, ¶ 2. Therefore, the Asserted Claims, when read in light of the specification and the prosecution history, "fail to inform, with reasonable certainty, those skilled in the art about the scope of the invention." *Nautilus, Inc. v. Biosig Instruments, Inc.*, 134 S. Ct. 2120, 2124 (2014).

2. Other Grounds for Invalidity

Apple reserves the right to assert that the asserted patents are invalid under 35 U.S.C. §102(f) and/or (g) in the event Apple obtains evidence that the named inventors of the '619 patent did not invent (either alone or in conjunction with other parties) the subject matter claimed in the '619 patent. Should Apple obtain such evidence, it will provide the name of the person(s) from whom and the circumstances under which the invention or any part of it was derived, and/or the circumstances surrounding the making of the invention before the patent application.

Apple reserves the right to supplement these disclosures based on further investigation and discovery.

XII. THE ’029 PATENT

A. Patent Rule 3-3(a): Identification of Prior Art

At this time, Apple contends that at least each of the prior art references described and charted in **Exhibits 029-A and 029-B** anticipates or renders obvious, either alone or in combination, one or more of the Asserted Claims of the ’029 patent.

Additional prior art that has not been charted, but is still relevant to the invalidity of the ’029 patent is listed in **Exhibit C**, including without limitation as evidence of the state of the art at the alleged time of invention. Apple reserves the right to amend these invalidity contentions to assert these references depending on the claim construction and infringement positions SEVEN may take as the case proceeds. Moreover, Apple reserves the right to use these references in combination with other references to render the claims of the ’029 patent obvious in the event SEVEN takes the position that certain claim limitations are missing from the references charted in **Exhibits 029-A and 029-B**.

B. Patent Rule 3-3(b): Whether Each Item Anticipates or Renders Obvious the Asserted Claims

SEVEN asserts claims 1-24 of the ’029 patent against Apple in this lawsuit. These claims are invalid because the ’029 patent fails to meet one or more of the requirements for patentability. The individual bases for invalidity are provided below and in the claim charts attached as **Exhibits 029-A and 029-B**. Each of the foregoing listed prior art documents, the underlying work, and/or the underlying apparatus or method qualifies as prior art under one or more sections of 35 U.S.C. §§ 102 and/or 103.

Although Apple has identified at least one citation per limitation for each reference, each and every disclosure of the same limitation in the same reference is not necessarily identified. Rather, in an effort to focus the issues, Apple has cited representative portions of identified

references, even where a reference may contain additional support for a particular claim element. In addition, persons of ordinary skill in the art generally read a prior art reference as a whole and in the context of other publications and literature. Thus, to understand and interpret any specific statement or disclosure within a prior art reference, such persons would rely on other information within the reference, along with other publications and their general scientific knowledge. Apple may rely upon uncited portions of the prior art references and on other publications and expert testimony to provide context, and as aids to understanding and interpreting the portions that are cited. Apple may also rely on uncited portions of the prior art references, other disclosed publications, and the testimony of experts to establish that a person of ordinary skill in the art would have been motivated to modify or combine certain of the cited references so as to render the claims obvious.

1. Priority

SEVEN's Patent Rule 3-1(e) disclosures provide that the Asserted Claims of the '029 patent are entitled to a priority date of July 26, 2010, which is the filing date of U.S. Provisional Application Nos. 61/367,870 ("870 provisional application") and 61/367,871 ("871 provisional application").

Apple reserves the right to challenge SEVEN's assertion that the '029 patent is entitled to claim the benefit of these provisional applications' filing date to the extent that these provisional applications do not support the full scope of the Asserted Claims, for example, depending on scope of the Asserted Claims as properly construed. To the extent the provisional application does not support the full scope of the Asserted Claims, the priority date of the '029 patent should be no earlier than the filing date of the '029 patent's application, which is December 1, 2017.

SEVEN has provided no evidence to support its contention that the Asserted Claims of the '029 patent are entitled to claim priority back to this or any earlier filed application, and

Apple therefore reserves the right to assert a later priority date based on any findings as to the priority date of the Asserted Claims by the Court, information learned through discovery, or otherwise.

a) The Asserted Claims of the ’029 Patent Cannot Claim Priority to the ’870 or ’871 Provisional Applications

None of the Asserted Claims are entitled to the filing date of the ’870 or ’871 provisional applications (the earliest priority date claimed) because they do not have written description support in these provisional applications. *See, e.g., Falko-Gunter Falkner v. Inglis,* 448 F.3d 1357 (Fed. Cir. 2006). Significant portions of the ’871 provisional application were reproduced tin the specification of the ’056 patent, and for at least the reasons provided below in Apple’s contentions as to why the ’029 patent specification does not support the Asserted Claims, this provisional application likewise do not provide support for these claims. Furthermore, the ’870 provisional application, which names an inventor that does not appear on the face of the ’029 patent, also do not provide support for the Asserted Claims. For example, neither the ’870 or the ’871 provisional applications discuss “fetching data” over a “second connection” that is “other than” a multiplexed connection.

b) The Asserted Claims of the ’029 Patent Cannot Claim Priority to Any Other Provisional Application

The remaining provisional applications also do not provide support for the Asserted Claims. The majority of these provisional applications were purportedly invented by individuals who are not named as inventors to the ’029 patent. *See* Provisional Application Nos. 61/408,846; 61/408,854; 61/408,826; 61/416,020; 61/416,033; 61/430,828. The remaining provisional applications also do not provide support for the limitations discussed below in Apple’s written description and enablement contentions. *See* Provisional Application Nos. 61/408,820; 61/408,829; 61/408,839; 61/408,858.

2. Anticipation

Some or all of the Asserted Claims of the ’029 patent are invalid as anticipated under 35 U.S.C. § 102 in view of each of the prior art references identified above and in the claim charts included in **Exhibit 029-A**, which identify specific examples of where each limitation of the Asserted Claims is found in the prior art references. As explained above, the cited portions of prior art references identified in the attached claim charts are exemplary only and representative of the content and teaching of the prior art references, and should be understood in the context of the reference as a whole and as they would be understood by a person of ordinary skill in the art.

Apple identifies the following references as anticipating one or more of the Asserted Claims of the ’029 patent under 35 U.S.C. § 102. The below table of anticipating references is exemplary, and it does not constitute an admission that any reference anticipates only the listed claims. Further, Apple contends that any prior art reference in the attached charts that is charted for each limitation of any given claim, anticipates that claim, regardless of whether that prior art reference is listed in the following table.

Ex. #	Anticipating Prior Art	Claims
029-A1	U.S. Patent No. 8,359,290 to Muthuprasanna Muthusrinivasan (“Muthusrinivasan”)	Claims 1-24
029-A2	U.S. Patent No. 7,865,570 to Xian-He Sun (“Sun”)	Claims 1-24
029-A3	U.S. Patent Application No. 2011/0177774 to Binita Gupta et al. (“Gupta”)	Claims 1-24
029-A5	U.S. Patent No. 8,356,026 to Scott Heimendinger (“Heimendinger”)	Claims 1-24
029-A6	U.S. Patent Application No. 2006/0200849 to Prabakar Sundarrajan et al. (“Sundarrajan”)	Claims 1-24
029-A7	U.S. Published Patent Application No. 2005/0108075 to Fredrick Douglis et al. (“Douglis”)	Claims 1-24

To the extent any item of prior art cited above is deemed not to disclose, explicitly or inherently, any limitation of an Asserted Claim of the ’029 patent, Apple reserves the right to argue that any difference between that prior art and the corresponding patent claim would have

been either inherent to the art, or obvious to a person of ordinary skill in the art, even if Apple has not specifically denoted that the art is to be combined with the knowledge of a person of ordinary skill in the art.

3. Obviousness

To the extent any limitation is deemed not to be exactly met by an item of prior art listed above and in **Exhibit 029-A**, then any purported differences are such that the claimed subject matter as a whole would have been obvious to one skilled in the art at the time of the alleged invention, in view of the state of the art and knowledge of those skilled in the art. The item of prior art would, therefore, render the relevant claims invalid for obviousness under 35 U.S.C. § 103.

In addition, the references identified above render one or more Asserted Claims of the '029 patent obvious when the references are read in combination with each other, and/or when read in view of the state of the art and knowledge of those skilled in the art. Each and every reference identified is also relevant to the state of the art at the time of the alleged invention. Any of the references disclosed above may be combined with one another to render obvious (and therefore invalid) each of SEVEN's Asserted Claims. Apple may rely upon a subset of the above identified references or all of the references identified above, including all references in **Exhibits 029-A, 029-B, and C**, for purposes of obviousness depending on the Court's claim construction, positions taken by SEVEN during this litigation, and further investigation and discovery.

To the extent the foregoing references are found not to anticipate the Asserted Claims, the foregoing references render the Asserted Claims obvious either alone or in combination with one or more of the other references identified above pursuant to Patent Rule 3-3(a). It would have been obvious to a person of skill in the art at the time of the alleged invention of the

Asserted Claims of the ’029 patent to combine the various references cited herein so as to disclose the Asserted Claims of the ’029 patent.

In accordance with Patent Rule 3-3(b), prior art references rendering the Asserted Claims obvious, alone or in combination with other references, are outlined below and included in **Exhibits 029-A and 029-B**, which include exemplary claim charts for the Asserted Claims of the ’029 patent showing specifically where in each reference or combinations of references each Asserted Claim is found, and an explanation of why the prior art renders the Asserted Claim obvious. Where applicable, **Exhibits 029-A and 029-B** include the motivation to combine references.

Moreover, in addition to the information contained elsewhere in these contentions and in particular **Exhibit 029-B**, Apple has identified additional motivations and reasons to combine the various references cited herein. In particular, multiple teachings, suggestions, and/or reasons to modify any of the references and/or to combine any two or more of the references in **Exhibits 029-A and 029-B** come from many sources, including the prior art (specific and as a whole), common knowledge, common sense, predictability, expectations, industry trends, design incentives or need, market demand or pressure, market forces, obvious to try, the nature of the problem faced, and/or knowledge possessed by one of ordinary skill. In addition, it would have been obvious to try combining the prior art references identified above because there were only a finite number of predictable solutions and/or because known work in one field or endeavor prompted variations based on predictable design incentives and/or market forces either in the same field or a different one. The combination of prior art references identified in these contentions would have been obvious because the claimed combinations represent the known potential options with a reasonable expectation of success. Additionally, one of ordinary skill in

the art would have been motivated to create combinations identified in these contentions using: known methods to yield predictable results; known techniques in the same way; a simple substitution of one known, equivalent element for another to obtain predictable results; and/or teaching, suggestion, or motivation in the prior art generally. Also, market forces in the industry, and the desire to improve features and performance, would motivate the addition of features to systems as they become available, become less expensive, become more commonly used, provide better performance, reduce costs, size or weight, or predictably achieve other clearly desirable results.

While Apple reserves the right to rely on any combination of the references reflected in their charts or incorporated herein by reference, Apple provides the following exemplary and non-exhaustive references and/or combinations evidencing invalidity of the claims of the Asserted Patents. The combinations of prior art listed below render obvious the Asserted Claims under the proper construction of the claims and/or under Plaintiff's apparent interpretation of the claims as set forth by Plaintiff in their Complaint and Infringement Contentions. Each combination renders the identified claims obvious through the express and/or inherent disclosure in the combination of references themselves, as well as in view of the knowledge of a person of ordinary skill in the art.

Obviousness Combinations	**Claims**
Muthusrinivasan in view of Sun, Craig Hunt, "TCP/IP Network Administration" (2nd Edition) ("Hunt"), Heimendinger, Sundarrajan, Douglis, U.S. Published Patent Application No. 2016/0323775 to Michael Luna et al. ("Luna 775"), U.S. Patent No. 6,243,755 to Masahiro Takagi et al. ("Takagi"), U.S. Published Patent Application No. 2014/0366042 to David Michael Chan et. al. ("Chan"), Nokia E72 System, and/or Einarsson	Claims 1-24
Muthusrinivasan in view of Hunt	Claims 1-24
Muthusrinivasan in view of Gupta	Claims 1-24
Muthusrinivasan in view of Gupta and Hunt	Claims 1-24
Muthusrinivasan in view of Sundarrajan	Claims 1-24

Obviousness Combinations	Claims
Muthusrinivasan in view of Sundarrajan and Gupta	Claims 1-24
Muthusrinivasan in view of Sun, Gupta, and Hunt	Claims 1-24
Muthusrinivasan in view of Sundarrajan, Gupta, Hunt, and Sun	Claims 1-24
Muthusrinivasan in view of Sundarrajan, Gupta, Hunt, Einarsson, and Sun	Claims 1-24
Muthusrinivasan in view of Sundarrajan, Gupta, Hunt, Einarsson, Sun, and Takagi	Claims 1-24
Sun in view of Gupta	Claims 1-24
Sun in view of Gupta and Hunt	Claims 1-24
Sun in view of Muthusrinivasan, Gupta, and Hunt	Claims 1-24
Sun in view of Muthusrinivasan, Gupta, Hunt, Heimendinger, Sundarrajan, Douglis, Luna 775, Takagi, Chan, Nokia E72 System, and/or Einarsson	Claims 1-24
Heimendinger in view of Muthusrinivasan, Douglis, and Takagi	Claims 1-24
Heimendinger in view of Muthusrinivasan, Sun, Gupta, Hunt, Sundarrajan, Douglis, Luna 775, Takagi, Chan, Nokia E72 System, and/or Einarsson	Claims 1-24
Sundarrajan in view of Muthusrinivasan	Claims 1-24
Sundarrajan in view of Muthusrinivasan and Douglis	Claims 1-24
Sundarrajan in view of Takagi	Claims 1-24
Sundarrajan in view of Muthusrinivasan, Douglis, and Takagi	Claims 1-24
Sundarrajan in view of Muthusrinivasan, Douglis, and Einarsson	Claims 1-24
Sundarrajan in view of Muthusrinivasan, Douglis, Gupta, Takagi, and Einarsson	Claims 1-24
Sundarrajan in view of Muthusrinivasan, Sun, Gupta, Hunt, Heimendinger, Douglis, Luna 775, Takagi, Chan, Nokia E72 System, and/or Einarsson	Claims 1-24
Luna 775 in view of Muthusrinivasan	Claims 1-24
Luna 775 in view of Muthusrinivasan and Douglis	Claims 1-24
Luna 775 in view of Muthusrinivasan, Douglis, and Takagi	Claims 1-24
Luna 775 in view of Muthusrinivasan, Douglis, Takagi, and Einarrson	Claims 1-24
Luna 775 in view of Chan	Claims 1-24
Luna 775 in view of Muthusrinivasan, Sun, Gupta, Hunt, Heimendinger, Sundarrajan, Douglis, Takagi, Chan, Nokia E72 System, and/or Einarsson	Claims 1-24
Chan in view of Luna 775	Claims 1-24
Chan in view of Muthusrinivasan, Sun, Gupta, Hunt, Heimendinger, Sundarrajan, Douglis, Luna 775, Takagi, Nokia E72 System, and/or Einarsson	Claims 1-24
Nokia E72 System in view of Muthusrinivasan	Claims 1-24
Nokia E72 System in view of Hunt	Claims 1-24
Nokia E72 System in view of Gupta	Claims 1-24
Nokia E72 System in view of Sundarrajan	Claims 1-24

Obviousness Combinations	Claims
Nokia E72 System in view of Douglis	Claims 1-24
Nokia E72 System in view of Douglis, Einarsson, and Takagi	Claims 1-24
Nokia E72 System in view of Luna 775 and/or Chan	Claims 1-24
Nokia E72 System in view of Muthusrinivasan, Sun, Gupta, Hunt, Heimendinger, Sundarrajan, Douglis, Luna 775, Takagi, Chan, and/or Einarsson	Claims 1-24
Einarsson in view of Muthusrinivasan, Douglis, and Takagi	Claims 1-24
Einarsson in view of Muthusrinivasan, Sun, Gupta, Hunt, Heimendinger, Sundarrajan, Douglis, Luna 775, Takagi, Chan, and/or Nokia E72 System	Claims 1-24

In addition to the specific combinations of prior art and the specific combinations of groups of prior art disclosed above, Apple reserves the right to rely on any other combination of any prior art references disclosed herein. Apple further reserves the right to rely upon combinations disclosed within the prosecution history of the references cited herein. These obviousness combinations reflect Apple's present understanding of the potential scope of the claims that SEVEN appears to be advocating and should not be seen as Apple's acquiescence to SEVEN's interpretation of the patent claims.

Apple also reserves the right to amend or supplement these contentions regarding anticipation or obviousness of the Asserted Claims, in view of further information from SEVEN, information discovered during discovery, or a claim construction ruling by the Court. SEVEN has not identified what elements or combinations it alleges were not known to one of ordinary skill in the art at the time. Therefore, for any claim limitation that SEVEN alleges is not disclosed in a particular prior art reference, Apple reserves the right to assert that any such limitation is either inherent in the disclosed reference or obvious to one of ordinary skill in the art at the time in light of the same, or that the limitation is disclosed in another of the references disclosed above and in combination would have rendered the Asserted Claim obvious.

C. Patent Rule 3-3(c): Charts Identifying Where Specifically in Each Alleged Item of Prior Art Each Asserted Claim Is Found

Pursuant to Patent Rule 3-3(c), charts identifying where specifically in each alleged item of prior art each limitation of each Asserted Claim is found, including for each limitation that Apple contends is governed by 35 U.S.C. § 112(6), the identity of the structure(s), act(s), or material(s) in each item of prior art that performs the claimed function, are attached in **Exhibits 029-A and 029-B**.

D. Patent Rule 3-3(d): Other Grounds for Invalidity

Apple identifies the following grounds for invalidity of the Asserted Claims of the '029 patent based on 35 U.S.C. §§ 101 and/or 112. Apple reserves the right to supplement these disclosures based on further investigation and discovery.

1. Invalidity Pursuant to 35 U.S.C. § 112

Apple further asserts that the Asserted Claims of the '029 patent are invalid under 35 U.S.C. § 112. The following are the grounds upon which Apple contends the Asserted Claims are invalid for failure to meet the requirements of 35 U.S.C. § 112, ¶¶ 1, 2, 4 and/or 6, based on Apple's investigation to date and currently-available information.

For each claim identified as invalid, any dependent claims of those invalid claims are also invalid under 35 U.S.C. § 112, ¶¶ 1, 2, 4, and/or 6. Apple reserves the right to supplement and amend these contentions based on further discovery and investigation including, in particular, the deposition of any of the named inventors of the Asserted Patent, the parties' claim construction positions, and further investigation of SEVEN's implied infringement positions.

a) Written Description and/or Enablement

At least in view of SEVEN's apparent construction of the claims in its Infringement Contentions, the Asserted Claims of the '029 patent are invalid because the specification as filed

does not contain adequate written description of the claimed inventions sufficient to lead a person of ordinary skill in the art to understand that the named inventors had possession of the purported inventions as claimed as required by 35 U.S.C. § 112, ¶ 1. Likewise, the specification does not enable one of ordinary skill in the art to make or use the claimed inventions without undue experimentation. Based on Apple's present understanding of SEVEN's infringement contentions, Apple asserts that the Asserted Claims of the of the '029 patent are invalid for reciting at least the following claim terms/phrases/limitations:

Claims 1 and 12 of the '029 patent and their dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain an adequate written description and/or enabling disclosure of "fetching data" over a "second connection." The term "fetch" does not appear in the '029 patent specification. Rather, the term "prefetch" is used—only once—in the '029 patent specification, and is not described as an action that is carried out over a "connection," much less a connection that is "other than" an established multiplexed connection. Rather, the specification describes "prefetching" (and, by extension, "fetching") as an action that is carried out internally within the device *prior* to transmission. *See* '029 patent at 8:57-59 ("In some instances, the local proxy 175 can delay, expedite (prefetch), and/or modify data prior to transmission to the proxy server 125."). Accordingly, the specification fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

Claims 1 and 12 of the '029 patent and their dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain an adequate written description and/or enabling disclosure of "receiving a selection from

a user whether to enable an application for fetching" and/or "wherein the data is fetched if the fetching is enabled by the user selection for the application." Similarly claims 5 and 16 and their dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain an adequate written description and/or enabling disclosure of "fetching of the data can be enabled or disabled by a user selection such that fetching for multiple applications can be enabled or disabled by a single user selection." As discussed above, the '029 patent specification does not disclose "fetching" in the manner recited by the claims. Moreover, the specification does not disclose enabling or disabling fetching based on user selection. Accordingly, the specification fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

Claims 1 and 12 of the '029 patent and their dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain an adequate written description and/or enabling disclosure of "disconnecting from the second connection." The term "disconnect" appears once in the '029 patent specification and states only "[q]uiet time hours should not affect the calculation of entering power save mode. However we should still respect the quiet time hours and disconnect during them." '029 Patent at 39:32-35. The specification does not make clear that the mobile device's "processor" is configured to perform this disconnection (as required by claim 1) or that the specific connection that must be disconnected is the one over which data is allegedly fetched and different from the established multiplexed connection. Accordingly, the specification fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

Claims 7 and 18 of the ’029 patent are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain an adequate written description and/or enabling disclosure of “application behavior can be used by the mobile device to optimize traffic by aligning content requests by applications.” The term “content requests” appears nowhere else in the patent’s claims, and it is unclear whether “content requests by applications” refers to applications running on a mobile device, applications running on a server, or both. The patent provides no explanation as to what constitutes “application behavior” or how that behavior can be used for aligning. Furthermore, it is unclear what constitutes a mobile device that merely ***can*** use application behavior to align content requests. Accordingly, the specification fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

Claims 8 and 19 of the ’029 patent are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain an adequate written description and/or enabling disclosure of “data requests for multiple applications are aligned.” The term “data requests” appears nowhere else in the patent’s claims. Neither the patent’s specification nor claims provide an explanation as to what constitutes “data requests for multiple applications” or aligning such requests. For example, it is unclear whether this refers to applications running on a mobile device, applications running on a server, or both. As another example, it is unclear what constitutes a data request for ***multiple*** applications. As another example, it is unclear whether this claim language refers to a request generated by an application (e.g., an application running on a mobile device or an application running on a server) or whether this claim language refers to some aspect of the communication that somehow requests an

application itself. Accordingly, the specification fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

b) Indefiniteness

At least in view of SEVEN's apparent construction of the claims in its Infringement Contentions, the Asserted Claims of the '029 patent are invalid because they fail to particularly point out and distinctly claim the subject matter which the applicant regards as his invention under 35 U.S.C. § 112, ¶¶ 2, 4, and/or 6. Based on Apple's present understanding of SEVEN's infringement contentions, Apple asserts that the Asserted Claims of the of the '029 patent are invalid for reciting at least the following claim terms/phrases/limitations:

- Claim 1 of the '029 patent and its dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 2, ¶ 4, and/or ¶ 6 because these claims recite a "processor configured to" perform various steps. Based on SEVEN's infringement contentions, SEVEN asserts these claims against products that must be modified to include the accused features. For example, Apple's products, as sold, are in an "off" state and are thus their processors are not "configured" to perform steps such as receiving or transmitting messages. As another example, SEVEN appears to accuse functionality that is dependent upon how end users modify their devices, which applications end users install on their devices, how app developers program those applications (as running on mobile devices and as running on application servers). As such, one of ordinary skill would not understand the metes and bounds of the identified claims, rendering them indefinite under 35 U.S.C. § 112, ¶ 2. Therefore, the Asserted Claims, when read in light of the specification and the prosecution history, "fail to inform,

with reasonable certainty, those skilled in the art about the scope of the invention." *Nautilus, Inc. v. Biosig Instruments, Inc*., 134 S. Ct. 2120, 2124 (2014).

- Claims 1 and 12 of the '029 patent and their dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 2, ¶ 4, and/or ¶ 6 because the specification does not describe or otherwise inform one of ordinary skill as to the scope recited terms "fetching data for the application before the activity session" and "wherein the data is fetched if the fetching is enabled by the user selection." The first term requires that (as to claim 1) the processor is configured for fetching data and that (as to claim 12) data is fetched. However, the second term conflicts with the first, in that it requires that data is fetched *if* fetching is enabled. Relatedly, a person of ordinary skill in the art would not be reasonable certain as to the claim limitation of "receiving a selection from a user whether to enable an application for fetching." As such, one of ordinary skill would not understand the metes and bounds of the identified claims, rendering them indefinite under 35 U.S.C. § 112, ¶ 2. Therefore, the Asserted Claims, when read in light of the specification and the prosecution history, "fail to inform, with reasonable certainty, those skilled in the art about the scope of the invention." *Nautilus, Inc. v. Biosig Instruments, Inc*., 134 S. Ct. 2120, 2124 (2014).
- Claim 6 of the '029 patent and its dependent claim are invalid for failure to satisfy the requirements of 35 U.S.C. § 112 because the term "application behavior detector to track application behavior" is indefinite. Because this term, including in view of the claim, specification, and file history, does not connote sufficiently

definite structure, this term is governed by § 112, ¶ 6. In addition, the '029 patent specification does not describe or otherwise inform one of ordinary skill about a corresponding structure for performing the claimed function let alone clearly link such a structure to the claimed function. Accordingly, claim 6 of the '029 patent and its dependent claims are invalid as indefinite under 35 U.S.C. § 112, ¶ 2.

2. Other Grounds for Invalidity

In addition to the preceding invalidity contentions, Apple further contends that each of the Asserted Claims of the '029 patent is drawn to subject matter that is not patentable under 35 U.S.C. § 101. The '029 patent Asserted Claims are invalid under 35 U.S.C. § 101 for failure to recite patent eligible subject matter. Specifically, all claims of the '029 patent are fatally abstract under the U.S. Supreme Court's decision in *Alice Corp. v. CLS Bank Int'l,* 134 S. Ct. 2345 (2014) and progeny. The ideas presented in the claims are generally directed to predicting when a user will need data and proactively retrieving that data before the user needs it. Under *Alice* Step 1, those ideas are abstract, as they relate to a fundamental long prevalent practice. *See Intellectual Ventures I LLC v. Symantec Corp*., 838 F.3d 1307, 1314 (Fed. Cir. 2016). Limiting the invention to a particular technological environment, e.g. generic computer hardware, "do[es] not render an otherwise abstract concept any less abstract." *Intellectual Ventures I LLC v. Capital One Fin. Corp*., 850 F.3d 1332, 1340 (Fed Cir. 2017). Nor does limiting the invention such that data is retrieved over a connection that is "other than" another multiplexed connection—a requirement devoid of explanation in the patent specification. Furthermore, because the patent relates to transmission of information, it is likewise abstract, as "information is … an intangible." *Electric Power Group, LLC v. Alstom S.A.*, 830 F.3d 1350, 1353 (Fed. Cir. 2016). Furthermore, under *Alice* Step 2 the '029 patent does not contain any inventive concept. The '029 patent Asserted Claims employs well-known components or functionality, as shown in

Apple's invalidity contentions involving anticipation and/or obviousness in this case, which is not enough to impart patent eligibility of an abstract idea. *See, e.g., Alice,* 134 S. Ct. at 2359 (holding that limitations describing "'well-understood, routine, conventional activit[ies]' previously known to the industry" were insufficient to supply an inventive concept (quoting *Mayo*, 132 S. Ct. at 1294)). Further detail regarding Apple's contentions that the Asserted Claims of the '029 patent do not qualify as patent-eligible subject matter are contained in **Exhibit 029-D**.

Apple reserves the right to assert that the asserted patents are invalid under 35 U.S.C. §102(f) and/or (g) in the event Apple obtains evidence that the named inventors of the '029 patent did not invent (either alone or in conjunction with other parties) the subject matter claimed in the '029 patent. Should Apple obtain such evidence, it will provide the name of the person(s) from whom and the circumstances under which the invention or any part of it was derived, and/or the circumstances surrounding the making of the invention before the patent application.

Apple reserves the right to supplement these disclosures based on further investigation and discovery.

XIII. THE '734 PATENT

A. Patent Rule 3-3(a): Identification of Prior Art

At this time, Apple contends that at least each of the prior art references described and charted in **Exhibits 734-A and 734-B** anticipates or renders obvious, either alone or in combination, one or more of the Asserted Claims of the '734 patent.

Additional prior art that has not been charted, but is still relevant to the invalidity of the '734 patent is listed in **Exhibit C**, including without limitation as evidence of the state of the art at the alleged time of invention. Apple reserves the right to amend these invalidity contentions to assert these references depending on the claim construction and infringement positions

SEVEN may take as the case proceeds. Moreover, Apple reserves the right to use these references in combination with other references to render the claims of the '734 patent obvious in the event SEVEN takes the position that certain claim limitations are missing from the references charted in **Exhibits 734-A and 734-B**.

B. Patent Rule 3-3(b): Whether Each Item Anticipates or Renders Obvious the Asserted Claims

SEVEN asserts claims 1-14 of the '734 patent against Apple in this lawsuit. These claims are invalid because the '734 patent fails to meet one or more of the requirements for patentability. The individual bases for invalidity are provided below and in the claim charts attached as **Exhibits 734-A and 734-B.** Each of the foregoing listed prior art documents, the underlying work, and/or the underlying apparatus or method qualifies as prior art under one or more sections of 35 U.S.C. §§ 102 and/or 103.

Although Apple has identified at least one citation per limitation for each reference, each and every disclosure of the same limitation in the same reference is not necessarily identified. Rather, in an effort to focus the issues, Apple has cited representative portions of identified references, even where a reference may contain additional support for a particular claim element. In addition, persons of ordinary skill in the art generally read a prior art reference as a whole and in the context of other publications and literature. Thus, to understand and interpret any specific statement or disclosure within a prior art reference, such persons would rely on other information within the reference, along with other publications and their general scientific knowledge. Apple may rely upon uncited portions of the prior art references and on other publications and expert testimony to provide context, and as aids to understanding and interpreting the portions that are cited. Apple may also rely on uncited portions of the prior art references, other disclosed publications, and the testimony of experts to establish that a person of ordinary skill in the art

would have been motivated to modify or combine certain of the cited references so as to render the claims obvious.

1. Priority

SEVEN's Patent Rule 3-1(e) disclosures provide that the Asserted Claims of the '734 patent are entitled to a priority date of July 26, 2010, which is the filing date of U.S. Provisional Application Nos. 61/367,870 and 61/367,871.

Apple reserves the right to challenge SEVEN's assertion that the '734 patent is entitled to claim the benefit of these provisional applications' filing date to the extent that these provisional applications do not support the full scope of the Asserted Claims, for example, depending on scope of the Asserted Claims as properly construed. To the extent the provisional application does not support the full scope of the Asserted Claims, the priority date of the '734 patent should be no earlier than the filing date of '734 patent's application, which is May 15, 2017.

SEVEN has provided no evidence to support its contention that the Asserted Claims of the '734 patent are entitled to claim priority back to this or any earlier filed application, and Apple therefore reserves the right to assert a later priority date based on any findings as to the priority date of the Asserted Claims by the Court, information learned through discovery, or otherwise.

a) The Asserted Claims of the '734 Patent Cannot Claim Priority to the '870 or '871 Provisionals

None of the Asserted Claims are entitled to the filing date of the '870 or '871 Provisionals (the earliest priority date claimed) because they do not have written description support in these provisional applications. *See Falko-Gunter Falkner v. Inglis,* 448 F.3d 1357 (Fed. Cir. 2006). At least for the reasons provided below in Apple's contentions as to why the '734 patent specification does not support the Asserted Claims, these provisional applications

likewise do not provide support for these claims. For example, neither the '870 or the '871 provisional applications discuss the various recited rules of the asserted claims that govern the mobile device's processor while "in the power save mode" versus the various recited rules that apply "when the power save mode is exited."

b) The Asserted Claims of the '734 Patent Cannot Claim Priority to Any Other Provisional

The remaining provisional applications also do not provide support for the Asserted Claims. The majority of these provisional applications were purportedly invented by individuals who are not named as inventors to the '734 patent. *See* Provisional Application Nos. 61/408,839; 61/408,846; 61/408,854; 61/408,826; 61/416,020; 61/416,033; 61/430,828. The remaining provisional applications also do not provide support for the limitations discussed below in Apple's written description and enablement contentions. *See* Provisional Application Nos. 61/408,820; 61/408,829; 61/408,858.

2. Anticipation

Some or all of the Asserted Claims of the '734 patent are invalid as anticipated under 35 U.S.C. § 102 in view of each of the prior art references identified above and in the claim charts included in **Exhibit 734-A**, which identify specific examples of where each limitation of the Asserted Claims is found in the prior art references. As explained above, the cited portions of prior art references identified in the attached claim charts are exemplary only and representative of the content and teaching of the prior art references, and should be understood in the context of the reference as a whole and as they would be understood by a person of ordinary skill in the art.

Apple identifies the following references as anticipating one or more of the Asserted Claims of the '734 patent under 35 U.S.C. § 102. The below table of anticipating references is exemplary, and it does not constitute an admission that any reference anticipates only the listed

claims. Further, Apple contends that any prior art reference in the attached charts that is charted for each limitation of any given claim, anticipates that claim, regardless of whether that prior art reference is listed in the following table.

Ex. #	Anticipating Prior Art	Claims
734-A01	U.S. Patent No. 10,091,734 to Bear ("Bear")	Claims 1-14
734-A02	U.S. Patent No. 8,620,344 to Huang ("Huang")	Claims 1-14
734-A03	Nokia E72 System	Claims 1-14
734-A05	U.S. Published Patent Application No. 2006/0200849 to Prabakar Sundarrajan et al. ("Sundarrajan")	Claims 1-14
734-A08	U.S. Patent No. 8,904,206 to Gregory R. Black et al. ("Black 206")	Claims 1-14
734-A09	U.S. Published Patent Application No. 2009/0307696 to Angelo Vals et al. ("Vals")	Claims 1-14
734-A10	U.S. Published Patent Application No. 2009/0217065 to Nelson S. Araujo ("Araujo")	Claims 1-14

To the extent any item of prior art cited above is deemed not to disclose, explicitly or inherently, any limitation of an Asserted Claim of the '734 patent, Apple reserves the right to argue that any difference between that prior art and the corresponding patent claim would have been either inherent to the art, or obvious to a person of ordinary skill in the art, even if Apple has not specifically denoted that the art is to be combined with the knowledge of a person of ordinary skill in the art.

3. Obviousness

To the extent any limitation is deemed not to be exactly met by an item of prior art listed above and in **Exhibit 734-A**, then any purported differences are such that the claimed subject matter as a whole would have been obvious to one skilled in the art at the time of the alleged invention, in view of the state of the art and knowledge of those skilled in the art. The item of prior art would, therefore, render the relevant claims invalid for obviousness under 35 U.S.C. § 103.

In addition, the references identified above render one or more Asserted Claims of the '734 patent obvious when the references are read in combination with each other, and/or when read in view of the state of the art and knowledge of those skilled in the art. Each and every reference identified is also relevant to the state of the art at the time of the alleged invention. Any of the references disclosed above may be combined with one another to render obvious (and therefore invalid) each of SEVEN's Asserted Claims. Apple may rely upon a subset of the above identified references or all of the references identified above, including all references in **Exhibits 734-A, 734-B, and C**, for purposes of obviousness depending on the Court's claim construction, positions taken by SEVEN during this litigation, and further investigation and discovery.

To the extent the foregoing references are found not to anticipate the Asserted Claims, the foregoing references render the Asserted Claims obvious either alone or in combination with one or more of the other references identified above pursuant to Patent Rule 3-3(a). It would have been obvious to a person of skill in the art at the time of the alleged invention of the Asserted Claims of the '734 patent to combine the various references cited herein so as to disclose the Asserted Claims of the '734 patent.

In accordance with Patent Rule 3-3(b), prior art references rendering the Asserted Claims obvious, alone or in combination with other references, are outlined below and included in **Exhibits 734-A and 734-B**, which include exemplary claim charts for the Asserted Claims of the '734 patent showing specifically where in each reference or combinations of references each Asserted Claim is found, and an explanation of why the prior art renders the Asserted Claim obvious. Where applicable, **Exhibits 734-A and 734-B** include the motivation to combine references.

Moreover, in addition to the information contained elsewhere in these contentions and in particular **Exhibit 734-B**, Apple has identified additional motivations and reasons to combine the various references cited herein. In particular, multiple teachings, suggestions, and/or reasons to modify any of the references and/or to combine any two or more of the references in **Exhibits 734-A and 734-B** come from many sources, including the prior art (specific and as a whole), common knowledge, common sense, predictability, expectations, industry trends, design incentives or need, market demand or pressure, market forces, obvious to try, the nature of the problem faced, and/or knowledge possessed by one of ordinary skill. In addition, it would have been obvious to try combining the prior art references identified above because there were only a finite number of predictable solutions and/or because known work in one field or endeavor prompted variations based on predictable design incentives and/or market forces either in the same field or a different one. The combination of prior art references identified in these contentions would have been obvious because the claimed combinations represent the known potential options with a reasonable expectation of success. Additionally, one of ordinary skill in the art would have been motivated to create combinations identified in these contentions using: known methods to yield predictable results; known techniques in the same way; a simple substitution of one known, equivalent element for another to obtain predictable results; and/or teaching, suggestion, or motivation in the prior art generally. Also, market forces in the industry, and the desire to improve features and performance, would motivate the addition of features to systems as they become available, become less expensive, become more commonly used, provide better performance, reduce costs, size or weight, or predictably achieve other clearly desirable results.

While Apple reserves the right to rely on any combination of the references reflected in their charts or incorporated herein by reference, Apple provides the following exemplary and non-exhaustive references and/or combinations evidencing invalidity of the claims of the Asserted Patents. The combinations of prior art listed below render obvious the Asserted Claims under the proper construction of the claims and/or under Plaintiff's apparent interpretation of the claims as set forth by Plaintiff in their Complaint and Infringement Contentions. Each combination renders the identified claims obvious through the express and/or inherent disclosure in the combination of references themselves, as well as in view of the knowledge of a person of ordinary skill in the art.

Obviousness Combinations	Claims
Bear in view of Huang, Nokia E72 System, Oestvall, Sundarrajan, Araujo, Douglis, Calamera, Vals, Luna 941, and/or Black 206	Claims 1-14
Huang in view of Bear, Nokia E72 System, Oestvall, Douglis, Calamera, Luna 941, Vals, Sundarrajan, Araujo, and/or Black 206	Claims 1-14
Nokia E72 System in view of Oestvall, Bear, Black 206, Luna 941, Sundarrajan, Araujo, Vals, Douglis, Calamera, and/or Huang	Claims 1-14
Sundarrajan in view of Nokia E72 System, Oestvall, Bear, Huang, Douglis, Calamera, Vals, Araujo, Luna 941, and/or Black 206	Claims 1-14
Black 206 in view of Nokia E72 System, Oestvall, Sundarrajan, Bear, Douglis, Calamera, Araujo, Vals, Luna 941, and/or Black 206	Claims 1-14
Vals in view of Araujo, Oestvall, Nokia E72 System, Sundarrajan, Bear, Huang, Douglis, Calamera, Luna 941, and/or Black 206	Claims 1-14
Araujo in view of Oestvall, Nokia E72 System, Sundarrajan, Bear, Huang, Douglis, Calamera, Vals, Luna 941, and/or Black 206	Claims 1-14
Luna 941 in view of Oestvall, Nokia E72 System, Sundarrajan, Bear, Huang, Douglis, Calamera, Vals, Araujo and/or Black 206	Claims 1-14

In addition to the specific combinations of prior art and the specific combinations of groups of prior art disclosed above, Apple reserves the right to rely on any other combination of

any prior art references disclosed herein. Apple further reserves the right to rely upon combinations disclosed within the prosecution history of the references cited herein. These obviousness combinations reflect Apple's present understanding of the potential scope of the claims that SEVEN appears to be advocating and should not be seen as Apple's acquiescence to SEVEN's interpretation of the patent claims.

Apple also reserves the right to amend or supplement these contentions regarding anticipation or obviousness of the Asserted Claims, in view of further information from SEVEN, information discovered during discovery, or a claim construction ruling by the Court. SEVEN has not identified what elements or combinations it alleges were not known to one of ordinary skill in the art at the time. Therefore, for any claim limitation that SEVEN alleges is not disclosed in a particular prior art reference, Apple reserves the right to assert that any such limitation is either inherent in the disclosed reference or obvious to one of ordinary skill in the art at the time in light of the same, or that the limitation is disclosed in another of the references disclosed above and in combination would have rendered the Asserted Claim obvious.

C. Patent Rule 3-3(c): Charts Identifying Where Specifically in Each Alleged Item of Prior Art Each Asserted Claim Is Found

Pursuant to Patent Rule 3-3(c), charts identifying where specifically in each alleged item of prior art each limitation of each Asserted Claim is found, including for each limitation that Apple contends is governed by 35 U.S.C. § 112(6), the identity of the structure(s), act(s), or material(s) in each item of prior art that performs the claimed function, are attached in **Exhibits 734-A and 734-B**.

D. Patent Rule 3-3(d): Other Grounds for Invalidity

Apple identifies the following grounds for invalidity of the Asserted Claims of the '734 patent based on 35 U.S.C. §§ 101 and/or 112. Apple reserves the right to supplement these disclosures based on further investigation and discovery.

1. Invalidity Pursuant to 35 U.S.C. § 112

Apple further asserts that the Asserted Claims of the '734 patent are invalid under 35 U.S.C. § 112. The following are the grounds upon which Apple contends the Asserted Claims are invalid for failure to meet the requirements of 35 U.S.C. § 112, ¶¶ 1, 2, 4 and/or 6, based on Apple's investigation to date and currently-available information.

For each claim identified as invalid, any dependent claims of those invalid claims are also invalid under 35 U.S.C. § 112, ¶¶ 1, 2, 4, and/or 6. Apple reserves the right to supplement and amend these contentions based on further discovery and investigation including, in particular, the deposition of any of the named inventors of the Asserted Patent, the parties' claim construction positions, and further investigation of SEVEN's implied infringement positions.

a) Written Description and/or Enablement

At least in view of SEVEN's apparent construction of the claims in its Infringement Contentions, the Asserted Claims of the '734 patent are invalid because the specification as filed does not contain adequate written description of the claimed inventions sufficient to lead a person of ordinary skill in the art to understand that the named inventors had possession of the purported inventions as claimed as required by 35 U.S.C. § 112, ¶ 1. Likewise, the specification does not enable one of ordinary skill in the art to make or use the claimed inventions without undue experimentation. Based on Apple's present understanding of SEVEN's infringement contentions, Apple asserts that the Asserted Claims of the of the '734 patent are invalid for reciting at least the following claim terms/phrases/limitations:

Claims 1 and 9 of the ’734 patent and their dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain an adequate written description and/or enabling disclosure of the various rules that must govern the mobile device’s processor while “in the power save mode” versus the various rules that apply “when the power save mode is exited.” Rather, to the extent these rules find any support in the patent specification at all, they appear to be randomly selected from disparate sections of the patent describing the behavior of the device in various contexts. The patent does not specify which of these behaviors would apply while “in” a power save mode versus when the device is “out” of the power save mode. Accordingly, the specification fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

Claims 1 and 9 of the ’734 patent and their dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain an adequate written description and/or enabling disclosure of “receiv[ing] instructions from a user to enter a power save mode” and/or “exit[ing] the power save mode based on received instructions from the user to exit the power save mode.” At best, the specification discloses turning power save mode on or off “via a user interface.” *See* ’734 Patent at 37:21-23. However, the specification does not specify that was is provided through this user interface are “instructions from a user to [enter]/[exit] the power save mode.” Accordingly, the specification fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

Claims 1 and 9 of the ’734 patent and their dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain an adequate written description and/or enabling disclosure of blocking “outgoing application data requests” “by user selection on an application-by-application basis.” The patent specification generally does not describe “blocking” outgoing data requests, much less enabling a user to select apps to block on an app-specific basis. Accordingly, the specification fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

Claims 4 and 12 of the ’734 patent are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain an adequate written description and/or enabling disclosure of entering into a “power save mode” based on “battery level.” Accordingly, the specification fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

b) Indefiniteness

At least in view of SEVEN’s apparent construction of the claims in its Infringement Contentions, the Asserted Claims of the ’734 patent are invalid because they fail to particularly point out and distinctly claim the subject matter which the applicant regards as his invention under 35 U.S.C. § 112, ¶¶ 2, 4, and/or 6. Based on Apple’s present understanding of SEVEN’s infringement contentions, Apple asserts that the Asserted Claims of the of the ’734 patent are invalid for reciting at least the following claim terms/phrases/limitations:

- Claims 1 and 9 of the ’734 patent and their dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 2, ¶ 4, and/or ¶ 6 because

the specification does not describe or otherwise inform one of ordinary skill about what constitutes "background status," or "foreground application requests." The patent does not specify how one distinguishes between "background" applications (as opposed to foreground applications) or "foreground" requests (as opposed to background requests). As such, one of ordinary skill would not understand the metes and bounds of the identified claims, rendering them indefinite under 35 U.S.C. § 112, ¶ 2. Therefore, these claims, when read in light of the specification and the prosecution history, "fail to inform, with reasonable certainty, those skilled in the art about the scope of the invention." *Nautilus, Inc. v. Biosig Instruments, Inc*., 134 S. Ct. 2120, 2124 (2014).

- Claims 1 and 9 of the '734 patent and their dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 2, ¶ 4, and/or ¶ 6 because the specification does not describe or otherwise inform one of ordinary skill about what constitutes "additional outgoing application data requests" or "the outgoing application data requests occurring while the mobile device is not in the power save mode." As to the first recited instance of outgoing application data requests, it is unclear in what way these requests are "additional." As to the second instance of outgoing application data requests, it is unclear whether this claim language refers to the first instance of outgoing application data requests or some other, previously unspecified data requests. As such, one of ordinary skill would not understand the metes and bounds of the identified claims, rendering them indefinite under 35 U.S.C. § 112, ¶ 2. Therefore, these claims, when read in light of the specification and the prosecution history, "fail to inform, with reasonable

certainty, those skilled in the art about the scope of the invention." *Nautilus, Inc. v. Biosig Instruments, Inc.*, 134 S. Ct. 2120, 2124 (2014).

- Claims 1 and 9 of the '734 patent and their dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 2, ¶ 4, and/or ¶ 6 because the specification does clarify the requirement that "additional outgoing application data requests" are allowed "in response to occurrence of [1] receipt of data transfer from a remote entity [and] [2] user input in response to a prompt displayed to the user, and [3] a change in a background status of an application executing on the mobile device." It is unclear whether this patent claim requires that all three conditions must exist to allow outgoing data requests, whether only one condition is required to allow outgoing data requests, or whether any of these conditions must "trigger" any of the other conditions or be otherwise related. Furthermore, it is unclear whether these condition(s) must allow ***all*** outgoing foreground application data requests or merely ***some*** outgoing foreground application data requests. As to the second instance of outgoing application data requests, it is unclear whether this claim language refers to the first instance of outgoing application data requests or some other, previously unspecified data requests. As such, one of ordinary skill would not understand the metes and bounds of the identified claims, rendering them indefinite under 35 U.S.C. § 112, ¶ 2. Therefore, these claims, when read in light of the specification and the prosecution history, "fail to inform, with reasonable certainty, those skilled in the art about the scope of the invention." *Nautilus, Inc. v. Biosig Instruments, Inc.*, 134 S. Ct. 2120, 2124 (2014).

- Claim 1 of the ’734 patent and its dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 2, ¶ 4, and/or ¶ 6 because these claims recite a “processor . . . configured to” perform various steps and include various features. Based on SEVEN’s infringement contentions, SEVEN asserts these claims against products that must be modified to include the accused features. For example, Apple’s products, as sold, are in an “off” state and are thus not “configured” to perform steps such as receiving or transmitting messages. As another example, SEVEN appears to accuse functionality that is dependent upon how end users modify their devices, which applications end users install on their devices, how app developers program those applications (as running on mobile devices and as running on application servers). As such, one of ordinary skill would not understand the metes and bounds of the identified claims, rendering them indefinite under 35 U.S.C. § 112, ¶ 2. Therefore, these claims, when read in light of the specification and the prosecution history, “fail to inform, with reasonable certainty, those skilled in the art about the scope of the invention.” *Nautilus, Inc. v. Biosig Instruments, Inc*., 134 S. Ct. 2120, 2124 (2014).

2. Other Grounds for Invalidity

In addition to the preceding invalidity contentions, Apple further contends that each of the Asserted Claims of the ’734 patent is drawn to subject matter that is not patentable under 35 U.S.C. § 101. The ’734 patent Asserted Claims are invalid under 35 U.S.C. § 101 for failure to recite patent eligible subject matter. Specifically, all claims of the ’734 patent are fatally abstract under the U.S. Supreme Court’s decision in *Alice Corp. v. CLS Bank Int’l,* 134 S. Ct. 2345 (2014) and progeny. The ideas presented in the claims are generally directed to concept of blocking some data requests for some applications while at the same time allowing that mobile

device to receive data. Under *Alice* Step 1, those ideas are abstract, as they relate to a fundamental long prevalent practice. *See Intellectual Ventures I LLC v. Symantec Corp*., 838 F.3d 1307, 1314 (Fed. Cir. 2016). Limiting the invention to a particular technological environment, e.g. generic computer hardware, "do[es] not render an otherwise abstract concept any less abstract." *Intellectual Ventures I LLC v. Capital One Fin. Corp*., 850 F.3d 1332, 1340 (Fed Cir. 2017). Furthermore, because the patent relates to transmission of information (i.e., generic "data" or "messages"), it is likewise abstract, as "information is … an intangible." *Electric Power Group, LLC v. Alstom S.A.*, 830 F.3d 1350, 1353 (Fed. Cir. 2016). Furthermore, under *Alice* Step 2 the '734 patent does not contain any inventive concept. The '734 patent Asserted Claims employs well-known components or functionality, as shown in Apple's invalidity contentions involving anticipation and/or obviousness in this case, which is not enough to impart patent eligibility of an abstract idea. *See, e.g., Alice*, 134 S. Ct. at 2359 (holding that limitations describing "'well-understood, routine, conventional activit[ies]' previously known to the industry" were insufficient to supply an inventive concept (quoting *Mayo*, 132 S. Ct. at 1294)). Further detail regarding Apple's contentions that the Asserted Claims of the '734 patent do not qualify as patent-eligible subject matter are contained in **Exhibit 734-D**.

Apple reserves the right to assert that the asserted patents are invalid under 35 U.S.C. §102(f) and/or (g) in the event Apple obtains evidence that the named inventors of the '734 patent did not invent (either alone or in conjunction with other parties) the subject matter claimed in the '734 patent. Should Apple obtain such evidence, it will provide the name of the person(s) from whom and the circumstances under which the invention or any part of it was derived, and/or the circumstances surrounding the making of the invention before the patent application.

Apple reserves the right to supplement these disclosures based on further investigation and discovery.

XIV. THE '534 PATENT

A. Patent Rule 3-3(a): Identification of Prior Art

At this time, Apple contends that at least each of the prior art references described and charted in **Exhibits 534-A and 534-B** anticipates or renders obvious, either alone or in combination, one or more of the Asserted Claims of the '534 patent.

Additional prior art that has not been charted, but is still relevant to the invalidity of the '534 patent is listed in **Exhibit C**, including without limitation as evidence of the state of the art at the alleged time of invention. Apple reserves the right to amend these invalidity contentions to assert these references depending on the claim construction and infringement positions SEVEN may take as the case proceeds. Moreover, Apple reserves the right to use these references in combination with other references to render the claims of the '534 patent obvious in the event SEVEN takes the position that certain claim limitations are missing from the references charted in **Exhibits 534A – 534B**.

B. Patent Rule 3-3(b): Whether Each Item Anticipates or Renders Obvious the Asserted Claims

SEVEN asserts claims 1-20 the '534 patent against Apple in this lawsuit. These claims are invalid because the '534 patent fails to meet one or more of the requirements for patentability. The individual bases for invalidity are provided below and in the claim charts attached as **Exhibits 534-A and 534-B**. Each of the foregoing listed prior art documents, the underlying work, and/or the underlying apparatus or method qualifies as prior art under one or more sections of 35 U.S.C. §§ 102 and/or 103.

Although Apple has identified at least one citation per limitation for each reference, each and every disclosure of the same limitation in the same reference is not necessarily identified. Rather, in an effort to focus the issues, Apple has cited representative portions of identified references, even where a reference may contain additional support for a particular claim element. In addition, persons of ordinary skill in the art generally read a prior art reference as a whole and in the context of other publications and literature. Thus, to understand and interpret any specific statement or disclosure within a prior art reference, such persons would rely on other information within the reference, along with other publications and their general scientific knowledge. Apple may rely upon uncited portions of the prior art references and on other publications and expert testimony to provide context, and as aids to understanding and interpreting the portions that are cited. Apple may also rely on uncited portions of the prior art references, other disclosed publications, and the testimony of experts to establish that a person of ordinary skill in the art would have been motivated to modify or combine certain of the cited references so as to render the claims obvious.

1. Priority

SEVEN's Patent Rule 3-1(e) disclosures provide that the Asserted Claims of the '534 patent are entitled to a priority date of January 8, 2002, which is the filing date of U.S. Provisional Application No. 60/346,881. SEVEN's Patent Rule 3-1(e) disclosures also provide that the Asserted Claims of the '534 patent claim the benefit of U.S. Provisional Application No. 60/403,249, filed August 12, 2002. SEVEN has provided no evidence to support its contention that the Asserted Claims of the '534 patent are entitled to claim priority back to this or any earlier filed application, and Apple therefore reserves the right to assert a later priority date based on any findings as to the priority date of the Asserted Claims by the Court, information learned through discovery, or otherwise.

Apple reserves the right to challenge SEVEN's assertion that the '534 patent is entitled to claim the benefit of the filing dates of U.S. Provisional Application Nos. 60/346,881 and 60/403,249 to the extent that these provisional applications do not support the full scope of the Asserted Claims, for example, depending on scope of the Asserted Claims as properly construed. To the extent the provisional applications do not support the full scope of the Asserted Claims, the priority date of the '534 patent should be the filing date of the first non-provisional patent application to which the '534 patent claims priority, which is January 8, 2003. Additionally, to the extent the non-provisional patent applications to which the '534 patent claim priority do not support the full scope of the Asserted Claims, the priority date of the '534 patent should be the filing date of the patent application for the '534 patent, which is October 28, 2016.

The provisional application must "contain a written description of the invention and the manner and process of making and using it, in such full, clear, concise, and exact terms," 35 U.S.C. § 112 ¶ 1, to enable a POSITA to practice the invention claimed in the non-provisional application. *Id*.

a) The Asserted Claims of the '534 Patent Cannot Claim Priority to the '534 Provisionals

None of the Asserted Claims are entitled to the filing dates of U.S. Provisional Application Nos. 60/346,881 and/or 60/403,249 ("the '534 Provisionals") because they do not have written description support in the '534 Provisionals. *See Falko-Gunter Falkner v. Inglis*, 448 F.3d 1357 (Fed. Cir. 2006).

The Asserted Claims are not entitled to the '534 Provisionals filing date(s) because the '534 Provisionals do not actually or inherently disclose each and every claim element. *PowerOasis, Inc. v. T-Mobile USA, Inc*., 522 F.3d 1299, 1306-07 (Fed. Cir. 2008).

None of the Asserted Claims are disclosed in the ’534 Provisionals. The Asserted Claims use abstract terminology that does not exist in the ‘534 Provisionals. For example, the Asserted Claims recite the following terms: (1) “first device;” (2) “second device;” (3) “first connection;” (4) “second connection;” (5) “first message;” (6) “second message;” (7) “third message;” and/or (8) “fourth message.”

SEVEN has failed to identify where these terms are found in the ’534 Provisionals. For example, SEVEN fails to explain in the ’534 Provisionals which devices referred to within them are the “first device” versus the “second device,” which connections are the “first connection” versus the “second connection,” or and which “messages” are the first, second, third and/or fourth “messages.” Apple sees no relevant disclosures of these terms and the distinctions between them in the ’534 Provisionals. The claims additionally define the relationship between these abstract terms, for example, requiring receiving a “first connection” associated with a “first device,” receiving a “first message” from the “first device” over the “first connection,” and so on. Because Apple is not aware of how SEVEN maps the Asserted Claims to the ’534 Provisionals, Apple is unable to provide further rebuttal until SEVEN sets forth its theory with respect to each of limitation of the Asserted Claims.

Furthermore, the ’534 patent uses generic terminology that could refer to multiple different things within the ’534 Provisionals. For example, the claimed “processor” and “memory” could refer to components used in the Slingshot Connection Server, the chipset used in the user’s PC, or the Slingshot Connection Client. Irrespective of which of these devices SEVEN maps to, however, the ’534 Provisionals do not disclose a “processor” or “memory” that satisfies the other steps of the claim.

For example, the ’534 Provisionals refer to the Slingshot system, but the Slingshot system does not support the claimed features. In some instances, such as with respect to the limitations requiring the generation of a second message for a second device based on the first message from the first device, wherein the second message is sent to the second device, the disclosure concerning the Slingshot system does not provide the necessary level of detail to determine that this limitation is satisfied. In other instances, the disclosure of the Slingshot system teaches away from the claimed invention (*e.g.*, U.S. Provisional Application Nos. 60/346,881, SEVEN Slingshot Architecture Plan at p. 4-5 (referring to a single connection being used for multiple events, whereas the claim requires using different connections)).

Consequently, neither the ’534 Provisionals do not actually or inherently disclose each and every element of the ’534 Asserted Claims. The introduction of these features into the claims result in the ’534 patent claims not being entitled to the filing date of the provisional applications.

2. Anticipation

Some or all of the Asserted Claims of the ’534 patent are invalid as anticipated under 35 U.S.C. § 102 in view of each of the prior art references identified above and in the claim charts included in **Exhibit 534-A**, which identify specific examples of where each limitation of the Asserted Claims is found in the prior art references. As explained above, the cited portions of prior art references identified in the attached claim charts are exemplary only and representative of the content and teaching of the prior art references, and should be understood in the context of the reference as a whole and as they would be understood by a person of ordinary skill in the art.

Apple identifies the following references as anticipating one or more of the Asserted Claims of the ’534 patent under 35 U.S.C. § 102. The below table of anticipating references is exemplary, and it does not constitute an admission that any reference anticipates only the listed

claims. Further, Apple contends that any prior art reference in the attached charts that is charted for each limitation of any given claim, anticipates that claim, regardless of whether that prior art reference is listed in the following table.

Exhibit No.	Anticipating Prior Art	Claims
534-A01	U.S. Patent No. 6,138,158 to Boyle et al. ("Boyle")	1-2, 4-6, 8-10, 11-12, 14-16, 18-20
534-A02	U.S. Patent Application Publication No. 2002/0038371 to Spacey ("Spacey")	2-3, 5-6, 8-10, 12-13, 15-16, 18-20
534-A03	U.S. Patent No. 8,326,940 to Yamamoto et al. ("Yamamoto")	2, 5-6, 9-10, 12, 15-16, 19-20
534-A04	Microsoft Pocket PC System	1-20

To the extent any item of prior art cited above is deemed not to disclose, explicitly or inherently, any limitation of an Asserted Claim of the '534 patent, Apple reserves the right to argue that any difference between that prior art and the corresponding patent claim would have been either inherent to the art, or obvious to a person of ordinary skill in the art, even if Apple has not specifically denoted that the art is to be combined with the knowledge of a person of ordinary skill in the art.

3. Obviousness

To the extent any limitation is deemed not to be exactly met by an item of prior art listed above and in **Exhibit 534-A**, then any purported differences are such that the claimed subject matter as a whole would have been obvious to one skilled in the art at the time of the alleged invention, in view of the state of the art and knowledge of those skilled in the art. The item of prior art would, therefore, render the relevant claims invalid for obviousness under 35 U.S.C. § 103.

In addition, the references identified above render one or more Asserted Claims of the '534 patent obvious when the references are read in combination with each other, and/or when

read in view of the state of the art and knowledge of those skilled in the art. Each and every reference identified is also relevant to the state of the art at the time of the alleged invention. Any of the references disclosed above may be combined with one another to render obvious (and therefore invalid) each of SEVEN's Asserted Claims. Apple may rely upon a subset of the above identified references or all of the references identified above, including all references in **Exhibits 534-A, 534-B, and C**, for purposes of obviousness depending on the Court's claim construction, positions taken by SEVEN during this litigation, and further investigation and discovery.

To the extent the foregoing references are found not to anticipate the Asserted Claims, the foregoing references render the Asserted Claims obvious either alone or in combination with one or more of the other references identified above pursuant to Patent Rule 3-3(a). It would have been obvious to a person of skill in the art at the time of the alleged invention of the Asserted Claims of the '534 patent to combine the various references cited herein so as to disclose the Asserted Claims of the '534 patent.

In accordance with Patent Rule 3-3(b), prior art references rendering the Asserted Claims obvious, alone or in combination with other references, are outlined below and included in **Exhibits 534-A and 534-B**, which include exemplary claim charts for the Asserted Claims of the '534 patent showing specifically where in each reference or combinations of references each Asserted Claim is found, and an explanation of why the prior art renders the Asserted Claim obvious. Where applicable, **Exhibits 534-A and 534-B** include the motivation to combine references.

Moreover, in addition to the information contained elsewhere in these contentions and in particular **Exhibit 539-B**, Apple has identified additional motivations and reasons to combine the

various references cited herein. In particular, multiple teachings, suggestions, and/or reasons to modify any of the references and/or to combine any two or more of the references in **Exhibits 534-A and 534-B** come from many sources, including the prior art (specific and as a whole), common knowledge, common sense, predictability, expectations, industry trends, design incentives or need, market demand or pressure, market forces, obvious to try, the nature of the problem faced, and/or knowledge possessed by one of ordinary skill. In addition, it would have been obvious to try combining the prior art references identified above because there were only a finite number of predictable solutions and/or because known work in one field or endeavor prompted variations based on predictable design incentives and/or market forces either in the same field or a different one. The combination of prior art references identified in these contentions would have been obvious because the claimed combinations represent the known potential options with a reasonable expectation of success. Additionally, one of ordinary skill in the art would have been motivated to create combinations identified in these contentions using: known methods to yield predictable results; known techniques in the same way; a simple substitution of one known, equivalent element for another to obtain predictable results; and/or teaching, suggestion, or motivation in the prior art generally. Also, market forces in the industry, and the desire to improve features and performance, would motivate the addition of features to systems as they become available, become less expensive, become more commonly used, provide better performance, reduce costs, size or weight, or predictably achieve other clearly desirable results.

While Apple reserves the right to rely on any combination of the references reflected in their charts or incorporated herein by reference, Apple provides the following exemplary and non-exhaustive references and/or combinations evidencing invalidity of the claims of the

Asserted Patents. The combinations of prior art listed below render obvious the Asserted Claims under the proper construction of the claims and/or under Plaintiff's apparent interpretation of the claims as set forth by Plaintiff in their Complaint and Infringement Contentions. Each combination renders the identified claims obvious through the express and/or inherent disclosure in the combination of references themselves, as well as in view of the knowledge of a person of ordinary skill in the art.

Obviousness Combinations	Claims
U.S. Patent No. 6,138,158 ("Boyle") in view of one or more of U.S. Patent App. Pub. No. 2002/0038371 to Spacey ("Spacey"), U.S. Patent No. 8,326,940 ("Yamamoto"), U.S. Patent No. 6,473,609 ("Schwartz"), U.S. Patent No. 7,007,083 ("Chesley"), U.S. Patent No. 6,421,781 ("Fox"), U.S. Patent No. 6,119,167 ("Boyle2") and/or U.S. Patent No. 7,443,126 ("Gilmore")	Claims 1-20
U.S. Patent App. Pub. No. 2002/0038371 to Spacey ("Spacey") in view of one or more of U.S. Patent No. 6,138,158 ("Boyle"), U.S. Patent No. 8,326,940 ("Yamamoto"), U.S. Patent No. 6,473,609 ("Schwartz"), U.S. Patent No. 7,007,083 ("Chesley"), U.S. Patent No. 6,421,781 ("Fox"), U.S. Patent No. 6,119,167 ("Boyle2") and/or U.S. Patent No. 7,443,126 ("Gilmore")	Claims 1-20
U.S. Patent No. 8,326,940 ("Yamamoto") in view of one or more of U.S. Patent No. 6,138,158 ("Boyle"), U.S. Patent App. Pub. No. 2002/0038371 to Spacey ("Spacey"), U.S. Patent No. 6,473,609 ("Schwartz"), U.S. Patent No. 7,007,083 ("Chesley"), U.S. Patent No. 6,421,781 ("Fox"), U.S. Patent No. 6,119,167 ("Boyle2") and/or U.S. Patent No. 7,443,126 ("Gilmore")	Claims 1-20

In addition to the specific combinations of prior art and the specific combinations of groups of prior art disclosed above, Apple reserves the right to rely on any other combination of any prior art references disclosed herein. Apple further reserves the right to rely upon combinations disclosed within the prosecution history of the references cited herein. These obviousness combinations reflect Apple's present understanding of the potential scope of the claims that SEVEN appears to be advocating and should not be seen as Apple's acquiescence to SEVEN's interpretation of the patent claims.

Apple also reserves the right to amend or supplement these contentions regarding anticipation or obviousness of the Asserted Claims, in view of further information from SEVEN, information discovered during discovery, or a claim construction ruling by the Court. SEVEN has not identified what elements or combinations it alleges were not known to one of ordinary skill in the art at the time. Therefore, for any claim limitation that SEVEN alleges is not disclosed in a particular prior art reference, Apple reserves the right to assert that any such limitation is either inherent in the disclosed reference or obvious to one of ordinary skill in the art at the time in light of the same, or that the limitation is disclosed in another of the references disclosed above and in combination would have rendered the Asserted Claim obvious.

C. Patent Rule 3-3(c): Charts Identifying Where Specifically in Each Alleged Item of Prior Art Each Asserted Claim Is Found

Pursuant to Patent Rule 3-3(c), charts identifying where specifically in each alleged item of prior art each limitation of each Asserted Claim is found, including for each limitation that Apple contends is governed by 35 U.S.C. § 112(6), the identity of the structure(s), act(s), or material(s) in each item of prior art that performs the claimed function, are attached in **Exhibits 534-A and 534-B**.

D. Patent Rule 3-3(d): Other Grounds for Invalidity

Apple identifies the following grounds for invalidity of the Asserted Claims of the ’534 patent based on 35 U.S.C. §§ 101 and/or 112. Apple reserves the right to supplement these disclosures based on further investigation and discovery.

1. Invalidity Pursuant to 35 U.S.C. § 112

Apple further asserts that the Asserted Claims of the ’534 patent are invalid under 35 U.S.C. § 112. The following are the grounds upon which Apple contends the Asserted Claims

are invalid for failure to meet the requirements of 35 U.S.C. § 112, ¶¶ 1, 2, 4 and/or 6, based on Apple's investigation to date and currently-available information.

For each claim identified as invalid, any dependent claims of those invalid claims are also invalid under 35 U.S.C. § 112, ¶¶ 1, 2, 4, and/or 6. Apple reserves the right to supplement and amend these contentions based on further discovery and investigation including, in particular, the deposition of any of the named inventors of the Asserted Patent, the parties' claim construction positions, and further investigation of SEVEN's implied infringement positions.

a) Written Description and/or Enablement

At least in view of SEVEN's apparent construction of the claims in its Infringement Contentions, the Asserted Claims of the '534 patent are invalid because the specification as filed does not contain adequate written description of the claimed inventions sufficient to lead a person of ordinary skill in the art to understand that the named inventors had possession of the purported inventions as claimed as required by 35 U.S.C. § 112, ¶ 1. Likewise, the specification does not enable one of ordinary skill in the art to make or use the claimed inventions without undue experimentation. Based on Apple's present understanding of SEVEN's infringement contentions, Apple asserts that the Asserted Claims of the of the '534 patent are invalid for reciting at least the following claim terms/phrases/limitations:

Claims 1 of the '534 patent and its dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain adequate written descriptions and/or enabling disclosures of "a communication interface." To the extent the claims require "a communication interface," the full scope of the claimed subject matter is not described or enabled. The phrase "communication interface" is not used in the patent's specification, and the patent's disclosures do not describe or enable a server comprising "a communication interface." Rather, the patent's specification describes "[a] communication

management system 16 *includes at least one management server . . . .*" '534 patent at 3:3-4 (emphasis added); *see also, id.* at Fig. 1; Fig. 2. Accordingly, the specification fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

Claims 1 and 11 of the '534 patent and their dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain adequate written descriptions and/or enabling disclosures of "a server" at least to the extent that SEVEN contends this limitation is satisfied by Apple's products. Apple's accused products are not implemented using a single server. The feature that SEVEN identifies in its infringement contentions is not "a server." Thus, to the extent the claim is interpreted broadly enough to include features where there is not "a server," this limitation lacks support.

Claim 1 of the '534 patent and its dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain adequate written descriptions and/or enabling disclosures of "a communication interface," "a processor communicatively coupled to the communication interface," and/or "a memory communicatively coupled to the processor, the memory containing instructions executable by the processor" at least to the extent that SEVEN contends this limitation is satisfied by Apple's products. Apple's accused products are not implemented using a single server comprising "a communication interface," "a processor," or "a memory." The feature that SEVEN identifies in its infringement contentions are not "a communication interface," "a processor," or "a memory." Thus, to the extent the claim is interpreted broadly enough to include features where there is not "a communication interface," "a processor," or "a memory," this limitation lacks support.

Claims 9 and 19 of the ’534 patent are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain adequate written descriptions and/or enabling disclosures of “manag[ing] transactions between the first device and the second device over the first and third connection” at least to the extent that SEVEN contends this limitation is satisfied by Apple’s products. Apple’s accused products do not manage transactions between the first device and the second device over the first and third connection.” The feature that SEVEN identifies in its infringement contentions is not “manag[ing] transactions between the first device and the second device over the first and third connection.” Thus, to the extent the claim is interpreted broadly enough to include features where there is no “manag[ing] transactions between the first device and the second device over the first and third connection,” this limitation lacks support.

b) Indefiniteness

At least in view of SEVEN’s apparent construction of the claims in its Infringement Contentions, the Asserted Claims of the ’534 patent are invalid because they fail to particularly point out and distinctly claim the subject matter which the applicant regards as his invention under 35 U.S.C. § 112, ¶¶ 2, 4, and/or 6. Based on Apple’s present understanding of SEVEN’s infringement contentions, Apple asserts that the Asserted Claims of the of the ’534 patent are invalid for reciting at least the following claim terms/phrases/limitations:

- Claim 1 the ’534 patent and its dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 2, ¶ 4, and/or ¶ 6 because the specification does not describe or otherwise inform one of ordinary skill about what constitutes “a communication interface.” Claim 1 requires a “server ***comprising***:” “a communication interface[.]” ’534 Patent at Claim 1 (emphasis added). However, the specification discloses that “[a]” communications management system 16

includes at least one management server 28 that manages the transactions between the mobile device 21 and the enterprise network 18." '534 Patent at 3:3-4 (emphasis added), Fig. 1. As such, one of ordinary skill would not understand the metes and bounds of the identified claims, rendering them indefinite under 35 U.S.C. § 112, ¶ 2. Therefore, the Asserted Claims, when read in light of the specification and the prosecution history, "fail to inform, with reasonable certainty, those skilled in the art about the scope of the invention." *Nautilus, Inc. v. Biosig Instruments, Inc*., 134 S. Ct. 2120, 2124 (2014).

- Claims 1 and 11 of the of the '534 patent and their dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 2, ¶ 4, and/or ¶ 6 because neither the specification nor the claims describe or otherwise inform one of ordinary skill what constitutes a "the first connection [that] ***includes*** a connection that is initiated by the first device" and/or "the second connection [that] ***includes*** a connection that is initiated by the second device[.]" *See* '534 Patent at Claim 1 (emphasis added). The '534 patent does not describe or explain how to distinguish "a connection that is initiated by the [first or second] device" from "the first connection [that] ***includes*** a connection that is initiated by the first device" and/or "the second connection [that] ***includes*** a connection that is initiated by the second device[.]" As such, one of ordinary skill would not understand the metes and bounds of the identified claims, rendering them indefinite under 35 U.S.C. § 112, ¶ 2. Therefore, the Asserted Claims, when read in light of the specification and the prosecution history, "fail to inform, with

reasonable certainty, those skilled in the art about the scope of the invention." *Nautilus, Inc. v. Biosig Instruments, Inc.*, 134 S. Ct. 2120, 2124 (2014).

- Claims 5, 9, 15 and 19 of the of the '534 patent are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 2, ¶ 4, and/or ¶ 6 because neither the specification nor the claims describe or otherwise inform one of ordinary skill what constitutes a "manage a transaction," "manage transactions," "managing a transaction" and/or "managing transactions." As such, one of ordinary skill would not understand the metes and bounds of the identified claims, rendering them indefinite under 35 U.S.C. § 112, ¶ 2. Therefore, the Asserted Claims, when read in light of the specification and the prosecution history, "fail to inform, with reasonable certainty, those skilled in the art about the scope of the invention." *Nautilus, Inc. v. Biosig Instruments, Inc.*, 134 S. Ct. 2120, 2124 (2014).
- Claims 1, 11, and their dependent claims, and claims 8 and 18 of the of the '534 patent are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 2, ¶ 4, and/or ¶ 6 because neither the specification nor the claims describe or otherwise inform one of ordinary skill what constitutes a "receiv[ing]" a connection. As such, one of ordinary skill would not understand the metes and bounds of the identified claims, rendering them indefinite under 35 U.S.C. § 112, ¶ 2. Therefore, the Asserted Claims, when read in light of the specification and the prosecution history, "fail to inform, with reasonable certainty, those skilled in the art about the scope of the invention." *Nautilus, Inc. v. Biosig Instruments, Inc.*, 134 S. Ct. 2120, 2124 (2014).

- Claims 1 and 11 of the of the ’534 patent and their dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 2, ¶ 4, and/or ¶ 6 because neither the specification nor the claims describe or otherwise inform one of ordinary skill what constitutes being “associated with” a device. As such, one of ordinary skill would not understand the metes and bounds of the identified claims, rendering them indefinite under 35 U.S.C. § 112, ¶ 2. Therefore, the Asserted Claims, when read in light of the specification and the prosecution history, “fail to inform, with reasonable certainty, those skilled in the art about the scope of the invention.” *Nautilus, Inc. v. Biosig Instruments, Inc.*, 134 S. Ct. 2120, 2124 (2014).
- Claims 1 and 11 of the of the ’534 patent and their dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 2, ¶ 4, and/or ¶ 6 because neither the specification nor the claims describe or otherwise inform one of ordinary skill what constitutes “generat[ing]” a message. As such, one of ordinary skill would not understand the metes and bounds of the identified claims, rendering them indefinite under 35 U.S.C. § 112, ¶ 2. Therefore, the Asserted Claims, when read in light of the specification and the prosecution history, “fail to inform, with reasonable certainty, those skilled in the art about the scope of the invention.” *Nautilus, Inc. v. Biosig Instruments, Inc.*, 134 S. Ct. 2120, 2124 (2014).
- Claims 2, 10, 12, and 20 of the of the ’534 patent are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 2, ¶ 4, and/or ¶ 6 because neither the specification nor the claims describe or explain how to distinguish or differentiate

"instructions from a user of the first device" from "response to a request from a user." As such, one of ordinary skill would not understand the metes and bounds of the identified claims, rendering them indefinite under 35 U.S.C. § 112, ¶ 2. Therefore, the Asserted Claims, when read in light of the specification and the prosecution history, "fail to inform, with reasonable certainty, those skilled in the art about the scope of the invention." *Nautilus, Inc. v. Biosig Instruments, Inc.*, 134 S. Ct. 2120, 2124 (2014).

2. Other Grounds for Invalidity

In addition to the preceding invalidity contentions, Apple further contends that each of the Asserted Claims of the '534 patent is drawn to subject matter that is not patentable under 35 U.S.C. § 101. The '534 patent Asserted Claims are invalid under 35 U.S.C. § 101 for failure to recite patent eligible subject matter. Specifically, all claims of the '534 patent are fatally abstract under the U.S. Supreme Court's decision in *Alice Corp. v. CLS Bank Int'l*, 134 S. Ct. 2345 (2014) and progeny. The ideas presented in the claims are generally directed to concepts of one entity querying information from another entity. Under *Alice* Step 1, those ideas are abstract, as they relate to a fundamental long prevalent practice. *See Intellectual Ventures I LLC v. Symantec Corp.*, 838 F.3d 1307, 1314 (Fed. Cir. 2016). Limiting the invention to a particular technological environment, e.g. generic computer hardware, "do[es] not render an otherwise abstract concept any less abstract." *Intellectual Ventures I LLC v. Capital One Fin. Corp.*, 850 F.3d 1332, 1340 (Fed Cir. 2017). Furthermore, because the patent relates to transmission of information, it is likewise abstract, as "information is … an intangible." *Electric Power Group, LLC v. Alstom S.A.*, 830 F.3d 1350, 1353 (Fed. Cir. 2016). Furthermore, under *Alice* Step 2 the '534 patent does not contain any inventive concept. The '534 patent Asserted Claims employs well-known components or functionality, as shown in Apple's invalidity contentions involving anticipation

and/or obviousness in this case, which is not enough to impart patent eligibility of an abstract idea. *See, e.g., Alice*, 134 S. Ct. at 2359 (holding that limitations describing "'well-understood, routine, conventional activit[ies]' previously known to the industry" were insufficient to supply an inventive concept (quoting *Mayo*, 132 S. Ct. at 1294)). Further detail regarding Apple's contentions that the Asserted Claims of the '534 patent do not qualify as patent-eligible subject matter are contained in **Exhibit 534-D**.

Apple reserves the right to assert that the asserted patents are invalid under 35 U.S.C. §102(f) and/or (g) in the event Apple obtains evidence that the named inventors of the '534 patent did not invent (either alone or in conjunction with other parties) the subject matter claimed in the '534 patent. Should Apple obtain such evidence, it will provide the name of the person(s) from whom and the circumstances under which the invention or any part of it was derived, and/or the circumstances surrounding the making of the invention before the patent application.

Apple reserves the right to supplement these disclosures based on further investigation and discovery.

XV. THE '771 PATENT

A. Patent Rule 3-3(a): Identification of Prior Art

At this time, Apple contends that at least each of the prior art references described and charted in **Exhibits 771-A and 771-B** anticipates or renders obvious, either alone or in combination, one or more of the Asserted Claims of the '771 patent.

Additional prior art that has not been charted, but is still relevant to the invalidity of the '771 patent is listed in **Exhibit C**, including without limitation as evidence of the state of the art at the alleged time of invention. Apple reserves the right to amend these invalidity contentions to assert these references depending on the claim construction and infringement positions SEVEN may take as the case proceeds. Moreover, Apple reserves the right to use these

references in combination with other references to render the claims of the ’771 patent obvious in the event SEVEN takes the position that certain claim limitations are missing from the references charted in **Exhibits 771-A and 771-B.**

B. Patent Rule 3-3(b): Whether Each Item Anticipates or Renders Obvious the Asserted Claims

SEVEN asserts claims 1-30 of the ’771 patent against Apple in this lawsuit. These claims are invalid because the ’771 patent fails to meet one or more of the requirements for patentability. The individual bases for invalidity are provided below and in the claim charts attached as **Exhibits 771-A and 771-B**. Each of the foregoing listed prior art documents, the underlying work, and/or the underlying apparatus or method qualifies as prior art under one or more sections of 35 U.S.C. §§ 102 and/or 103.

Although Apple has identified at least one citation per limitation for each reference, each and every disclosure of the same limitation in the same reference is not necessarily identified. Rather, in an effort to focus the issues, Apple has cited representative portions of identified references, even where a reference may contain additional support for a particular claim element. In addition, persons of ordinary skill in the art generally read a prior art reference as a whole and in the context of other publications and literature. Thus, to understand and interpret any specific statement or disclosure within a prior art reference, such persons would rely on other information within the reference, along with other publications and their general scientific knowledge. Apple may rely upon uncited portions of the prior art references and on other publications and expert testimony to provide context, and as aids to understanding and interpreting the portions that are cited. Apple may also rely on uncited portions of the prior art references, other disclosed publications, and the testimony of experts to establish that a person of ordinary skill in the art

would have been motivated to modify or combine certain of the cited references so as to render the claims obvious.

1. Priority

SEVEN's Patent Rule 3-1(e) disclosures provide that the Asserted Claims of the '771 patent are entitled to a priority date of January 8, 2002, which is the filing date of U.S. Provisional Application No. 60/346,881. SEVEN has provided no evidence to support its contention that the Asserted Claims of the '771 patent are entitled to claim priority back to this or any earlier filed application, and Apple therefore reserves the right to assert a later priority date based on any findings as to the priority date of the Asserted Claims by the Court, information learned through discovery, or otherwise.

The '771 patent claims priority to two provisional applications: (1) Provisional Application No. 60/403,249 (the '249 application) filed on August 12, 2002 and (2) Provisional Application No. 60/346,881 (the '881 application) filed on January 8, 2002. Apple reserves the right to challenge SEVEN's assertion that the '771 patent is entitled to claim the benefit of either provisional application's filing date to the extent that the provisional application does not support the full scope of the Asserted Claims, for example, depending on scope of the Asserted Claims as properly construed. To the extent the provisional application does not support the full scope of the Asserted Claims, the priority date of the '771 patent should be the filing date of the patent application of which the '771 patent is a continuation, which is January 8, 2003.

None of the Asserted Claims are entitled to the filing date of either the '249 or the '881 applications because each and every claim does not have written description support from the provisional applications. *See Falko-Gunter Falkner v. Inglis*, 448 F.3d 1357 (Fed. Cir. 2006). Each and every asserted claim is not entitled to either the '249 or the '881 application filing dates

because those applications do not actually or inherently disclose each and every claim element. *PowerOasis, Inc. v. T-Mobile USA, Inc*., 522 F.3d 1299, 1306-07 (Fed. Cir. 2008).

For example, the claims recite the features relating to "receiving a token issued by an intermediary server" and "wherein the payload data is transmitted to a second computer by the intermediary server based on the token," and variations of those limitations. Nothing in the '249 or the '881 provisional applications shows that the inventors possessed and enabled functionalities relating to these limitations as recited in the Asserted Claims. The provisional applications are merely user guides that do not disclose the limitations by which a token is used to dictate any routing information, for example.

Consequently the '249 and '881 provisional applications do not actually or inherently disclose each and every element of the '771 patent claims and therefore the '771 patent claims do not deserve the filing date of the provisional applications from which to claim priority.

2. Anticipation

Some or all of the Asserted Claims of the '771 patent are invalid as anticipated under 35 U.S.C. § 102 in view of each of the prior art references identified above and in the claim charts included in **Exhibit 771-A**, which identify specific examples of where each limitation of the Asserted Claims is found in the prior art references. As explained above, the cited portions of prior art references identified in the attached claim charts are exemplary only and representative of the content and teaching of the prior art references, and should be understood in the context of the reference as a whole and as they would be understood by a person of ordinary skill in the art.

Apple identifies the following references as anticipating one or more of the Asserted Claims of the '771 patent under 35 U.S.C. § 102. The below table of anticipating references is exemplary, and it does not constitute an admission that any reference anticipates only the listed claims. Further, Apple contends that any prior art reference in the attached charts that is charted

for each limitation of any given claim, anticipates that claim, regardless of whether that prior art reference is listed in the following table.

Exhibit	Anticipating Prior Art	Claims
771-A01	U.S. Patent Appl. No. 2002/0178370 to Gurevich et al.	1-30
771-A03	U.S. Patent No. 6,167,513 to Inoue et al.	1, 2, 3, 4, 5, 7, 8, 9, 10, 11, 12, 14, 15, 16, 17, 18, 20, 21, 22, 23, 24, 26, 27, 28, 29
771-A04	U.S. Patent No. 9,941,951 to Felsher et al.	1-30
771-A05	U.S. Patent No. 7,814,208 to Stephenson et al.	1-30

To the extent any item of prior art cited above is deemed not to disclose, explicitly or inherently, any limitation of an Asserted Claim of the ’771 patent, Apple reserves the right to argue that any difference between that prior art and the corresponding patent claim would have been either inherent to the art, or obvious to a person of ordinary skill in the art, even if Apple has not specifically denoted that the art is to be combined with the knowledge of a person of ordinary skill in the art.

3. Obviousness

To the extent any limitation is deemed not to be exactly met by an item of prior art listed above and in **Exhibit 771-A**, then any purported differences are such that the claimed subject matter as a whole would have been obvious to one skilled in the art at the time of the alleged invention, in view of the state of the art and knowledge of those skilled in the art. The item of prior art would, therefore, render the relevant claims invalid for obviousness under 35 U.S.C. § 103.

In addition, the references identified above render one or more Asserted Claims of the ’771 patent obvious when the references are read in combination with each other, and/or when read in view of the state of the art and knowledge of those skilled in the art. Each and every reference identified is also relevant to the state of the art at the time of the alleged invention.

Any of the references disclosed above may be combined with one another to render obvious (and therefore invalid) each of SEVEN's Asserted Claims. Apple may rely upon a subset of the above identified references or all of the references identified above, including all references in **Exhibits 771-A, 771-B, and C**, for purposes of obviousness depending on the Court's claim construction, positions taken by SEVEN during this litigation, and further investigation and discovery.

To the extent the foregoing references are found not to anticipate the Asserted Claims, the foregoing references render the Asserted Claims obvious either alone or in combination with one or more of the other references identified above pursuant to Patent Rule 3-3(a). It would have been obvious to a person of skill in the art at the time of the alleged invention of the Asserted Claims of the '771 patent to combine the various references cited herein so as to disclose the Asserted Claims of the '771 patent.

In accordance with Patent Rule 3-3(b), prior art references rendering the Asserted Claims obvious, alone or in combination with other references, are outlined below and included in **Exhibits 771-A and 771-B**, which include exemplary claim charts for the Asserted Claims of the '771 patent showing specifically where in each reference or combinations of references each Asserted Claim is found, and an explanation of why the prior art renders the Asserted Claim obvious. Where applicable, **Exhibits 771-A and 771-B** include the motivation to combine references.

Moreover, in addition to the information contained elsewhere in these contentions and in particular **Exhibit 771-B**, Apple has identified additional motivations and reasons to combine the various references cited herein. In particular, multiple teachings, suggestions, and/or reasons to modify any of the references and/or to combine any two or more of the references in **Exhibits**

771-A and 771-B come from many sources, including the prior art (specific and as a whole), common knowledge, common sense, predictability, expectations, industry trends, design incentives or need, market demand or pressure, market forces, obvious to try, the nature of the problem faced, and/or knowledge possessed by one of ordinary skill. In addition, it would have been obvious to try combining the prior art references identified above because there were only a finite number of predictable solutions and/or because known work in one field or endeavor prompted variations based on predictable design incentives and/or market forces either in the same field or a different one. The combination of prior art references identified in these contentions would have been obvious because the claimed combinations represent the known potential options with a reasonable expectation of success. Additionally, one of ordinary skill in the art would have been motivated to create combinations identified in these contentions using: known methods to yield predictable results; known techniques in the same way; a simple substitution of one known, equivalent element for another to obtain predictable results; and/or teaching, suggestion, or motivation in the prior art generally. Also, market forces in the industry, and the desire to improve features and performance, would motivate the addition of features to systems as they become available, become less expensive, become more commonly used, provide better performance, reduce costs, size or weight, or predictably achieve other clearly desirable results.

While Apple reserves the right to rely on any combination of the references reflected in their charts or incorporated herein by reference, Apple provides the following exemplary and non-exhaustive references and/or combinations evidencing invalidity of the claims of the Asserted Patents. The combinations of prior art listed below render obvious the Asserted Claims under the proper construction of the claims and/or under Plaintiff's apparent interpretation of the

claims as set forth by Plaintiff in their Complaint and Infringement Contentions. Each combination renders the identified claims obvious through the express and/or inherent disclosure in the combination of references themselves, as well as in view of the knowledge of a person of ordinary skill in the art.

Obviousness Combinations	Claims
U.S. Patent App. No. 2002/0178370 ("Gurevich") in view of U.S. Patent No. 9,419,951 ("Felsher"), U.S. Patent No. 7,814,208 to Stephenson et al. ("Stephenson"), U.S. Patent No. 6,167,513 ("Inoue"), The U-Guard System at https://web.archive.org/web/*/http://uguard.com (U-Guard), U.S. Patent No. 7,747,856 ("Favazza"), and/or one or more of and/or one or more of Int. Pat. App. WO 97/45981 ("Johnston"), U.S. Patent No. 8,090,951 ("Erlingsson"), U.S. Patent App. No. 2002/0019932 ("Toh"), and/or U.S. Patent No. 8,543,644 ("Gage")	All Asserted Claims
Gurevich in view of Felsher, and/or one or more of and/or one or more of Johnston, Erlingsson, Toh, and/or Gage	All Asserted Claims
Gurevich in view of Stephenson, and/or one or more of and/or one or more of Johnston, Erlingsson, Toh, and/or Gage	All Asserted Claims
Gurevich in view of Inoue, and/or one or more of and/or one or more of Johnston, Erlingsson, Toh, and/or Gage	All Asserted Claims
Gurevich in view of U-Guard, and/or one or more of and/or one or more of Johnston, Erlingsson, Toh, and/or Gage	All Asserted Claims
Gurevich in view of Favazza, and/or one or more of and/or one or more of Johnston, Erlingsson, Toh, and/or Gage	All Asserted Claims
Gurevich in view of Felsher, Stephenson, Inoue, U-Guard, and/or Favazza	All Asserted Claims
Felsher in view of Gurevich, and/or one or more of and/or one or more of Johnston, Erlingsson, Toh, and/or Gage	All Asserted Claims
Felsher in view of Stephenson, and/or one or more of and/or one or more of Johnston, Erlingsson, Toh, and/or Gage	All Asserted Claims
Felsher in view of Inoue, and/or one or more of and/or one or more of Johnston, Erlingsson, Toh, and/or Gage	All Asserted Claims
Felsher in view of U-Guard, and/or one or more of and/or one or more of Johnston, Erlingsson, Toh, and/or Gage	All Asserted Claims
Felsher in view of Favazza, and/or one or more of and/or one or more of Johnston, Erlingsson, Toh, and/or Gage	All Asserted Claims
Felsher in view of Gurevich, Stephenson, Inoue, U-Guard, and/or Favazza	All Asserted Claims
Felsher in view of Gurevich, Stephenson, Inoue, U-Guard, Favazza, and/or one or more of and/or one or more of Johnston, Erlingsson, Toh, and/or Gage	All Asserted Claims

Obviousness Combinations	Claims
Stephenson in view of Felsher, and/or one or more of and/or one or more of Johnston, Erlingsson, Toh, and/or Gage	All Asserted Claims
Stephenson in view of Gurevich, and/or one or more of and/or one or more of Johnston, Erlingsson, Toh, and/or Gage	All Asserted Claims
Stephenson in view of Inoue, and/or one or more of and/or one or more of Johnston, Erlingsson, Toh, and/or Gage	All Asserted Claims
Stephenson in view of U-Guard, and/or one or more of and/or one or more of Johnston, Erlingsson, Toh, and/or Gage	All Asserted Claims
Stephenson in view of Favazza, and/or one or more of and/or one or more of Johnston, Erlingsson, Toh, and/or Gage	All Asserted Claims
Stephenson in view of Felsher, Gurevich, Inoue, U-Guard, and/or Favazza	All Asserted Claims
Stephenson in view of Felsher, Gurevich, Inoue, U-Guard, Favazza, and/or one or more of and/or one or more of Johnston, Erlingsson, Toh, and/or Gage	All Asserted Claims
Inoue in view of Gurevich, and/or one or more of and/or one or more of Johnston, Erlingsson, Toh, and/or Gage	All Asserted Claims
Inoue in view of Stephenson, and/or one or more of and/or one or more of Johnston, Erlingsson, Toh, and/or Gage	All Asserted Claims
Inoue in view of Felsher, and/or one or more of and/or one or more of Johnston, Erlingsson, Toh, and/or Gage	All Asserted Claims
Inoue in view of U-Guard, and/or one or more of and/or one or more of Johnston, Erlingsson, Toh, and/or Gage	All Asserted Claims
Inoue in view of Favazza, and/or one or more of and/or one or more of Johnston, Erlingsson, Toh, and/or Gage	All Asserted Claims
Inoue in view of Gurevich, Stephenson, Felsher, U-Guard, and/or Favazza	All Asserted Claims
Inoue in view of Felsher, Stephenson, Gurevich, U-Guard, Favazza, and/or one or more of and/or one or more of Johnston, Erlingsson, Toh, and/or Gage	All Asserted Claims
Favazza in view of Felsher, and/or one or more of and/or one or more of Johnston, Erlingsson, Toh, and/or Gage	All Asserted Claims
Favazza in view of Stephenson, and/or one or more of and/or one or more of Johnston, Erlingsson, Toh, and/or Gage	All Asserted Claims
Favazza in view of Inoue, and/or one or more of and/or one or more of Johnston, Erlingsson, Toh, and/or Gage	All Asserted Claims
Favazza in view of U-Guard, and/or one or more of and/or one or more of Johnston, Erlingsson, Toh, and/or Gage	All Asserted Claims
Favazza in view of Gurevich, and/or one or more of and/or one or more of Johnston, Erlingsson, Toh, and/or Gage	All Asserted Claims
Favazza in view of Felsher, Stephenson, Inoue, U-Guard, and/or Gurevich	All Asserted Claims
Favazza in view of Felsher, Stephenson, Inoue, U-Guard, Gurevich, and/or one or more of and/or one or more of Johnston, Erlingsson, Toh, and/or Gage	All Asserted Claims

Obviousness Combinations	Claims
U-Guard in view of Gurevich, and/or one or more of and/or one or more of Johnston, Erlingsson, Toh, and/or Gage	All Asserted Claims
U-Guard in view of Stephenson, and/or one or more of and/or one or more of Johnston, Erlingsson, Toh, and/or Gage	All Asserted Claims
U-Guard in view of Inoue, and/or one or more of and/or one or more of Johnston, Erlingsson, Toh, and/or Gage	All Asserted Claims
U-Guard in view of Felsher, and/or one or more of and/or one or more of Johnston, Erlingsson, Toh, and/or Gage	All Asserted Claims
U-Guard in view of Favazza, and/or one or more of and/or one or more of Johnston, Erlingsson, Toh, and/or Gage	All Asserted Claims
U-Guard in view of Felsher, Gurevich, Stephenson, Inoue, and/or Favazza	All Asserted Claims
U-Guard in view of Felsher, Stephenson, Inoue, Gurevich, Favazza, and/or one or more of and/or one or more of Johnston, Erlingsson, Toh, and/or Gage	All Asserted Claims

In addition to the specific combinations of prior art and the specific combinations of groups of prior art disclosed above, Apple reserves the right to rely on any other combination of any prior art references disclosed herein. Apple further reserves the right to rely upon combinations disclosed within the prosecution history of the references cited herein. These obviousness combinations reflect Apple's present understanding of the potential scope of the claims that SEVEN appears to be advocating and should not be seen as Apple's acquiescence to SEVEN's interpretation of the patent claims.

Apple also reserves the right to amend or supplement these contentions regarding anticipation or obviousness of the Asserted Claims, in view of further information from SEVEN, information discovered during discovery, or a claim construction ruling by the Court. SEVEN has not identified what elements or combinations it alleges were not known to one of ordinary skill in the art at the time. Therefore, for any claim limitation that SEVEN alleges is not disclosed in a particular prior art reference, Apple reserves the right to assert that any such limitation is either inherent in the disclosed reference or obvious to one of ordinary skill in the

art at the time in light of the same, or that the limitation is disclosed in another of the references disclosed above and in combination would have rendered the Asserted Claim obvious.

C. Patent Rule 3-3(c): Charts Identifying Where Specifically in Each Alleged Item of Prior Art Each Asserted Claim Is Found

Pursuant to Patent Rule 3-3(c), charts identifying where specifically in each alleged item of prior art each limitation of each Asserted Claim is found, including for each limitation that Apple contends is governed by 35 U.S.C. § 112(6), the identity of the structure(s), act(s), or material(s) in each item of prior art that performs the claimed function, are attached in **Exhibits 771-A and 771-B**.

D. Patent Rule 3-3(d): Other Grounds for Invalidity

Apple identifies the following grounds for invalidity of the Asserted Claims of the '771 patent based on 35 U.S.C. §§ 101 and/or 112. Apple reserves the right to supplement these disclosures based on further investigation and discovery.

1. Invalidity Pursuant to 35 U.S.C. § 112

Apple further asserts that the Asserted Claims of the '771 patent are invalid under 35 U.S.C. § 112. The following are the grounds upon which Apple contends the Asserted Claims are invalid for failure to meet the requirements of 35 U.S.C. § 112, ¶¶ 1, 2, 4 and/or 6, based on Apple's investigation to date and currently-available information.

For each claim identified as invalid, any dependent claims of those invalid claims are also invalid under 35 U.S.C. § 112, ¶¶ 1, 2, 4, and/or 6. Apple reserves the right to supplement and amend these contentions based on further discovery and investigation including, in particular, the deposition of any of the named inventors of the Asserted Patent, the parties' claim construction positions, and further investigation of SEVEN's implied infringement positions.

a) Written Description and/or Enablement

At least in view of SEVEN's apparent construction of the claims in its Infringement Contentions, the Asserted Claims of the '771 patent are invalid because the specification as filed does not contain adequate written description of the claimed inventions sufficient to lead a person of ordinary skill in the art to understand that the named inventors had possession of the purported inventions as claimed as required by 35 U.S.C. § 112, ¶ 1. Likewise, the specification does not enable one of ordinary skill in the art to make or use the claimed inventions without undue experimentation. Based on Apple's present understanding of SEVEN's infringement contentions, Apple asserts that the Asserted Claims of the of the '771 patent are invalid for reciting at least the following claim terms/phrases/limitations:

Claims 1, 14, and 26 of the '771 patent and their dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification does not contain an adequate written description and/or enabling disclosure of "intermediary server." To the extent the term "intermediary server" is construed to mean more than a specific set of computers acting as a single server as identified in the '771 patent specification, the full scope of the claimed subject matter is not described or enabled. Accordingly, the specification fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

b) Indefiniteness

At least in view of SEVEN's apparent construction of the claims in its Infringement Contentions, the Asserted Claims of the '771 patent are invalid because they fail to particularly point out and distinctly claim the subject matter which the applicant regards as his invention under 35 U.S.C. § 112, ¶¶ 2, 4, and/or 6. Based on Apple's present understanding of SEVEN's

infringement contentions, Apple asserts that the Asserted Claims of the of the '771 patent are invalid for reciting at least the following claim terms/phrases/limitations:

Claims 1, 14, and 26 of the '771 patent and their dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 2, ¶ 4, and/or ¶ 6 because the specification does not describe or otherwise inform one of ordinary skill about what constitutes an "intermediary server." The '771 patent does not describe or explain how to limit an intermediary server. According to SEVEN, an intermediary server has no bounds, including based on the amount of physical servers involved or the type of server involved, such that SEVEN would consider all servers to be one server. As such, one of ordinary skill would not understand the metes and bounds of the identified claims, rendering them indefinite under 35 U.S.C. § 112, ¶ 2. Therefore, the Asserted Claims, when read in light of the specification and the prosecution history, "fail to inform, with reasonable certainty, those skilled in the art about the scope of the invention." *Nautilus, Inc. v. Biosig Instruments, Inc*., 134 S. Ct. 2120, 2124 (2014).

2. Other Grounds for Invalidity

In addition to the preceding invalidity contentions, Apple further contends that each of the Asserted Claims of the '771 patent is drawn to subject matter that is not patentable under 35 U.S.C. § 101. The '771 patent Asserted Claims are invalid under 35 U.S.C. § 101 for failure to recite patent eligible subject matter. Specifically, all claims of the '771 patent are fatally abstract under the U.S. Supreme Court's decision in *Alice Corp. v. CLS Bank Int'l*, 134 S. Ct. 2345 (2014) and progeny. The ideas presented in the claims are generally directed to concepts of routing information, such as (1) receiving routing information and (2) sending a message based on the routing information. Under *Alice* Step 1, those ideas are abstract, as they relate to a fundamental long prevalent practice. *See Intellectual Ventures I LLC v. Symantec Corp.*, 838 F.3d 1307, 1314 (Fed. Cir. 2016). Limiting the invention to a particular technological

environment, *e.g.*, generic computer hardware or as being "over a mobile network," "do[es] not render an otherwise abstract concept any less abstract." *Intellectual Ventures I LLC v. Capital One Fin. Corp.*, 850 F.3d 1332, 1340 (Fed Cir. 2017). Courts have found that the steps of routing information (*i.e.*, transmitting a transaction message based on a previously received token) are abstract. *Two-Way Media Ltd. v. Comcast Cable Commc'ns LLC*, 874 F.3d 1329 (Fed. Cir. 2017) ("Claim 1 recites a method for routing information using result-based functional language."). Furthermore, because the patent relates to the secure transmission of information, it is likewise abstract, as "information is … an intangible." *Electric Power Group, LLC v. Alstom S.A.*, 830 F.3d 1350, 1353 (Fed. Cir. 2016). Furthermore, under *Alice* Step 2 the '771 patent does not contain any inventive concept. The '771 patent's Asserted Claims employ well-known components or functionality, as shown in Apple's invalidity contentions involving anticipation and/or obviousness in this case, which is not enough to impart patent eligibility of an abstract idea. *See, e.g.*, *Alice*, 134 S. Ct. at 2359 (holding that limitations describing "'well-understood, routine, conventional activit[ies]' previously known to the industry" were insufficient to supply an inventive concept (quoting *Mayo*, 132 S. Ct. at 1294)). Further detail regarding Apple's contentions that the Asserted Claims of the '771 patent do not qualify as patent-eligible subject matter are contained in **Exhibit 771-D**.

Apple reserves the right to assert that the asserted patents are invalid under 35 U.S.C. §102(f) and/or (g) in the event Apple obtains evidence that the named inventors of the '771 patent did not invent (either alone or in conjunction with other parties) the subject matter claimed in the '771 patent. Should Apple obtain such evidence, it will provide the name of the person(s) from whom and the circumstances under which the invention or any part of it was derived, and/or the circumstances surrounding the making of the invention before the patent application.

Apple reserves the right to supplement these disclosures based on further investigation and discovery.

XVI. THE '962 PATENT

A. Patent Rule 3-3(a): Identification of Prior Art

At this time, Apple contends that at least each of the prior art references described and charted in **Exhibits 962-A and 962-B** anticipates or renders obvious, either alone or in combination, one or more of the Asserted Claims of the '962 patent.

Additional prior art that has not been charted, but is still relevant to the invalidity of the '962 patent is listed in **Exhibit C**, including without limitation as evidence of the state of the art at the alleged time of invention. Apple reserves the right to amend these invalidity contentions to assert these references depending on the claim construction and infringement positions SEVEN may take as the case proceeds. Moreover, Apple reserves the right to use these references in combination with other references to render the claims of the '962 patent obvious in the event SEVEN takes the position that certain claim limitations are missing from the references charted in **Exhibits 962-A and 962-B**.

B. Patent Rule 3-3(b): Whether Each Item Anticipates or Renders Obvious the Asserted Claims

SEVEN asserts claims 1–44 of the '962 patent against Apple in this lawsuit. These claims are invalid because the '962 patent fails to meet one or more of the requirements for patentability. The individual bases for invalidity are provided below and in the claim charts attached as **Exhibits 962-A and 962-B**. Each of the foregoing listed prior art documents, the underlying work, and/or the underlying apparatus or method qualifies as prior art under one or more sections of 35 U.S.C. §§ 102 and/or 103.

Although Apple has identified at least one citation per limitation for each reference, each and every disclosure of the same limitation in the same reference is not necessarily identified. Rather, in an effort to focus the issues, Apple has cited representative portions of identified references, even where a reference may contain additional support for a particular claim element. In addition, persons of ordinary skill in the art generally read a prior art reference as a whole and in the context of other publications and literature. Thus, to understand and interpret any specific statement or disclosure within a prior art reference, such persons would rely on other information within the reference, along with other publications and their general scientific knowledge. Apple may rely upon uncited portions of the prior art references and on other publications and expert testimony to provide context, and as aids to understanding and interpreting the portions that are cited. Apple may also rely on uncited portions of the prior art references, other disclosed publications, and the testimony of experts to establish that a person of ordinary skill in the art would have been motivated to modify or combine certain of the cited references so as to render the claims obvious.

1. Priority

SEVEN's Patent Rule 3-1(e) disclosures provide that the Asserted Claims of the '962 patent are entitled to a priority date of April 21, 2005, which is the filing date of U.S. Patent Application No. 11/112,690 (the '690 application), which issued as U.S. Patent No. 7,792,742. Apple reserves the right to challenge SEVEN's assertion that the '962 patent is entitled to claim the benefit of the '690 application to the extent it does not support the full scope of the Asserted Claims, for example, depending on scope of the Asserted Claims as properly construed. To the extent the '690 application does not support the full scope of the Asserted Claims, the priority date of the '962 patent should be the filing date of the patent application of which the '962 patent

is a continuation-in-part, which is U.S. Application No. 11/640,629 (the '629 application) filed on December 18, 2006, which issued as U.S. Patent No. 8,438,633.

SEVEN has provided no evidence to support its contention that the Asserted Claims of the '962 patent are entitled to claim priority back to the '690 or any earlier filed application, and Apple therefore reserves the right to assert a later priority date based on any findings as to the priority date of the Asserted Claims by the Court, information learned through discovery, or otherwise.

a) The Asserted Claims of the '962 Patent Cannot Claim Priority to the '690 Application

None of the Asserted Claims are entitled to the filing date of U.S. Application No. 11/112,690 ("the '690 application"), which issued as U.S. Patent No. 7,796,742 because the '962 patent claims 1, 23, and dependent claims thereof, as well as claims 7, 9, 10, 12, 13, 14, 15, 16, 17, 18, 19, 22, 29, 31, 33, 34, 35, 36, 37, 38, 39, and 44 do not have written description support in the '690 application. *See PowerOasis, Inc. v. T-Mobile USA, Inc*., 522 F.3d 1299, 1306-07 (Fed. Cir. 2008).

Claims 1 and 23 are not entitled to the '690 application filing date because the '690 application does not actually or inherently disclose each and every claim element. *Id*. at 1306-07. Claims 1 and 23 recite features relating to a server sending messages to a client device which find no support in the '690 application. Nothing in the '690 application shows the inventor(s) possessed and enabled functionalities relating to "sending a first message indicative of new information at the data store," "transmitting a second message to the client device in response to receipt of the first message," and "wherein additional information associated with the first message is sent from the data store to the client device upon receipt of the second message by the client device," as recited in claims 1 and 23.

Importantly, the ’690 application never uses the terms “first message,” “second message,” “indicative of new information,” or “additional information,” or otherwise discloses the concepts. The ’690 application does make one reference to sending a “text message,” but such text message is not “indicative of new information at the data store” or sent “in response to a first message.” ’690 application ¶ [0038] (“In order to associate the unique identifier to the device 102 for recognition during future contact with the server 106, a text message, for example, can be sent to the device 102 with the unique identifier.”). The ’690 application never mentions sending messages or additional information in the context and based on the factors recited in the ’962 patent claims. Thus, the ’690 application does not adequately provide written description support for sending a first message, sending a second message, or providing additional information in response to the sending of the messages.

Moreover, claims 1 and 23 relate to “sending a keep-alive message” and “maintenance of a subsequent connection.” The ’690 application never uses the terms “keep-alive message” or “maintenance” of a subsequent connection, or otherwise discloses the concepts. Thus, the ’690 application does not adequately provide written description support for sending a keep-alive message or maintenance of a subsequent connection.

As to claims 7 and 29, the ’690 application fails to disclose “wherein the first message is received when the first message matches a predefined characteristic set by the data store.” As noted above, the ’690 application never uses the term “first message” and does not disclose sending any communication “indicative of new information at the data store,” and in addition, does not disclose sending any such first message based on predefined characteristics. The ’690 application does not use the term “predefined characteristics” or otherwise disclose the concept.

Thus, the ’690 application does not adequately provide written description support for sending a first message when the first message matches a predefined characteristic set by the data store.

As to claims 9 and 31, the ’690 application fails to disclose “wherein the server is configured to direct the client device to delete content thereon in response to an indication that the client device is misappropriated.” The ’690 application does not use the term “misappropriated,” “delete” or “indication” or otherwise disclose the concept. Thus, the ’690 application does not adequately provide written description support for “wherein the server is configured to direct the client device to delete content thereon in response to an indication that the client device is misappropriated.

As to claims 10 and 32, the ’690 application fails to disclose “wherein the additional information is sent over a subsequently established connection that is independent of the server.” As noted above, the ’690 application never uses the term “additional information” and does not disclose sending any “additional information” upon receipt of the second message, and in addition, does not disclose sending any such additional information over a subsequently established connection that is independent of the server. The ’690 application does not use the term “subsequent connection” or “independent connection” or otherwise disclose the concept. Thus, the ’690 application does not adequately provide written description support for “wherein the additional information is sent over a subsequently established connection that is independent of the server.”

As to claims 12 and 33, the ’690 application fails to disclose “wherein an IP connection is established between the client device and the data store in response to transmission of the second message to the client device by the server for sending of the additional information.” As noted above, the ’690 application never uses the term “additional information” and does not disclose

sending any "additional information" upon receipt of the second message, and in addition, does not disclose establishing an IP connection between the client device and the data store for sending such additional information. The '690 application does not use the term "IP connection" or otherwise disclose the concept. Thus, the '690 application does not adequately provide written description support for "wherein an IP connection is established between the client device and the data store in response to transmission of the second message to the client device by the server for sending of the additional information."

As to claims 13 and 34, the '690 application fails to disclose "wherein the second message is encrypted." As noted above, the '690 application never uses the term "second message," or otherwise disclose sending a second message, and in addition, does not disclose an encrypted second message. The '690 application does not use the term "encrypted" or "encryption," or otherwise disclose the concept. Thus, the '690 application does not adequately provide written description support for "wherein the second message is encrypted."

As to claims 14 and 35, the '690 application fails to disclose "wherein an additional message indicative of new data at the first data store is transmitted over the subsequent connection." As noted above, the '690 application does not disclose a "first message," a "second message," much less an "additional message." The '690 application does not use the term "indicative of new data at the first data store" or "subsequent connection," or otherwise disclose the concepts. Thus, the '690 application does not adequately provide written description support for "wherein an additional message indicative of new data at the first data store is transmitted over the subsequent connection."

As to claims 15 and 36, the '690 application fails to disclose "wherein the server is further configured to receive a third message from a second data store, wherein the third message

from the second data store is indicative of new information at the second data store, wherein a fourth message is associated with the second data store is transmitted over the subsequent connection." As noted above, the '690 application does not disclose sending any messages under the a "first message," a "second message," much less a "third message" or "fourth message." The '690 application does not use the term "indicative of new data at the first data store" or "subsequent connection," or otherwise disclose the concepts. Thus, the '690 application does not adequately provide written description support for "wherein the server is further configured to receive a third message from a second data store, wherein the third message from the second data store is indicative of new information at the second data store, wherein a fourth message is associated with the second data store is transmitted over the subsequent connection."

As to claims 16, 17, 18, 38, 39, and 40, which each relate to establishing a "subsequent connection" over different networks or different wireless network, the '690 application fails to disclose a "subsequent connection" or different networks. The '690 application does not use the term "subsequent connection" or otherwise disclose the concept of multiple networks. Thus, the '690 application does not adequately provide written description support for these "subsequent connection" limitations.

As to claims 19 and 41, which claim a server "further configured to monitor active connections established with the client device, wherein transmitting the second message is based on the monitoring," the '690 application fails to disclose sufficient written support. As discussed above, the '690 application does not disclose a "second message," and further does not use the term "active connections" or "monitoring," or otherwise disclose the concepts. Thus, the '690 application does not adequately provide written description support for these "monitor active connections" limitations. *Id.*

Consequently, the ’690 application does not actually or inherently disclose each and every element of the ’962 patent claims. *PowerOasis*, 522 F.3d at 1306-07. The introduction of these features into the claims resulted in the ’962 patent claims not being entitled to the filing date of the ’690 application, and are, at most, entitled to the filing date of December 18, 2006—the filing date of the ’629 application.

2. Anticipation

Some or all of the Asserted Claims of the ’962 patent are invalid as anticipated under 35 U.S.C. § 102 in view of each of the prior art references identified above and in the claim charts included in **Exhibit 962-A**, which identify specific examples of where each limitation of the Asserted Claims is found in the prior art references. As explained above, the cited portions of prior art references identified in the attached claim charts are exemplary only and representative of the content and teaching of the prior art references, and should be understood in the context of the reference as a whole and as they would be understood by a person of ordinary skill in the art.

Apple identifies the following references as anticipating one or more of the Asserted Claims of the ’962 patent under 35 U.S.C. § 102. The below table of anticipating references is exemplary, and it does not constitute an admission that any reference anticipates only the listed claims. Further, Apple contends that any prior art reference in the attached charts that is charted for each limitation of any given claim, anticipates that claim, regardless of whether that prior art reference is listed in the following table.

Exhibit No.	Anticipating Prior Art	Claims
962–A1	U.S. Patent No. 7,191,218 to Innes [“Innes”]	1–8, 10–30, 32–44

To the extent any item of prior art cited above is deemed not to disclose, explicitly or inherently, any limitation of an Asserted Claim of the ’962 patent, Apple reserves the right to argue that any difference between that prior art and the corresponding patent claim would have

been either inherent to the art, or obvious to a person of ordinary skill in the art, even if Apple has not specifically denoted that the art is to be combined with the knowledge of a person of ordinary skill in the art.

3. Obviousness

To the extent any limitation is deemed not to be exactly met by an item of prior art listed above and in **Exhibit 962-A**, then any purported differences are such that the claimed subject matter as a whole would have been obvious to one skilled in the art at the time of the alleged invention, in view of the state of the art and knowledge of those skilled in the art. The item of prior art would, therefore, render the relevant claims invalid for obviousness under 35 U.S.C. § 103.

In addition, the references identified above render one or more Asserted Claims of the '962 patent obvious when the references are read in combination with each other, and/or when read in view of the state of the art and knowledge of those skilled in the art. Each and every reference identified is also relevant to the state of the art at the time of the alleged invention. Any of the references disclosed above may be combined with one another to render obvious (and therefore invalid) each of SEVEN's Asserted Claims. Apple may rely upon a subset of the above identified references or all of the references identified above, including all references in **Exhibits 962-A, 962-B, and C**, for purposes of obviousness depending on the Court's claim construction, positions taken by SEVEN during this litigation, and further investigation and discovery.

To the extent the foregoing references are found not to anticipate the Asserted Claims, the foregoing references render the Asserted Claims obvious either alone or in combination with one or more of the other references identified above pursuant to Patent Rule 3-3(a). It would have been obvious to a person of skill in the art at the time of the alleged invention of the

Asserted Claims of the ’962 patent to combine the various references cited herein so as to disclose the Asserted Claims of the ’962 patent.

In accordance with Patent Rule 3-3(b), prior art references rendering the Asserted Claims obvious, alone or in combination with other references, are outlined below and included in **Exhibits 962-A and 962-B**, which include exemplary claim charts for the Asserted Claims of the ’962 patent showing specifically where in each reference or combinations of references each Asserted Claim is found, and an explanation of why the prior art renders the Asserted Claim obvious. Where applicable, **Exhibits 962-A and 962-B** include the motivation to combine references.

Moreover, in addition to the information contained elsewhere in these contentions and in particular **Exhibit 962-B**, Apple has identified additional motivations and reasons to combine the various references cited herein. In particular, multiple teachings, suggestions, and/or reasons to modify any of the references and/or to combine any two or more of the references in **Exhibits 962-A and 962-B** come from many sources, including the prior art (specific and as a whole), common knowledge, common sense, predictability, expectations, industry trends, design incentives or need, market demand or pressure, market forces, obvious to try, the nature of the problem faced, and/or knowledge possessed by one of ordinary skill. In addition, it would have been obvious to try combining the prior art references identified above because there were only a finite number of predictable solutions and/or because known work in one field or endeavor prompted variations based on predictable design incentives and/or market forces either in the same field or a different one. The combination of prior art references identified in these contentions would have been obvious because the claimed combinations represent the known potential options with a reasonable expectation of success. Additionally, one of ordinary skill in

the art would have been motivated to create combinations identified in these contentions using: known methods to yield predictable results; known techniques in the same way; a simple substitution of one known, equivalent element for another to obtain predictable results; and/or teaching, suggestion, or motivation in the prior art generally. Also, market forces in the industry, and the desire to improve features and performance, would motivate the addition of features to systems as they become available, become less expensive, become more commonly used, provide better performance, reduce costs, size or weight, or predictably achieve other clearly desirable results.

While Apple reserves the right to rely on any combination of the references reflected in their charts or incorporated herein by reference, Apple provides the following exemplary and non-exhaustive references and/or combinations evidencing invalidity of the claims of the Asserted Patents. The combinations of prior art listed below render obvious the Asserted Claims under the proper construction of the claims and/or under Plaintiff's apparent interpretation of the claims as set forth by Plaintiff in their Complaint and Infringement Contentions. Each combination renders the identified claims obvious through the express and/or inherent disclosure in the combination of references themselves, as well as in view of the knowledge of a person of ordinary skill in the art.

Obviousness Combinations	**Claims**
U.S. Patent No. 7,191,218 to Innes ["Innes"] in view of U.S. Patent No. 7,426,569 to Dunk ["Dunk"]	1–8, 10–30, 32–44
Innes in view of one of U.S. Patent No. 5,898,783 to Rohrbach ["Rohrbach"], U.S. Patent No. 7,054,624 to Cocita ["Cocita"], or U.S. Patent No. 7,181,252 to Komsi ["Komsi]	1–44
Innes in view of Dunk and/or one of Rohrbach, Cocita, or Komsi	1–44
Innes in view of International Pat. App. WO 00/65424 to Barrett et al. ["Barrett"]	1–8, 10–30, 32–44
Innes in view of Barrett and/or Dunk	1–8, 10–30, 32–44
Innes in view of Barrett and/or one of Rohrbach, Cocita, or Komsi	1–44

Obviousness Combinations	Claims
Innes in view of U.S. Patent Application Publication No. 2003/0149781 to Yared et al. ["Yared"]	1–8, 10–30, 32–44
Innes in view of Yared and/or Dunk	1–8, 10–30, 32–44
Innes in view of Yared and/or one of Rohrbach, Cocita, or Komsi	1–44
Yared in view of Dunk	1–8, 10–30, 32–44
Yared in view of one of Rohrbach, Cocita, or Komsi	1–44
Yared in view of Dunk and/or one of Rohrbach, Cocita, or Komsi	1–44
Yared in view of Innes	1–8, 10–30, 32–44
Yared in view of Innes and/or Dunk	1–8, 10–30, 32–44
Yared in view of Innes and/or Dunk and/or one of Rohrbach, Cocita, or Komsi	1–44
Yared in view of Barrett	1–8, 10–30, 32–44
Yared in view of Barrett and/or Dunk	1–8, 10–30, 32–44
Yared in view of Barrett and/or Dunk and/or one of Rohrbach, Cocita, or Komsi	1–44
Yared in view of Lefeber	1–8, 10–30, 32–44
Yared in view of Lefeber and/or Dunk	1–8, 10–30, 32–44
Yared in view of Lefeber and/or Dunk and/or one of Rohrbach, Cocita, or Komsi`	1–44
Yared in view of Yamamoto	1–8, 10–30, 32–44
Yared in view of Yamamoto and one of Rohrbach, Cocita, or Komsi	1–44
Yared in view of Yamamoto and/or Dunk and/or one of Rohrbach, Cocita, or Komsi	1–44
Lefeber in view of one of Rohrbach, Cocita, or Komsi	1–44
Lefeber in view of Innes	1–8, 10–30, 32–44
Lefeber in view of Barrett	1–8, 10–30, 32–44
Lefeber in view of Barriga	1–8, 10–30, 32–44
Lefeber in view of Yared	1–8, 10–30, 32–44
Microsoft .Net Passport and .Net Alert System	1–8, 10–30, 32–44
Microsoft .Net Passport and .Net Alert System in view of one of Rohrbach, Cocita, and/or Komsi	1–44

In addition to the specific combinations of prior art and the specific combinations of groups of prior art disclosed above, Apple reserves the right to rely on any other combination of any prior art references disclosed herein. Apple further reserves the right to rely upon combinations disclosed within the prosecution history of the references cited herein. These obviousness combinations reflect Apple's present understanding of the potential scope of the

claims that SEVEN appears to be advocating and should not be seen as Apple's acquiescence to SEVEN's interpretation of the patent claims.

Apple also reserves the right to amend or supplement these contentions regarding anticipation or obviousness of the Asserted Claims, in view of further information from SEVEN, information discovered during discovery, or a claim construction ruling by the Court. SEVEN has not identified what elements or combinations it alleges were not known to one of ordinary skill in the art at the time. Therefore, for any claim limitation that SEVEN alleges is not disclosed in a particular prior art reference, Apple reserves the right to assert that any such limitation is either inherent in the disclosed reference or obvious to one of ordinary skill in the art at the time in light of the same, or that the limitation is disclosed in another of the references disclosed above and in combination would have rendered the Asserted Claim obvious.

C. Patent Rule 3-3(c): Charts Identifying Where Specifically in Each Alleged Item of Prior Art Each Asserted Claim Is Found

Pursuant to Patent Rule 3-3(c), charts identifying where specifically in each alleged item of prior art each limitation of each Asserted Claim is found, including for each limitation that Apple contends is governed by 35 U.S.C. § 112(6), the identity of the structure(s), act(s), or material(s) in each item of prior art that performs the claimed function, are attached in **Exhibits 962-A and 962-B**.

D. Patent Rule 3-3(d): Other Grounds for Invalidity

Apple identifies the following grounds for invalidity of the Asserted Claims of the '962 patent based on 35 U.S.C. §§ 101 and/or 112. Apple reserves the right to supplement these disclosures based on further investigation and discovery.

1. Invalidity Pursuant to 35 U.S.C. § 112

Apple further asserts that the Asserted Claims of the '962 patent are invalid under 35 U.S.C. § 112. The following are the grounds upon which Apple contends the Asserted Claims are invalid for failure to meet the requirements of 35 U.S.C. § 112, ¶¶ 1, 2, 4 and/or 6, based on Apple's investigation to date and currently-available information.

For each claim identified as invalid, any dependent claims of those invalid claims are also invalid under 35 U.S.C. § 112, ¶¶ 1, 2, 4, and/or 6. Apple reserves the right to supplement and amend these contentions based on further discovery and investigation including, in particular, the deposition of any of the named inventors of the Asserted Patent, the parties' claim construction positions, and further investigation of SEVEN's implied infringement positions.

a) Written Description and/or Enablement

At least in view of SEVEN's apparent construction of the claims in its Infringement Contentions, the Asserted Claims of the '962 patent are invalid because the specification as filed does not contain adequate written description of the claimed inventions sufficient to lead a person of ordinary skill in the art to understand that the named inventors had possession of the purported inventions as claimed as required by 35 U.S.C. § 112, ¶ 1. Likewise, the specification does not enable one of ordinary skill in the art to make or use the claimed inventions without undue experimentation. Based on Apple's present understanding of SEVEN's infringement contentions, Apple asserts that the Asserted Claims of the of the '962 patent are invalid for reciting at least the following claim terms/phrases/limitations:

Claim 1 of the '962 patent and its dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1 because the specification as filed does not contain an adequate written description and/or enabling disclosure of "configure a service to receive data from the first data store on behalf of the client device, wherein the service is based on the second

identifier." The phrases "second identifier" and "configure a service" are not used in the '962 patent's specification, and the patent's disclosures do not otherwise describe or enable the "configure a service" limitation. Accordingly, the specification fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed. The similar limitation in claim 23, "configuring a service to receive data from the first data store on behalf of the client device, wherein the service is based on the second identifier," is deficient for the same reasons.

Claims 9 and 31 of the '962 patent are invalid for failure to satisfy the requirements of 35 U.S.C. 112, ¶ 1 because the specification as filed does not contain an adequate written description and/or enabling disclosure of "directing the client device to delete content thereon in response to an indication that the client device is misappropriated." The term "misappropriated" is not used in the specification, nor is there any disclosure of the conditions or communications which might indicate that a device has been misappropriated. Although the specification does address "data obliteration" operations, there is no enabling disclosure of how "the sever" may direct the device to accomplish such a data obliteration. The only disclosure is of unspecified "client software" and an unspecified user-initiated command. '962 patent, 17:60–18:4. The only other discussion of deletion of data appears in the context of discussing conditions under which data may be deleted from the mail server, not the mobile device. *See, e.g.*, '962 patent, 14:30–37 (discussing the conditions under which e-mail may be deleted in POP and IMAP protocols). Accordingly, the specification fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

Claims 1 and 23 and their dependent claims also lack written description support and/or are not enabled, at least to the extent that SEVEN contends the "a server" or "the server" limitations are satisfied by Apple's products. To the extent the term "a server" is construed to mean more than a specific set of computers acting as a single server, as identified in the '962 patent specification, the full scope of the claimed subject matter is not described or enabled. Accordingly, the specification fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

b) Indefiniteness

At least in view of SEVEN's apparent construction of the claims in its Infringement Contentions, the Asserted Claims of the '962 patent are invalid because they fail to particularly point out and distinctly claim the subject matter which the applicant regards as his invention under 35 U.S.C. § 112, ¶¶ 2, 4, and/or 6. Based on Apple's present understanding of SEVEN's infringement contentions, Apple asserts that the Asserted Claims of the of the '962 patent are invalid for reciting at least the following claim terms/phrases/limitations:

Independent claims 1 and 23 of the '962 patent and their dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 2, ¶ 4, and/or ¶ 6 because the specification does not describe or otherwise inform one of ordinary skill about what constitutes "a subsequent connection with the server." The '962 patent does not describe or explain how to distinguish a "subsequent connection" from any other connection, including the conditions and or timing of a "subsequent connection." As such, one of ordinary skill would not understand the metes and bounds of the identified claims, rendering them indefinite under 35 U.S.C. § 112, ¶ 2. Therefore, the Asserted Claims, when read in light of the specification and the prosecution

history, "fail to inform, with reasonable certainty, those skilled in the art about the scope of the invention." *Nautilus, Inc. v. Biosig Instruments, Inc.*, 134 S. Ct. 2120, 2124 (2014).

Claims 1 and 23 of the '962 patent and their dependent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 2, ¶ 4, and/or ¶ 6 because the specification does not describe or otherwise inform one of ordinary skill about what constitutes "a server." The '962 patent does not describe or explain how to limit an a server. According to SEVEN, a server has no bounds, including based on the amount of physical servers involved or the type of server involved, such that SEVEN would consider all servers to be one server. As such, one of ordinary skill would not understand the metes and bounds of the identified claims, rendering them indefinite under 35 U.S.C. § 112, ¶ 2. Therefore, the Asserted Claims, when read in light of the specification and the prosecution history, "fail to inform, with reasonable certainty, those skilled in the art about the scope of the invention." *Nautilus, Inc. v. Biosig Instruments, Inc.*, 134 S. Ct. 2120, 2124 (2014).

2. Other Grounds for Invalidity

In addition to the preceding invalidity contentions, Apple reserves the right to assert that the asserted patents are invalid under 35 U.S.C. §102(f) and/or (g) in the event Apple obtains evidence that the named inventors of the '962 patent did not invent (either alone or in conjunction with other parties) the subject matter claimed in the '962 patent. For example, although the '962 patent purports to be a continuation of the '176 patent and the two patents share the same specification and their claims share many of the same limitations and a terminal disclaimer to the same patent, the named inventors the differ: the '176 patent identifies Parvinder Sawhney and five others as inventors whereas the '962 patent identifies Parvinder Sawhney and one other (who was not an inventor on the '176 patent) as '962 patent inventors. The '962 patent—with fewer and different named inventors—adds limitations to those included in the

claims of the ’176 patent. SEVEN has identified no evidence from which it may be determined that inventorship is correct as to the ’962 and ’176 patent. Should Apple obtain further such evidence, it will provide the name of the person(s) from whom and the circumstances under which the invention or any part of it was derived, and/or the circumstances surrounding the making of the invention before the patent application.

Apple reserves the right to supplement these disclosures based on further investigation and discovery.

PATENT RULE 3-4 DISCLOSURES

Based on its investigation to date and its understanding of SEVEN’s infringement contentions, Apple has produced documents and has made available for inspection upon reasonable notice from SEVEN a source code computer pursuant to Patent Rule 3-4(a), which directs the production of “[s]ource code, specifications, schematics, flow charts, artwork, formulas, or other documentation sufficient to show the operation of any aspects or elements of an Accused Instrumentality identified by the patent claimant in its P.R. 3-1(c) chart.” The source code computer is available upon reasonable notice from SEVEN for inspection and review pursuant to the provisions of the Protective Order in this matter (Dkt. No. 41) at the Houston offices of Fish & Richardson P.C., 1221 McKinney Street, Suite 2800, Houston, TX 77010.

Based on its investigation to date, pursuant to P.R. 3-4(b), Apple hereby produces documents currently within its possession, custody, or control that are the prior art references identified above and/or in the attached Exhibits in connection with Apple’s P.R. 3-3 disclosures. In addition, devices, systems, publications, software, source code and related documentation not produced herewith are available upon reasonable notice from SEVEN for inspection at the Houston, Texas office of Fish & Richardson.

Apple reserves the right to identify and produce additional documents pursuant to the Patent Rules and the orders of the Court.

Dated: August 26, 2019

Respectfully submitted,

FISH & RICHARDSON P.C.

/s/ Noah C. Graubart

Ruffin Cordell (Lead Counsel)
cordell@fr.com
Texas Bar Number 04820550
Indranil Mukerji
mukerji@fr.com
Massachusetts Bar Number 644059
FISH & RICHARDSON P.C.
1000 Maine Avenue SW, Suite 1000
Washington, DC 20024
Telephone: 202-783-5070
Facsimile: 202-783-2331

Benjamin C. Elacqua
Texas Bar Number 24055443
elacqua@fr.com
Raisa Ahmad
Texas Bar Number 24101437
ahmad@fr.com
Kathryn Quisenberry
Texas Bar Number 24105639
quisenberry@fr.com
FISH & RICHARDSON P.C.
1221 McKinney Street, Suite 2800
Houston, TX 77010
Telephone: 713-654-5300
Facsimile: 713-652-0109

Betty Chen
California Bar No. 290588
bchen@fr.com
FISH & RICHARDSON P.C.
500 Arguello Street, Suite 500
Redwood City, CA 94063
Telephone: 650-839-5070
Facsimile: 650-839-5071

Noah Graubart
Georgia Bar Number 141862
graubart@fr.com
FISH & RICHARDSON P.C.
1180 Peachtree Street, NE, 21st Floor
Atlanta, GA 30309
Telephone: 404-582-5005
Facsimile: 404-582-5002

Melissa Smith
Texas Bar No.24001351
melissa@gillamsmithlaw.com
GILLAM & SMITH, LLP
303 South Washington Avenue
Marshall, Texas 75670
Telephone: 903-934-8450
Facsimile: 903-934-9257

COUNSEL FOR DEFENDANT APPLE INC.

CERTIFICATE OF SERVICE

The undersigned hereby certifies that a true and correct copy of the foregoing document was served on SEVEN through its counsel of record via email on this 26th day of August, 2019.

/s/ Noah C. Graubart
Noah C. Graubart

EXHIBIT 619-A01

Invalidity Contentions for U.S. Patent No. 10,027,619 ("the '619 patent")

Based on: International Patent Application No. WO 01/29731 to Thompson et al. ("Thompson")

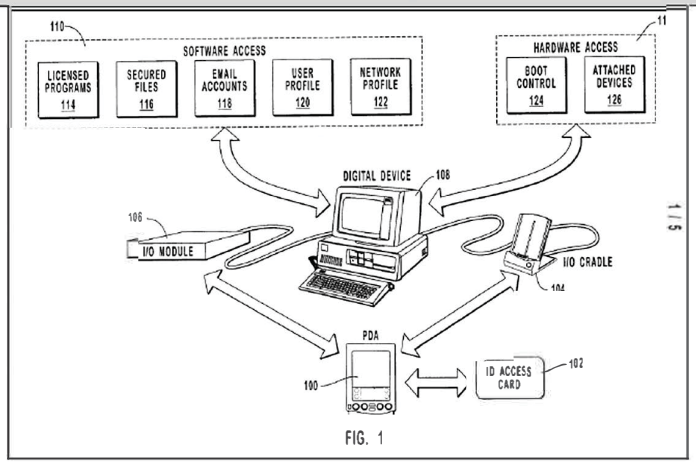
Based on SEVEN's apparent positions as to the scope of the patent's claims, as best they can be deciphered, the reference(s) charted below anticipate(s) or at least render(s) obvious the identified claims. The portions of the prior art reference cited below are not exhaustive but are exemplary in nature. Where Apple identifies a portion of the prior art reference's text, the identification should be understood as referencing any corresponding figure or diagram, and vice versa.

This disclosure is not an admission that Apple concedes any claim construction implied or suggested by SEVEN's apparent positions as to the scope of the patent's claims, nor is it an admission by Apple that any of its products are covered by or infringe the patent's claims, particularly when they are properly construed and applied. Apple is not taking any claim construction positions through this disclosure, including whether the preamble is a limitation.

Apple reserves the right to rely on additional citations or sources of evidence that also may be applicable, or that may become applicable in light of claim construction, changes in SEVEN's infringement contentions, and/or information obtained during discovery as the case progresses. Apple further reserves the right to amend or supplement this claim chart at a later date as more fully set forth in the Invalidity Contentions.

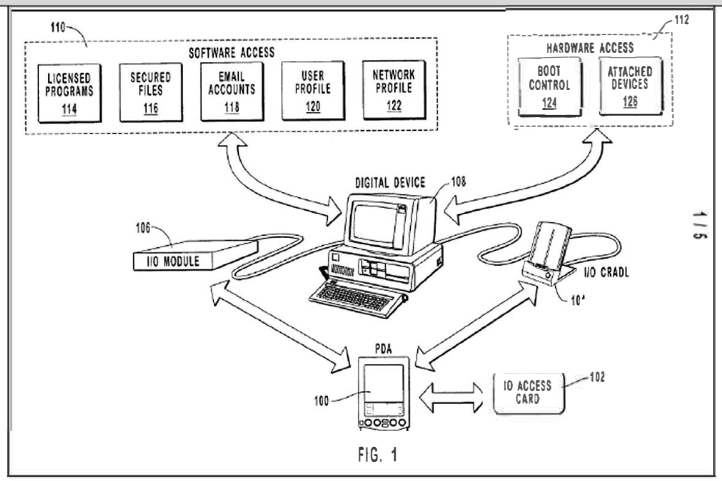
Thompson qualifies as prior art under at least pre-AIA 35 U.S.C. §§ 102(a), (b) and/or (e). Thompson is an International Patent Application that was filed on October 13, 2000 and published on April 26, 2001.

'619 Patent – Claim 22	Thompson
[22pre] A device comprising:	To the extent the preamble is limiting, Thompson discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:

’619 Patent – Claim 22	Thompson
	 FIG. 1 Thompson, Fig. 1. *See also*, Figs. 2-5. “An access control system combining PDA functionality with user authentication so that only the authorized user or users may obtain access control codes from a PDA device for an access control point. The access control point can be a computer terminal (108), a computer file, a door, a checkstand, a visa authorization point, a gate, or other situation wherein high security is desirable. In a preferred embodiment, the access control system attaches to a computer (108) via a PDA cradle (104) and transmits access control codes that include a series of authentication codes or identification codes having encoded data stored within a PDA database. In another form of the invention, user authentication is obtained by comparing biometric data such as a fingerprint with digitally stored data of the authorized user. A decision to grant access affects the release, an electronic release or electronic strike, or electronic software hold. If desired, a write feature can be included into the

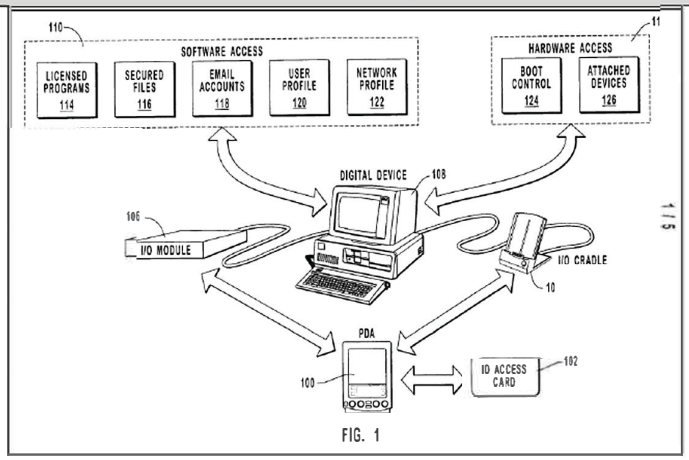
'619 Patent – Claim 22	Thompson
	system whereby each access control point accessed or attempted to be accessed by a PDA user will be recorded on the PDA to determine where access has been attempted. Additional records could be maintained along with the authentication I.D. including checking account information, credit card information, membership information, network information, user profile information (120), e-mail information (118), and personal information." Thompson at ABSTRACT. "In addition to receiving information from an I.D. access card 102, the PDA interface devices can be used to facilitate communication between the PDA 100 and a digital device 108. Various PDA interface devices are employed to communicate with devices in the outside world including, but not limited to, the standard serial RS-232 port, a parallel port, an IR port, a PDA cradle connection, a RF bandwidth transceiver, Wegand device, magnetic coding or sensor, bar code reader, USB, wireless transceiver, and laser communication. Once an interface device is selected by the PDA 100, it can either interface with an I/O module 106 or with a PDA cradle 104. These interface input/output transceivers are in electronic communication with digital device 108. Once the digital device 108 has access to the PDA 100, it can verify whether access should be granted to a user for software access 110 or hardware access 112." Thompson at 8:7-17. "1. A method for authorizing access control to digital resources of a digital device using a person digital assistant (PDA), said method comprising of the steps of: initializing a database controlled by said PDA with access control codes; requesting access to said digital resources of said digital device; relaying said access control codes upon request to said digital device; selectively authorizing access by PDA to said digital resources based on said access control codes. 2. A method as recited in claim 1, where said digital resources include: licensed executable programs, secured data files, e-mail accounts, user profiles, network

'619 Patent – Claim 22	Thompson
	profiles, and attached peripheral devices. 3. A method as recited in claim 1, wherein said access control codes are automatically relayed between the digital device and the PDA when the PDA is electronically connected with at least one of a I/O cradle or an I/O module. 4. A method as recited in claim 3, wherein said I/O module comprises at least one of a serial port, a parallel port, an IR port, a PDA cradle connection interface, an RF transceiver, a Wegand interface, 2 magnetic sensor, a bar code render, a modem, a NIC, a USB, or 2 laser communication devices." Thompson at 15:1-20. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[22a] a radio;	Thompson discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:

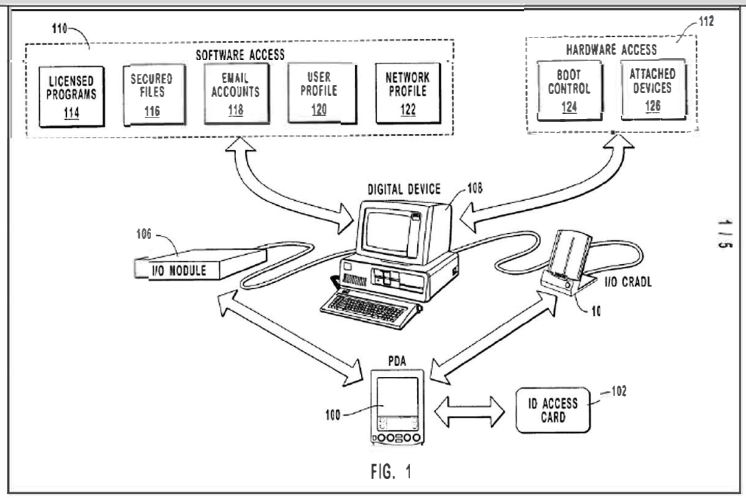
’619 Patent – Claim 22	Thompson
	 FIG. 1 Thompson, Fig. 1. *See also*, Figs. 2-5. “PDA device to selectively retrieve the information for service controllers or security outlets. The user may also enter the access control information directly to the PDA device through an interface device. The access control information includes access control codes used to enable the boot-up process for a connected digital device. These codes may also be used to authorize the transfer of funds in a commercial transaction. Access control codes can instruct the PDA device to produce the enabling or disabling signal for an electronic lock on items as diverse as a door and a secured computer file. Just as there are many different types of access control codes, there are multiple methods of delivering the codes to a service controller or security outlet. One method is through the I O cradle attached to the PDA device and the digital device. I/O cradles are usually attached to either the serial RS-232 port or the parallel port. Another interface method is between a PDA Infra-Red (IR) port and an I/O

'619 Patent – Claim 22	Thompson
	module attached to the digital device with a IR interface. A preferred embodiment of the present invention utilizes wireless transceiver, built into the PDA device to communicate with a receiver. Finally traditional interface parts, coils, or transmissions may be effectively used. These interfaces include RF, Wegand, magnetic, USB, or laser communication. A final potential embodiment includes integrating an IC chip into the digital device providing access control codes faster." Thompson at 3:34-4:17. "In addition to receiving information from an I.D. access card 102, the PDA interface devices can be used to facilitate communication between the PDA 100 and a digital device 108. Various PDA interface devices are employed to communicate with devices in the outside world including, but not limited to, the standard serial RS-232 port, a parallel port, an IR port, a PDA cradle connection, a RF bandwidth transceiver, Wegand device, magnetic coding or sensor, bar code reader, USB, wireless transceiver, and laser communication. Once an interface device is selected by the PDA 100, it can either interface with an I/O module 106 or with a PDA cradle 104. These interface input/output transceivers are in electronic communication with digital device 108. Once the digital device 108 has access to the PDA 100, it can verify whether access should be granted to a user for software access 110 or hardware access 112." Thompson at 8:7-17. "1. A method for authorizing access control to digital resources of a digital device using a person digital assistant (PDA), said method comprising of the steps of: initializing a database controlled by said PDA with access control codes; requesting access to said digital resources of said digital device; relaying said access control codes upon request to said digital device; selectively authorizing access by PDA to said digital resources based on said access control codes. 2. A method as recited in claim 1, where said digital resources include: licensed executable programs, secured data files, e-mail accounts, user profiles, network

'619 Patent – Claim 22	Thompson
	profiles, and attached peripheral devices. 3. A method as recited in claim 1, wherein said access control codes are automatically relayed between the digital device and the PDA when the PDA is electronically connected with at least one of a I/O cradle or an I/O module. 4. A method as recited in claim 3, wherein said I/O module comprises at least one of a serial port, a parallel port, an IR port, a PDA cradle connection interface, an RF transceiver, a Wegand interface, 2 magnetic sensor, a bar code render, a modem, a NIC, a USB, or 2 laser communication devices." Thompson at 15:1-20. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[22b] a processor and memory containing instructions executable by the processor whereby the device is operable to:	Thompson discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:

’619 Patent – Claim 22	Thompson
	 FIG. 1 Thompson, Fig. 1. *See also*, Figs. 2-5. “An access control system combining PDA functionality with user authentication so that only the authorized user or users may obtain access control codes from a PDA device for an access control point. The access control point can be a computer terminal (108) , a computer file, a door, a checkstand, a visa authorization point, a gate, or other situation wherein high security is desirable. In a preferred embodiment, the access control system attaches to a computer (108) via a PDA cradle (104) and transmits access control codes that include a series of authentication codes or identification codes having encoded data stored within a PDA database. In another form of the invention, user authentication is obtained by comparing biometric data such as a fingerprint with digitally stored data of the authorized user. A decision to grant access affects the release, an electronic release or electronic strike, or electronic software hold. If desired, a write feature can be included into the

'619 Patent – Claim 22	Thompson
	system whereby each access control point accessed or attempted to be accessed by a PDA user will be recorded on the PDA to determine where access has been attempted. Additional records could be maintained along with the authentication I.D. including checking account information, credit card information, membership information, network information, user profile information (120), e-mail information (118), and personal information." Thompson at ABSTRACT. "The system and method of the present invention utilize a PDA device to provide improved access control for a user. According to the present invention, a PDA device is programmed to provide various access control codes to multiple security outlets or service controllers, specifically including access codes for: desktop computers during the boot up process, selective secured computer data files, protected or licensed programs, mechanical hardware such as those used with electronic latch doors, and service identification numbers such as credit card numbers and checking accounts." Thompson at 3:27-33. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[22c] optically receive information including a displayed service activation code from a remote device;	Thompson discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:

’619 Patent – Claim 22	Thompson
	 FIG. 1 Thompson, Fig. 1. *See also*, Figs. 2-5. “An access control system combining PDA functionality with user authentication so that only the authorized user or users may obtain access control codes from a PDA device for an access control point. The access control point can be a computer terminal (108) , a computer file, a door, a checkstand, a visa authorization point, a gate, or other situation wherein high security is desirable. In a preferred embodiment, the access control system attaches to a computer (108) via a PDA cradle (104) and transmits access control codes that include a series of authentication codes or identification codes having encoded data stored within a PDA database. In another form of the invention, user authentication is obtained by comparing biometric data such as a fingerprint with digitally stored data of the authorized user. A decision to grant access affects the release, an electronic release or electronic strike, or

'619 Patent – Claim 22	Thompson
	electronic software hold. If desired, a write feature can be included into the system whereby each access control point accessed or attempted to be accessed by a PDA user will be recorded on the PDA to determine where access has been attempted. Additional records could be maintained along with the authentication I.D. including checking account information, credit card information, membership information, network information, user profile information (120), e-mail information (118), and personal information." Thompson at ABSTRACT. "Examples of computer data felt to require access control include secure files, personalized e-mail accounts, specific user profiles, specific network profiles, and access to licensed programs. A secure file may be created by a user encrypting the file with a password. E-mail accounts obtain limited security by archiving data into personalized data structures or by password protecting e-mail access. Access to specific user profiles and network profiles are often controlled by operating system passwords. Many licensed programs require that only a specific quantity of users within a company be granted access and that additional users are not allowed access to these program. This regulation is generally accomplished by either assigning an access control code to each authorized user or the licensed program may regulate a hard quantity limitation on the total number of copies of the program that can be running from a server at any one time. By focusing on access control mechanisms surrounding the files, productivity and efficiency are reduced. These problems are enhanced if an individual user regularly switches work station locations to different access points within the company. Hence, a portable system which provides all file, user, network, or licensing authentication for a particular user would be useful for a corporation in managing its computer usage or license usages and would increase the efficiency and productivity of the user. Not to mention the added benefit of no longer needing to remember all the passwords used for each "secure" application." Thompson at 2:11-29. "A variety of access control systems and devices presently exist, however;

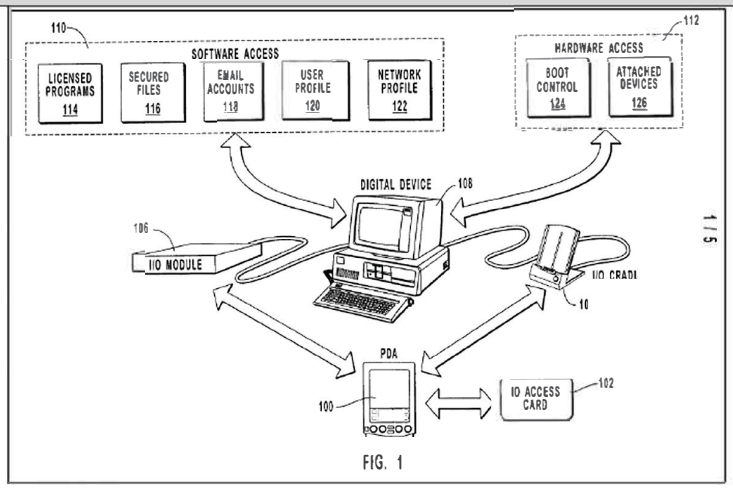
'619 Patent – Claim 22	Thompson
	these access control systems do not interface or coordinate with PDA devices. Specifically, a user attempting to gain access to various resources within a company is often required to carry an access card, an access key, or an I.D. access badge. The user may be required to know an access number, a PIN number, a combination, a password, or to provide a computer authorization number. In addition to these standard electronic and mechanical access control devices, some high security areas require an individual to provide specific biometric information such as fingerprint verification or a retinal scan. A system that provides all of the necessary access control information using a PDA device as a substitute for the aforementioned keys, cards, or passwords would considerably lessen the security delays and inefficiencies created by the multiple verification devices presently required to obtain site access authorization, not to mention the additional benefit of drastically reducing the extent and magnitude of security access devices necessary for any one individual to carry with them." Thompson at 2:30-3:8. "PDA device to selectively retrieve the information for service controllers or security outlets. The user may also enter the access control information directly to the PDA device through an interface device. The access control information includes access control codes used to enable the boot-up process for a connected digital device. These codes may also be used to authorize the transfer of funds in a commercial transaction. Access control codes can instruct the PDA device to produce the enabling or disabling signal for an electronic lock on items as diverse as a door and a secured computer file. Just as there are many different types of access control codes, there are multiple methods of delivering the codes to a service controller or security outlet. One method is through the I O cradle attached to the PDA device and the digital device. I/O cradles are usually attached to either the serial RS-232 port or the parallel port. Another interface method is between a PDA Infra-Red (IR) port and an I/O module attached to the digital device with a IR interface. A preferred embodiment of the present invention utilizes wireless transceiver, built into the PDA device to communicate with a receiver. Finally traditional interface parts,

'619 Patent – Claim 22	Thompson
	coils, or transmissions may be effectively used. These interfaces include RF, Wegand, magnetic, USB, or laser communication. A final potential embodiment includes integrating an IC chip into the digital device providing access control codes faster." Thompson at 3:34-4:17. "In one embodiment, the system and method of the present invention provides all the file, user, network, or licensing authentication necessary for a particular user. Once the PDA device is plugged into an I/O cradle, all of the necessary password verification or authentication is supplied by the PDA device. A less memory intensive approach calls for the storage of a solitary password within the PDA access control database which downloads a user profile from a network location. Additional security checks could be implemented to verify that the PDA device holder is the actual user without negatively affecting the efficiency and productivity of the user because of the overall reduction in the number of access control codes. Another embodiment maintains communication between the PDA device and the digital device through an I/O module, such as a wireless transceiver or IR port. If a wireless transceiver is used, the PDA device can download information from the user's workstation at any time or from any location. The wireless PDA device embodiment could alert a user when someone is attempting unauthorized access to the user's computer. Another embodiment utilizes the PDA device to provide the access control codes for a user and then retrieves a customized user desktop setting for the user specified by the PDA device. This feature allows an individual user to attach to any computer within a company's network and obtain their customized desktop. This feature allows for incredible flexibility and versatility, not to mention the added benefit of no longer needing to remember all the passwords used for each "secure" application." Thompson at 4:18-36. "Figure 1 provides an overview illustrating the use of a PDA device to control software and hardware access electronically connected to a digital device. A PDA 100 interfaces with an I.D. access card 102. The I.D. access card 102 may be in permanent, removable, or flexible communication with the PDA 100. A

'619 Patent – Claim 22	Thompson
	permanent connection is demonstrated by the addition of a chip which is installed within the PDA 100. The chip method has been established in other applications, but it has not been applied to PDA devices specifically in regards to access control or security features. If an IC chip is added to the PDA 100, the IC chip will have access to the PDA interfaces to the outside world through the PDA's processor. One embodiment would use the PDA's processor to read access numbers from the security chip and transmit the number to the device making the query. The querying device could then compare the transmitted number to its database to see if it was an acceptable number. Upon comparison of the devices the querying device could either accept or refuse access to its function e.g., building entry, computer access, transactional support, or purchasing. Removable communication generally involves attaching the I.D. access card 102 to an interface on the PDA 100 for a limited time period to either download access control database or to program an access control extension. Examples would include serial cables, PDA cradles, hard coded memory cards, PCMCIA cards, disks, Wegand devices, or other encoding equipment. Once the I.D. access card 102 contacts the PDA 100, it provides either secured data structures or an encrypted I.D. database that can be verified later by local controller access points. One embodiment uses the I.D. access card 102 by attaching the card or similar device to the PDA 100 through a clip-on method. Appropriate hardware and software could be added so that when a query was made on the interface to the outside world, the PDA's processor would read the number from the security card and transmit to the device making the query. The querying device could authorize the PDA request based on a successful comparison of the transmitted number to the querying device's database. Examples of some PDA access control requests include: building entry, computer access, car entry, purchasing transactions, goods, etc." Thompson at 7:6-19. "In addition to receiving information from an I.D. access card 102, the PDA interface devices can be used to facilitate communication between the PDA 100 and a digital device 108. Various PDA interface devices are employed to

'619 Patent – Claim 22	Thompson
	communicate with devices in the outside world including, but not limited to, the standard serial RS-232 port, a parallel port, an IR port, a PDA cradle connection, a RF bandwidth transceiver, Wegand device, magnetic coding or sensor, bar code reader, USB, wireless transceiver, and laser communication. Once an interface device is selected by the PDA 100, it can either interface with an I/O module 106 or with a PDA cradle 104. These interface input/output transceivers are in electronic communication with digital device 108. Once the digital device 108 has access to the PDA 100, it can verify whether access should be granted to a user for software access 110 or hardware access 112." Thompson at 8:7-17. "1. A method for authorizing access control to digital resources of a digital device using a person digital assistant (PDA), said method comprising of the steps of: initializing a database controlled by said PDA with access control codes; requesting access to said digital resources of said digital device; relaying said access control codes upon request to said digital device; selectively authorizing access by PDA to said digital resources based on said access control codes. 2. A method as recited in claim 1, where said digital resources include: licensed executable programs, secured data files, e-mail accounts, user profiles, network profiles, and attached peripheral devices. 3. A method as recited in claim 1, wherein said access control codes are automatically relayed between the digital device and the PDA when the PDA is electronically connected with at least one of a I/O cradle or an I/O module. 4. A method as recited in claim 3, wherein said I/O module comprises at least one of a serial port, a parallel port, an IR port, a PDA cradle connection interface, an RF transceiver, a Wegand interface, 2 magnetic sensor, a bar code render, a modem, a NIC, a USB, or 2 laser communication devices." Thompson at 15:1-20.

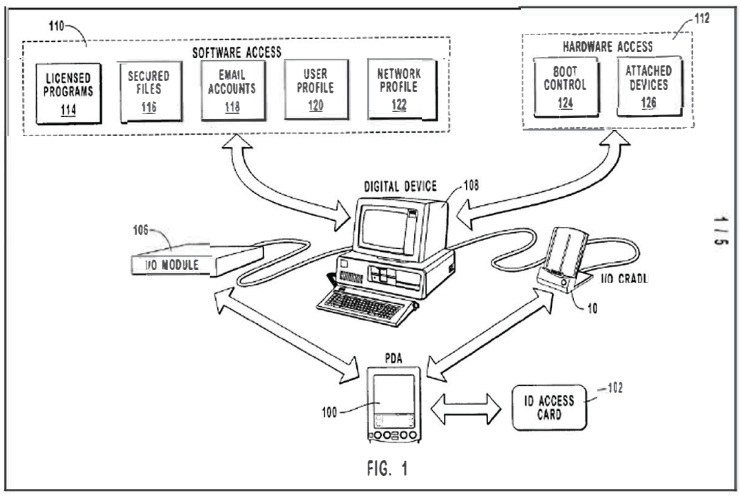
'619 Patent – Claim 22	Thompson
	"The system and method of the present invention utilize a PDA device to provide improved access control for a user. According to the present invention, a PDA device is programmed to provide various access control codes to multiple security outlets or service controllers, specifically including access codes for: desktop computers during the boot up process, selective secured computer data files, protected or licensed programs, mechanical hardware such as those used with electronic latch doors, and service identification numbers such as credit card numbers and checking accounts." Thompson at 3:27-33. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[22d] register the remote device for access to a messaging account using the service activation code;	Thompson discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:

’619 Patent – Claim 22	Thompson
	 FIG. 1 Thompson, Fig. 1. *See also*, Figs. 2-5. “An access control system combining PDA functionality with user authentication so that only the authorized user or users may obtain access control codes from a PDA device for an access control point. The access control point can be a computer terminal (108) , a computer file, a door, a checkstand, a visa authorization point, a gate, or other situation wherein high security is desirable. In a preferred embodiment, the access control system attaches to a computer (108) via a PDA cradle (104) and transmits access control codes that include a series of authentication codes or identification codes having encoded data stored within a PDA database. In another form of the invention, user authentication is obtained by comparing biometric data such as a fingerprint with digitally stored data of the authorized user. A decision to grant access affects the release, an electronic release or electronic strike, or

'619 Patent – Claim 22	Thompson
	electronic software hold. If desired, a write feature can be included into the system whereby each access control point accessed or attempted to be accessed by a PDA user will be recorded on the PDA to determine where access has been attempted. Additional records could be maintained along with the authentication I.D. including checking account information, credit card information, membership information, network information, user profile information (120), e-mail information (118), and personal information." Thompson at ABSTRACT. "In one embodiment, special booting software is installed on a computer so that if the PDA device is not in the cradle, the computer can not be accessed. An access card code interface could also be used for protecting e-mail and communications between computers by requiring the PDA device to be in its cradle or near its receptor before access control would be allowed. This system would add security by controlling access to all things controlled or accessed by the PDA device, without requiring unnecessary security to impede the process. Various software access 110 features include inquiring whether the individual has approval to use licensed programs 114, whether approval exists to secured files 116, whether access should be granted to personal e-mail accounts 118, whether a specific user profile 120 should replace the standard desktop profile, and if a network profile 122 exists for a particular user. The network profile 122 could be stored on a central computer and, upon verification of a PDA 100 within an I/O cradle 108 at a particular digital device 108 access and rights and privileges to network, drives, data, and resources could be granted to the individual user, thereby allowing him to use local printers, fax machines, and other local facilities but also providing him with access to printers at his home location. In essence, the user would only need to plug his PDA 100 into I/O cradle 104 or interface with I/O module 106 to obtain personalized access throughout a company's LAN or WAN network." Thompson at 8:18-35. "Figure 3 is a block diagram of an access control protocol that can be applied to software or hardware access. The access control protocol is initiated in

'619 Patent – Claim 22	Thompson
	execution block 300 whenever there is a request to access of an access control protocol that can be applied to software or hardware access. A protected software or hardware resource, such as e- mail or a protected file. At this point, a subprotocol initiates the security confirmation protocol which prevents the program from providing access or from loading further until the PDA has been verified. In decision block 302, the protocol discovers whether the PDA is connected. If the authorized PDA is not connected, execution block 304 prompts the user to connected the appropriate PDA to the computer. Once the PDA is connected, execution block 306 exchanges of identification information. Decision block 308 determines whether the exchanged identification information is valid. If the information is valid, then execution block 310 allows access to the file, e-mail, or other computer software or hardware resource. If it is not valid, then the access control protocol ends without giving access to the file. This access control protocol allows users to access their files on a common computer shared with multiple users. E-mail files are optionally loaded directly down to the PDA once the identification authorization has been made. Additionally, a user could use a traveling work station in which he was only required to carry his PDA containing the appropriate identification information to request from the network server the user's standard desktop and access to the user's e-mail files. As a result, a traveler could go to a foreign office or another work site location, plug his PDA into the control port and be granted access to the computer with the same restrictions and limitations that he may have had at his workstation at home." Thompson at 9:30-10:15. "1. A method for authorizing access control to digital resources of a digital device using a person digital assistant (PDA), said method comprising of the steps of: initializing a database controlled by said PDA with access control codes; requesting access to said digital resources of said digital device; relaying said access control codes upon request to said digital device; selectively authorizing access by PDA to said digital resources based on said access

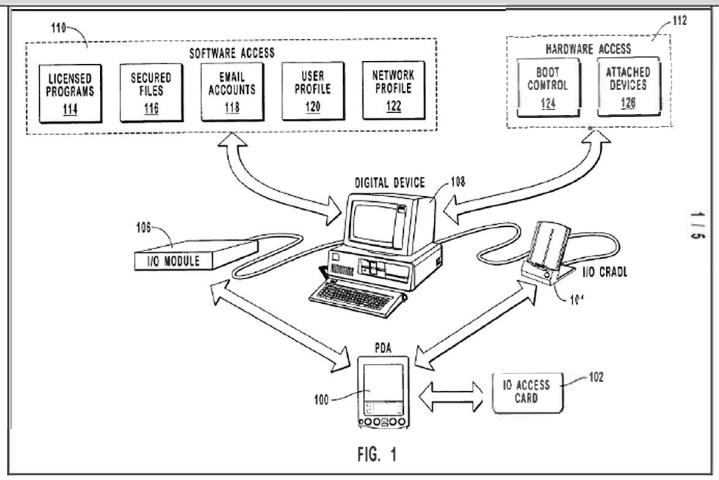
'619 Patent – Claim 22	Thompson
	control codes. 2. A method as recited in claim 1, where said digital resources include: licensed executable programs, secured data files, e-mail accounts, user profiles, network profiles, and attached peripheral devices. 3. A method as recited in claim 1, wherein said access control codes are automatically relayed between the digital device and the PDA when the PDA is electronically connected with at least one of a I/O cradle or an I/O module. 4. A method as recited in claim 3, wherein said I/O module comprises at least one of a serial port, a parallel port, an IR port, a PDA cradle connection interface, an RF transceiver, a Wegand interface, 2 magnetic sensor, a bar code render, a modem, a NIC, a USB, or 2 laser communication devices." Thompson at 15:1-20. "The present invention provides access control codes to multiple security outlets or service controllers through a PDA device. If the codes are accepted the digital device releases access to a requested resource. This release includes access to: desktop computers for boot up, selective computer data or programs, mechanical hardware such as electronic doors, and service identification numbers such as credit card numbers and checking accounts. Additionally, one embodiment of the invention is a portable system which provides all file, user, network, or licensing authentication for a particular user." Thompson at 5:33-6:3. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and

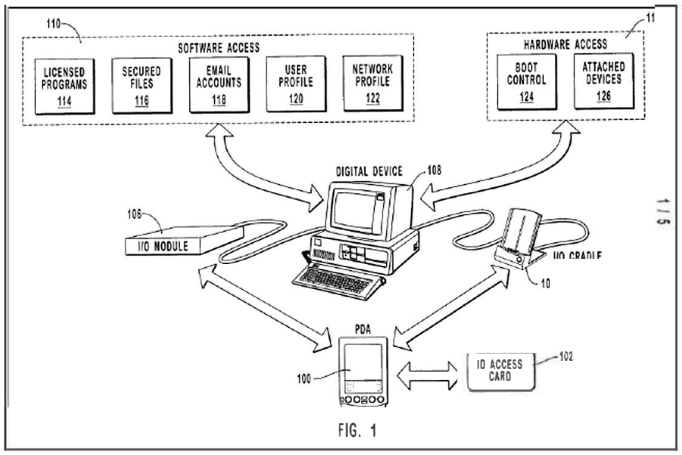
’619 Patent – Claim 22	Thompson
	Exhibit 619-B.
[22e] receive a message for the messaging account;	Thompson discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:  FIG. 1 Thompson, Fig. 1. *See also*, Figs. 2-5. “An access control system combining PDA functionality with user authentication so that only the authorized user or users may obtain access control codes from a PDA device for an access control point. The access control point can be a computer terminal (108) , a computer file, a door, a checkstand, a visa authorization point, a gate, or other situation wherein high security is desirable. In a preferred embodiment, the access control system attaches to a computer (108) via a PDA cradle (104) and transmits access

'619 Patent – Claim 22	Thompson
	control codes that include a series of authentication codes or identification codes having encoded data stored within a PDA database. In another form of the invention, user authentication is obtained by comparing biometric data such as a fingerprint with digitally stored data of the authorized user. A decision to grant access affects the release, an electronic release or electronic strike, or electronic software hold. If desired, a write feature can be included into the system whereby each access control point accessed or attempted to be accessed by a PDA user will be recorded on the PDA to determine where access has been attempted. Additional records could be maintained along with the authentication I.D. including checking account information, credit card information, membership information, network information, user profile information (120), e-mail information (118), and personal information." Thompson at ABSTRACT. "In one embodiment, special booting software is installed on a computer so that if the PDA device is not in the cradle, the computer can not be accessed. An access card code interface could also be used for protecting e-mail and communications between computers by requiring the PDA device to be in its cradle or near its receptor before access control would be allowed. This system would add security by controlling access to all things controlled or accessed by the PDA device, without requiring unnecessary security to impede the process. Various software access 110 features include inquiring whether the individual has approval to use licensed programs 114, whether approval exists to secured files 116, whether access should be granted to personal e-mail accounts 118, whether a specific user profile 120 should replace the standard desktop profile, and if a network profile 122 exists for a particular user. The network profile 122 could be stored on a central computer and, upon verification of a PDA 100 within an I/O cradle 108 at a particular digital device 108 access and rights and privileges to network, drives, data, and resources could be granted to the individual user, thereby allowing him to use local printers, fax machines, and other local facilities but also providing him with access to printers at his home location. In essence, the user would only need to plug his PDA 100 into I/O

'619 Patent – Claim 22	Thompson
	cradle 104 or interface with I/O module 106 to obtain personalized access throughout a company's LAN or WAN network." Thompson at 8:18-35. "Figure 3 is a block diagram of an access control protocol that can be applied to software or hardware access. The access control protocol is initiated in execution block 300 whenever there is a request to access of an access control protocol that can be applied to software or hardware access. A protected software or hardware resource, such as e- mail or a protected file. At this point, a subprotocol initiates the security confirmation protocol which prevents the program from providing access or from loading further until the PDA has been verified. In decision block 302, the protocol discovers whether the PDA is connected. If the authorized PDA is not connected, execution block 304 prompts the user to connected the appropriate PDA to the computer. Once the PDA is connected, execution block 306 exchanges of identification information. Decision block 308 determines whether the exchanged identification information is valid. If the information is valid, then execution block 310 allows access to the file, e-mail, or other computer software or hardware resource. If it is not valid, then the access control protocol ends without giving access to the file. This access control protocol allows users to access their files on a common computer shared with multiple users. E-mail files are optionally loaded directly down to the PDA once the identification authorization has been made. Additionally, a user could use a traveling work station in which he was only required to carry his PDA containing the appropriate identification information to request from the network server the user's standard desktop and access to the user's e-mail files. As a result, a traveler could go to a foreign office or another work site location, plug his PDA into the control port and be granted access to the computer with the same restrictions and limitations that he may have had at his workstation at home." Thompson at 9:30-10:15. "1. A method for authorizing access control to digital resources of a digital device using a person digital assistant (PDA), said method comprising of the

'619 Patent – Claim 22	Thompson
	steps of: initializing a database controlled by said PDA with access control codes; requesting access to said digital resources of said digital device; relaying said access control codes upon request to said digital device; selectively authorizing access by PDA to said digital resources based on said access control codes. 2. A method as recited in claim 1, where said digital resources include: licensed executable programs, secured data files, e-mail accounts, user profiles, network profiles, and attached peripheral devices. 3. A method as recited in claim 1, wherein said access control codes are automatically relayed between the digital device and the PDA when the PDA is electronically connected with at least one of a I/O cradle or an I/O module. 4. A method as recited in claim 3, wherein said I/O module comprises at least one of a serial port, a parallel port, an IR port, a PDA cradle connection interface, an RF transceiver, a Wegand interface, 2 magnetic sensor, a bar code render, a modem, a NIC, a USB, or 2 laser communication devices." Thompson at 15:1-20. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[22f] encrypt the message using an encryption key; and	Thompson discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:

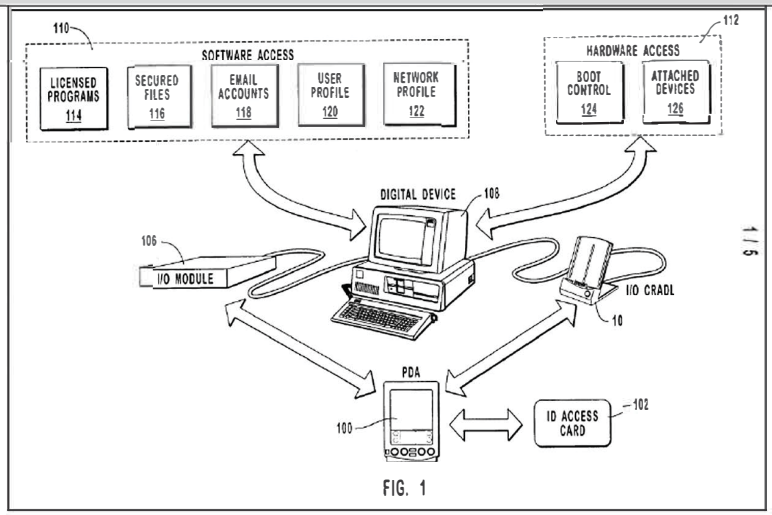
’619 Patent – Claim 22	Thompson
	 FIG. 1 Thompson, Fig. 1. *See also*, Figs. 2-5. “Examples of computer data felt to require access control include secure files, personalized e-mail accounts, specific user profiles, specific network profiles, and access to licensed programs. A secure file may be created by a user encrypting the file with a password. E-mail accounts obtain limited security by archiving data into personalized data structures or by password protecting e-mail access.” Thompson at 2:11-29. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine

’619 Patent – Claim 22	Thompson
	references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[22g] send the message to the remote device,	Thompson discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:  FIG. 1 Thompson, Fig. 1. *See also*, Figs. 2-5. “An access control system combining PDA functionality with user authentication so that only the authorized user or users may obtain access control codes from a PDA device for an access control point. The access control point can be a computer terminal (108) , a computer file, a door, a checkstand, a visa authorization point, a gate, or other situation wherein high security is desirable. In a preferred embodiment, the access control system attaches to a computer (108) via a PDA cradle (104) and transmits access control codes that include a series of authentication codes or identification

’619 Patent – Claim 22	Thompson
	codes having encoded data stored within a PDA database. In another form of the invention, user authentication is obtained by comparing biometric data such as a fingerprint with digitally stored data of the authorized user. A decision to grant access affects the release, an electronic release or electronic strike, or electronic software hold. If desired, a write feature can be included into the system whereby each access control point accessed or attempted to be accessed by a PDA user will be recorded on the PDA to determine where access has been attempted. Additional records could be maintained along with the authentication I.D. including checking account information, credit card information, membership information, network information, user profile information (120), e-mail information (118), and personal information.” Thompson at ABSTRACT. “In one embodiment, special booting software is installed on a computer so that if the PDA device is not in the cradle, the computer can not be accessed. An access card code interface could also be used for protecting e-mail and communications between computers by requiring the PDA device to be in its cradle or near its receptor before access control would be allowed. This system would add security by controlling access to all things controlled or accessed by the PDA device, without requiring unnecessary security to impede the process. Various software access 110 features include inquiring whether the individual has approval to use licensed programs 114, whether approval exists to secured files 116, whether access should be granted to personal e-mail accounts 118, whether a specific user profile 120 should replace the standard desktop profile, and if a network profile 122 exists for a particular user. The network profile 122 could be stored on a central computer and, upon verification of a PDA 100 within an I/O cradle 108 at a particular digital device 108 access and rights and privileges to network, drives, data, and resources could be granted to the individual user, thereby allowing him to use local printers, fax machines, and other local facilities but also providing him with access to printers at his home location. In essence, the user would only need to plug his PDA 100 into I/O cradle 104 or interface with I/O module 106 to obtain personalized access

'619 Patent – Claim 22	Thompson
	throughout a company's LAN or WAN network." Thompson at 8:18-35. "Figure 3 is a block diagram of an access control protocol that can be applied to software or hardware access. The access control protocol is initiated in execution block 300 whenever there is a request to access of an access control protocol that can be applied to software or hardware access. A protected software or hardware resource, such as e- mail or a protected file. At this point, a subprotocol initiates the security confirmation protocol which prevents the program from providing access or from loading further until the PDA has been verified. In decision block 302, the protocol discovers whether the PDA is connected. If the authorized PDA is not connected, execution block 304 prompts the user to connected the appropriate PDA to the computer. Once the PDA is connected, execution block 306 exchanges of identification information. Decision block 308 determines whether the exchanged identification information is valid. If the information is valid, then execution block 310 allows access to the file, e-mail, or other computer software or hardware resource. If it is not valid, then the access control protocol ends without giving access to the file. This access control protocol allows users to access their files on a common computer shared with multiple users. E-mail files are optionally loaded directly down to the PDA once the identification authorization has been made. Additionally, a user could use a traveling work station in which he was only required to carry his PDA containing the appropriate identification information to request from the network server the user's standard desktop and access to the user's e-mail files. As a result, a traveler could go to a foreign office or another work site location, plug his PDA into the control port and be granted access to the computer with the same restrictions and limitations that he may have had at his workstation at home." Thompson at 9:30-10:15. "1. A method for authorizing access control to digital resources of a digital device using a person digital assistant (PDA), said method comprising of the steps of: initializing a database controlled by said PDA with access control

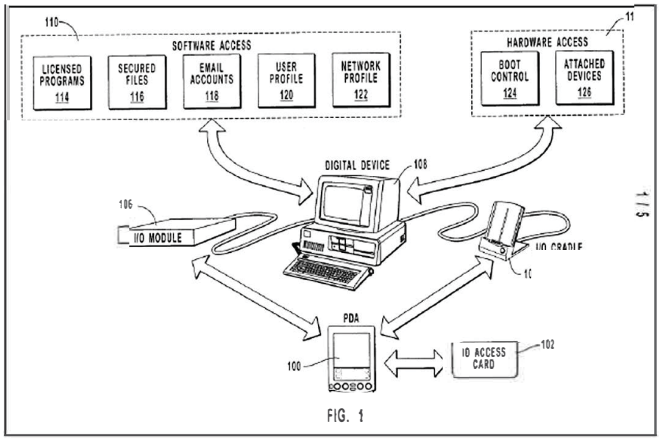
'619 Patent – Claim 22	Thompson
	codes; requesting access to said digital resources of said digital device; relaying said access control codes upon request to said digital device; selectively authorizing access by PDA to said digital resources based on said access control codes. 2. A method as recited in claim 1, where said digital resources include: licensed executable programs, secured data files, e-mail accounts, user profiles, network profiles, and attached peripheral devices. 3. A method as recited in claim 1, wherein said access control codes are automatically relayed between the digital device and the PDA when the PDA is electronically connected with at least one of a I/O cradle or an I/O module. 4. A method as recited in claim 3, wherein said I/O module comprises at least one of a serial port, a parallel port, an IR port, a PDA cradle connection interface, an RF transceiver, a Wegand interface, 2 magnetic sensor, a bar code render, a modem, a NIC, a USB, or 2 laser communication devices." Thompson at 15:1-20. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[22h] wherein the device is authenticated to access the messaging account.	Thompson discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:

’619 Patent – Claim 22	Thompson
	 FIG. 1 Thompson, Fig. 1. *See also*, Figs. 2-5. “An access control system combining PDA functionality with user authentication so that only the authorized user or users may obtain access control codes from a PDA device for an access control point. The access control point can be a computer terminal (108) , a computer file, a door, a checkstand, a visa authorization point, a gate, or other situation wherein high security is desirable. In a preferred embodiment, the access control system attaches to a computer (108) via a PDA cradle (104) and transmits access control codes that include a series of authentication codes or identification codes having encoded data stored within a PDA database. In another form of the invention, user authentication is obtained by comparing biometric data such as a fingerprint with digitally stored data of the authorized user. A decision to

'619 Patent – Claim 22	Thompson
	grant access affects the release, an electronic release or electronic strike, or electronic software hold. If desired, a write feature can be included into the system whereby each access control point accessed or attempted to be accessed by a PDA user will be recorded on the PDA to determine where access has been attempted. Additional records could be maintained along with the authentication I.D. including checking account information, credit card information, membership information, network information, user profile information (120), e-mail information (118), and personal information." Thompson at ABSTRACT. "In one embodiment, special booting software is installed on a computer so that if the PDA device is not in the cradle, the computer can not be accessed. An access card code interface could also be used for protecting e-mail and communications between computers by requiring the PDA device to be in its cradle or near its receptor before access control would be allowed. This system would add security by controlling access to all things controlled or accessed by the PDA device, without requiring unnecessary security to impede the process. Various software access 110 features include inquiring whether the individual has approval to use licensed programs 114, whether approval exists to secured files 116, whether access should be granted to personal e-mail accounts 118, whether a specific user profile 120 should replace the standard desktop profile, and if a network profile 122 exists for a particular user. The network profile 122 could be stored on a central computer and, upon verification of a PDA 100 within an I/O cradle 108 at a particular digital device 108 access and rights and privileges to network, drives, data, and resources could be granted to the individual user, thereby allowing him to use local printers, fax machines, and other local facilities but also providing him with access to printers at his home location. In essence, the user would only need to plug his PDA 100 into I/O cradle 104 or interface with I/O module 106 to obtain personalized access throughout a company's LAN or WAN network." Thompson at 8:18-35. "Figure 3 is a block diagram of an access control protocol that can be applied to

’619 Patent – Claim 22	Thompson
	software or hardware access. The access control protocol is initiated in execution block 300 whenever there is a request to access of an access control protocol that can be applied to software or hardware access. A protected software or hardware resource, such as e- mail or a protected file. At this point, a subprotocol initiates the security confirmation protocol which prevents the program from providing access or from loading further until the PDA has been verified. In decision block 302, the protocol discovers whether the PDA is connected. If the authorized PDA is not connected, execution block 304 prompts the user to connected the appropriate PDA to the computer. Once the PDA is connected, execution block 306 exchanges of identification information. Decision block 308 determines whether the exchanged identification information is valid. If the information is valid, then execution block 310 allows access to the file, e-mail, or other computer software or hardware resource. If it is not valid, then the access control protocol ends without giving access to the file. This access control protocol allows users to access their files on a common computer shared with multiple users. E-mail files are optionally loaded directly down to the PDA once the identification authorization has been made. Additionally, a user could use a traveling work station in which he was only required to carry his PDA containing the appropriate identification information to request from the network server the user's standard desktop and access to the user's e-mail files. As a result, a traveler could go to a foreign office or another work site location, plug his PDA into the control port and be granted access to the computer with the same restrictions and limitations that he may have had at his workstation at home.” Thompson at 9:30-10:15. “1. A method for authorizing access control to digital resources of a digital device using a person digital assistant (PDA), said method comprising of the steps of: initializing a database controlled by said PDA with access control codes; requesting access to said digital resources of said digital device; relaying said access control codes upon request to said digital device; selectively authorizing access by PDA to said digital resources based on said access

'619 Patent – Claim 22	Thompson
	control codes. 2. A method as recited in claim 1, where said digital resources include: licensed executable programs, secured data files, e-mail accounts, user profiles, network profiles, and attached peripheral devices. 3. A method as recited in claim 1, wherein said access control codes are automatically relayed between the digital device and the PDA when the PDA is electronically connected with at least one of a I/O cradle or an I/O module. 4. A method as recited in claim 3, wherein said I/O module comprises at least one of a serial port, a parallel port, an IR port, a PDA cradle connection interface, an RF transceiver, a Wegand interface, 2 magnetic sensor, a bar code render, a modem, a NIC, a USB, or 2 laser communication devices." Thompson at 15:1-20. "Whereas, a key required that a specific key be used on a specific machine, boot control 124 is applied to the entire computer network. Hardware access 112 also extends to attached devices 126 electrically finked or controlled by digital device 108. Attached devices 126 may include local printers, local modems, local network access, local e-mail access, local infra-red transceivers and various other attached devices like scanners, digital cameras, wireless links, main frame connections, etc." Thompson at 9:5-14. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

'619 Patent – Claim 23	Thompson
[23] The device of claim 22, wherein the information including the service activation code is received by the device in response to user input at the remote device.	Thompson discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22pre]-[22h], *above*.  FIG. 1 Thompson, Fig. 1. *See also*, Figs. 2-5. "An access control system combining PDA functionality with user authentication so that only the authorized user or users may obtain access control codes from a PDA device for an access control point. The access control point can be a computer terminal (108) , a computer file, a door, a checkstand, a visa authorization point, a gate, or other situation wherein high security is desirable. In a preferred embodiment, the access control system attaches to a computer (108) via a PDA cradle (104) and transmits access control codes that include a series of authentication codes or identification

'619 Patent – Claim 23	Thompson
	codes having encoded data stored within a PDA database. In another form of the invention, user authentication is obtained by comparing biometric data such as a fingerprint with digitally stored data of the authorized user. A decision to grant access affects the release, an electronic release or electronic strike, or electronic software hold. If desired, a write feature can be included into the system whereby each access control point accessed or attempted to be accessed by a PDA user will be recorded on the PDA to determine where access has been attempted. Additional records could be maintained along with the authentication I.D. including checking account information, credit card information, membership information, network information, user profile information (120), e-mail information (118), and personal information." Thompson at ABSTRACT. "Examples of computer data felt to require access control include secure files, personalized e-mail accounts, specific user profiles, specific network profiles, and access to licensed programs. A secure file may be created by a user encrypting the file with a password. E-mail accounts obtain limited security by archiving data into personalized data structures or by password protecting e-mail access. Access to specific user profiles and network profiles are often controlled by operating system passwords. Many licensed programs require that only a specific quantity of users within a company be granted access and that additional users are not allowed access to these program. This regulation is generally accomplished by either assigning an access control code to each authorized user or the licensed program may regulate a hard quantity limitation on the total number of copies of the program that can be running from a server at any one time. By focusing on access control mechanisms surrounding the files, productivity and efficiency are reduced. These problems are enhanced if an individual user regularly switches work station locations to different access points within the company. Hence, a portable system which provides all file, user, network, or licensing authentication for a particular user would be useful for a corporation in managing its computer usage or license usages and would increase the efficiency and productivity of the user. Not to mention the added

'619 Patent – Claim 23	Thompson
	benefit of no longer needing to remember all the passwords used for each "secure" application." Thompson at 2:11-29. "A variety of access control systems and devices presently exist, however; these access control systems do not interface or coordinate with PDA devices. Specifically, a user attempting to gain access to various resources within a company is often required to carry an access card, an access key, or an I.D. access badge. The user may be required to know an access number, a PIN number, a combination, a password, or to provide a computer authorization number. In addition to these standard electronic and mechanical access control devices, some high security areas require an individual to provide specific biometric information such as fingerprint verification or a retinal scan. A system that provides all of the necessary access control information using a PDA device as a substitute for the aforementioned keys, cards, or passwords would considerably lessen the security delays and inefficiencies created by the multiple verification devices presently required to obtain site access authorization, not to mention the additional benefit of drastically reducing the extent and magnitude of security access devices necessary for any one individual to carry with them." Thompson at 2:30-3:8. "PDA device to selectively retrieve the information for service controllers or security outlets. The user may also enter the access control information directly to the PDA device through an interface device. The access control information includes access control codes used to enable the boot-up process for a connected digital device. These codes may also be used to authorize the transfer of funds in a commercial transaction. Access control codes can instruct the PDA device to produce the enabling or disabling signal for an electronic lock on items as diverse as a door and a secured computer file. Just as there are many different types of access control codes, there are multiple methods of delivering the codes to a service controller or security outlet. One method is through the I O cradle attached to the PDA device and the digital device. I/O cradles are usually attached to either the serial RS-232 port or the parallel port.

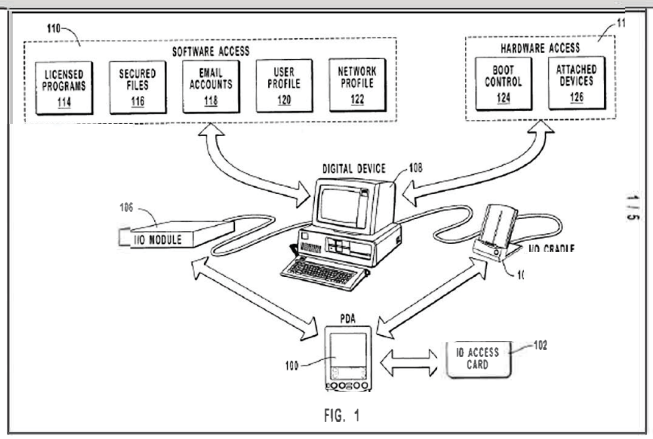
’619 Patent – Claim 23	Thompson
	Another interface method is between a PDA Infra-Red (IR) port and an I/O module attached to the digital device with a IR interface. A preferred embodiment of the present invention utilizes wireless transceiver, built into the PDA device to communicate with a receiver. Finally traditional interface parts, coils, or transmissions may be effectively used. These interfaces include RF, Wegand, magnetic, USB, or laser communication. A final potential embodiment includes integrating an IC chip into the digital device providing access control codes faster.” Thompson at 3:34-4:17. “In one embodiment, the system and method of the present invention provides all the file, user, network, or licensing authentication necessary for a particular user. Once the PDA device is plugged into an I/O cradle, all of the necessary password verification or authentication is supplied by the PDA device. A less memory intensive approach calls for the storage of a solitary password within the PDA access control database which downloads a user profile from a network location. Additional security checks could be implemented to verify that the PDA device holder is the actual user without negatively affecting the efficiency and productivity of the user because of the overall reduction in the number of access control codes. Another embodiment maintains communication between the PDA device and the digital device through an I/O module, such as a wireless transceiver or IR port. If a wireless transceiver is used, the PDA device can download information from the user's workstation at any time or from any location. The wireless PDA device embodiment could alert a user when someone is attempting unauthorized access to the user's computer. Another embodiment utilizes the PDA device to provide the access control codes for a user and then retrieves a customized user desktop setting for the user specified by the PDA device. This feature allows an individual user to attach to any computer within a company's network and obtain their customized desktop. This feature allows for incredible flexibility and versatility, not to mention the added benefit of no longer needing to remember all the passwords used for each "secure" application.” Thompson at 4:18-36.

'619 Patent – Claim 23	Thompson
	"Figure 1 provides an overview illustrating the use of a PDA device to control software and hardware access electronically connected to a digital device. A PDA 100 interfaces with an I.D. access card 102. The I.D. access card 102 may be in permanent, removable, or flexible communication with the PDA 100. A permanent connection is demonstrated by the addition of a chip which is installed within the PDA 100. The chip method has been established in other applications, but it has not been applied to PDA devices specifically in regards to access control or security features. If an IC chip is added to the PDA 100, the IC chip will have access to the PDA interfaces to the outside world through the PDA's processor. One embodiment would use the PDA's processor to read access numbers from the security chip and transmit the number to the device making the query. The querying device could then compare the transmitted number to its database to see if it was an acceptable number. Upon comparison of the devices the querying device could either accept or refuse access to its function e.g., building entry, computer access, transactional support, or purchasing. Removable communication generally involves attaching the I.D. access card 102 to an interface on the PDA 100 for a limited time period to either download access control database or to program an access control extension. Examples would include serial cables, PDA cradles, hard coded memory cards, PCMCIA cards, disks, Wegand devices, or other encoding equipment. Once the I.D. access card 102 contacts the PDA 100, it provides either secured data structures or an encrypted I.D. database that can be verified later by local controller access points. One embodiment uses the I.D. access card 102 by attaching the card or similar device to the PDA 100 through a clip-on method. Appropriate hardware and software could be added so that when a query was made on the interface to the outside world, the PDA's processor would read the number from the security card and transmit to the device making the query. The querying device could authorize the PDA request based on a successful comparison of the transmitted number to the querying device's database. Examples of some PDA access control requests include: building entry, computer access, car entry, purchasing transactions, goods, etc."

'619 Patent – Claim 23	Thompson
	Thompson at 7:6-19. "In addition to receiving information from an I.D. access card 102, the PDA interface devices can be used to facilitate communication between the PDA 100 and a digital device 108. Various PDA interface devices are employed to communicate with devices in the outside world including, but not limited to, the standard serial RS-232 port, a parallel port, an IR port, a PDA cradle connection, a RF bandwidth transceiver, Wegand device, magnetic coding or sensor, bar code reader, USB, wireless transceiver, and laser communication. Once an interface device is selected by the PDA 100, it can either interface with an I/O module 106 or with a PDA cradle 104. These interface input/output transceivers are in electronic communication with digital device 108. Once the digital device 108 has access to the PDA 100, it can verify whether access should be granted to a user for software access 110 or hardware access 112." Thompson at 8:7-17. "1. A method for authorizing access control to digital resources of a digital device using a person digital assistant (PDA), said method comprising of the steps of: initializing a database controlled by said PDA with access control codes; requesting access to said digital resources of said digital device; relaying said access control codes upon request to said digital device; selectively authorizing access by PDA to said digital resources based on said access control codes. 2. A method as recited in claim 1, where said digital resources include: licensed executable programs, secured data files, e-mail accounts, user profiles, network profiles, and attached peripheral devices. 3. A method as recited in claim 1, wherein said access control codes are automatically relayed between the digital device and the PDA when the PDA is electronically connected with at least one of a I/O cradle or an I/O module. 4. A method as recited in claim 3, wherein said I/O module comprises at least

'619 Patent – Claim 23	Thompson
	one of a serial port, a parallel port, an IR port, a PDA cradle connection interface, an RF transceiver, a Wegand interface, 2 magnetic sensor, a bar code render, a modem, a NIC, a USB, or 2 laser communication devices." Thompson at 15:1-20. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

'619 Patent – Claim 24	Thompson
[24] The device of claim 22, wherein the information including the service activation code is received by the device in an off-line communication.	Thompson discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22pre]-[22h], ***above***.

’619 Patent – Claim 24	Thompson
	 Thompson, Fig. 1. *See also*, Figs. 2-5. “An access control system combining PDA functionality with user authentication so that only the authorized user or users may obtain access control codes from a PDA device for an access control point. The access control point can be a computer terminal (108) , a computer file, a door, a checkstand, a visa authorization point, a gate, or other situation wherein high security is desirable. In a preferred embodiment, the access control system attaches to a computer (108) via a PDA cradle (104) and transmits access control codes that include a series of authentication codes or identification codes having encoded data stored within a PDA database. In another form of the invention, user authentication is obtained by comparing biometric data such as a fingerprint with digitally stored data of the authorized user. A decision to grant access affects the release, an electronic release or electronic strike, or electronic software hold. If desired, a write feature can be included into the system whereby each access control point accessed or attempted to be accessed

'619 Patent – Claim 24	Thompson
	by a PDA user will be recorded on the PDA to determine where access has been attempted. Additional records could be maintained along with the authentication I.D. including checking account information, credit card information, membership information, network information, user profile information (120), e-mail information (118), and personal information." Thompson at ABSTRACT. "Examples of computer data felt to require access control include secure files, personalized e-mail accounts, specific user profiles, specific network profiles, and access to licensed programs. A secure file may be created by a user encrypting the file with a password. E-mail accounts obtain limited security by archiving data into personalized data structures or by password protecting e-mail access. Access to specific user profiles and network profiles are often controlled by operating system passwords. Many licensed programs require that only a specific quantity of users within a company be granted access and that additional users are not allowed access to these program. This regulation is generally accomplished by either assigning an access control code to each authorized user or the licensed program may regulate a hard quantity limitation on the total number of copies of the program that can be running from a server at any one time. By focusing on access control mechanisms surrounding the files, productivity and efficiency are reduced. These problems are enhanced if an individual user regularly switches work station locations to different access points within the company. Hence, a portable system which provides all file, user, network, or licensing authentication for a particular user would be useful for a corporation in managing its computer usage or license usages and would increase the efficiency and productivity of the user. Not to mention the added benefit of no longer needing to remember all the passwords used for each "secure" application." Thompson at 2:11-29. "A variety of access control systems and devices presently exist, however; these access control systems do not interface or coordinate with PDA devices. Specifically, a user attempting to gain access to various resources within a

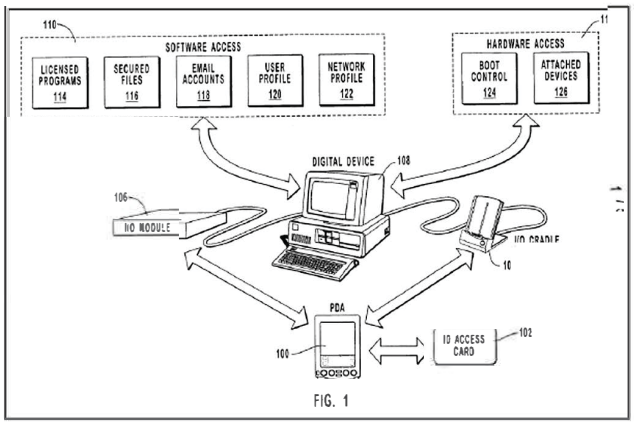
'619 Patent – Claim 24	Thompson
	company is often required to carry an access card, an access key, or an I.D. access badge. The user may be required to know an access number, a PIN number, a combination, a password, or to provide a computer authorization number. In addition to these standard electronic and mechanical access control devices, some high security areas require an individual to provide specific biometric information such as fingerprint verification or a retinal scan. A system that provides all of the necessary access control information using a PDA device as a substitute for the aforementioned keys, cards, or passwords would considerably lessen the security delays and inefficiencies created by the multiple verification devices presently required to obtain site access authorization, not to mention the additional benefit of drastically reducing the extent and magnitude of security access devices necessary for any one individual to carry with them." Thompson at 2:30-3:8. "PDA device to selectively retrieve the information for service controllers or security outlets. The user may also enter the access control information directly to the PDA device through an interface device. The access control information includes access control codes used to enable the boot-up process for a connected digital device. These codes may also be used to authorize the transfer of funds in a commercial transaction. Access control codes can instruct the PDA device to produce the enabling or disabling signal for an electronic lock on items as diverse as a door and a secured computer file. Just as there are many different types of access control codes, there are multiple methods of delivering the codes to a service controller or security outlet. One method is through the I O cradle attached to the PDA device and the digital device. I/O cradles are usually attached to either the serial RS-232 port or the parallel port. Another interface method is between a PDA Infra-Red (IR) port and an I/O module attached to the digital device with a IR interface. A preferred embodiment of the present invention utilizes wireless transceiver, built into the PDA device to communicate with a receiver. Finally traditional interface parts, coils, or transmissions may be effectively used. These interfaces include RF, Wegand, magnetic, USB, or laser communication. A final potential

'619 Patent – Claim 24	Thompson
	embodiment includes integrating an IC chip into the digital device providing access control codes faster." Thompson at 3:34-4:17. "In one embodiment, the system and method of the present invention provides all the file, user, network, or licensing authentication necessary for a particular user. Once the PDA device is plugged into an I/O cradle, all of the necessary password verification or authentication is supplied by the PDA device. A less memory intensive approach calls for the storage of a solitary password within the PDA access control database which downloads a user profile from a network location. Additional security checks could be implemented to verify that the PDA device holder is the actual user without negatively affecting the efficiency and productivity of the user because of the overall reduction in the number of access control codes. Another embodiment maintains communication between the PDA device and the digital device through an I/O module, such as a wireless transceiver or IR port. If a wireless transceiver is used, the PDA device can download information from the user's workstation at any time or from any location. The wireless PDA device embodiment could alert a user when someone is attempting unauthorized access to the user's computer. Another embodiment utilizes the PDA device to provide the access control codes for a user and then retrieves a customized user desktop setting for the user specified by the PDA device. This feature allows an individual user to attach to any computer within a company's network and obtain their customized desktop. This feature allows for incredible flexibility and versatility, not to mention the added benefit of no longer needing to remember all the passwords used for each "secure" application." Thompson at 4:18-36. "Figure 1 provides an overview illustrating the use of a PDA device to control software and hardware access electronically connected to a digital device. A PDA 100 interfaces with an I.D. access card 102. The I.D. access card 102 may be in permanent, removable, or flexible communication with the PDA 100. A permanent connection is demonstrated by the addition of a chip which is installed within the PDA 100. The chip method has been established in other

'619 Patent – Claim 24	Thompson
	applications, but it has not been applied to PDA devices specifically in regards to access control or security features. If an IC chip is added to the PDA 100, the IC chip will have access to the PDA interfaces to the outside world through the PDA's processor. One embodiment would use the PDA's processor to read access numbers from the security chip and transmit the number to the device making the query. The querying device could then compare the transmitted number to its database to see if it was an acceptable number. Upon comparison of the devices the querying device could either accept or refuse access to its function e.g., building entry, computer access, transactional support, or purchasing. Removable communication generally involves attaching the I.D. access card 102 to an interface on the PDA 100 for a limited time period to either download access control database or to program an access control extension. Examples would include serial cables, PDA cradles, hard coded memory cards, PCMCIA cards, disks, Wegand devices, or other encoding equipment. Once the I.D. access card 102 contacts the PDA 100, it provides either secured data structures or an encrypted I.D. database that can be verified later by local controller access points. One embodiment uses the I.D. access card 102 by attaching the card or similar device to the PDA 100 through a clip-on method. Appropriate hardware and software could be added so that when a query was made on the interface to the outside world, the PDA's processor would read the number from the security card and transmit to the device making the query. The querying device could authorize the PDA request based on a successful comparison of the transmitted number to the querying device's database. Examples of some PDA access control requests include: building entry, computer access, car entry, purchasing transactions, goods, etc." Thompson at 7:6-19. "In addition to receiving information from an I.D. access card 102, the PDA interface devices can be used to facilitate communication between the PDA 100 and a digital device 108. Various PDA interface devices are employed to communicate with devices in the outside world including, but not limited to, the standard serial RS-232 port, a parallel port, an IR port, a PDA cradle

'619 Patent – Claim 24	Thompson
	connection, a RF bandwidth transceiver, Wegand device, magnetic coding or sensor, bar code reader, USB, wireless transceiver, and laser communication. Once an interface device is selected by the PDA 100, it can either interface with an I/O module 106 or with a PDA cradle 104. These interface input/output transceivers are in electronic communication with digital device 108. Once the digital device 108 has access to the PDA 100, it can verify whether access should be granted to a user for software access 110 or hardware access 112." Thompson at 8:7-17. "1. A method for authorizing access control to digital resources of a digital device using a person digital assistant (PDA), said method comprising of the steps of: initializing a database controlled by said PDA with access control codes; requesting access to said digital resources of said digital device; relaying said access control codes upon request to said digital device; selectively authorizing access by PDA to said digital resources based on said access control codes. 2. A method as recited in claim 1, where said digital resources include: licensed executable programs, secured data files, e-mail accounts, user profiles, network profiles, and attached peripheral devices. 3. A method as recited in claim 1, wherein said access control codes are automatically relayed between the digital device and the PDA when the PDA is electronically connected with at least one of a I/O cradle or an I/O module. 4. A method as recited in claim 3, wherein said I/O module comprises at least one of a serial port, a parallel port, an IR port, a PDA cradle connection interface, an RF transceiver, a Wegand interface, 2 magnetic sensor, a bar code render, a modem, a NIC, a USB, or 2 laser communication devices." Thompson at 15:1-20. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in

’619 Patent – Claim 24	Thompson
	Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

’619 Patent – Claim 25	Thompson
[25] The device of claim 24, wherein the off-line communication involves a local connection.	Thompson discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22pre]-[22h] and [24], *above*.  FIG. 1 Thompson, Fig. 1. *See also*, Figs. 2-5.

'619 Patent – Claim 25	Thompson
	"An access control system combining PDA functionality with user authentication so that only the authorized user or users may obtain access control codes from a PDA device for an access control point. The access control point can be a computer terminal (108) , a computer file, a door, a checkstand, a visa authorization point, a gate, or other situation wherein high security is desirable. In a preferred embodiment, the access control system attaches to a computer (108) via a PDA cradle (104) and transmits access control codes that include a series of authentication codes or identification codes having encoded data stored within a PDA database. In another form of the invention, user authentication is obtained by comparing biometric data such as a fingerprint with digitally stored data of the authorized user. A decision to grant access affects the release, an electronic release or electronic strike, or electronic software hold. If desired, a write feature can be included into the system whereby each access control point accessed or attempted to be accessed by a PDA user will be recorded on the PDA to determine where access has been attempted. Additional records could be maintained along with the authentication I.D. including checking account information, credit card information, membership information, network information, user profile information (120), e-mail information (118), and personal information." Thompson at ABSTRACT. "Examples of computer data felt to require access control include secure files, personalized e-mail accounts, specific user profiles, specific network profiles, and access to licensed programs. A secure file may be created by a user encrypting the file with a password. E-mail accounts obtain limited security by archiving data into personalized data structures or by password protecting e-mail access. Access to specific user profiles and network profiles are often controlled by operating system passwords. Many licensed programs require that only a specific quantity of users within a company be granted access and that additional users are not allowed access to these program. This regulation is generally accomplished by either assigning an access control code to each authorized user or the licensed program may regulate a hard quantity limitation

'619 Patent – Claim 25	Thompson
	on the total number of copies of the program that can be running from a server at any one time. By focusing on access control mechanisms surrounding the files, productivity and efficiency are reduced. These problems are enhanced if an individual user regularly switches work station locations to different access points within the company. Hence, a portable system which provides all file, user, network, or licensing authentication for a particular user would be useful for a corporation in managing its computer usage or license usages and would increase the efficiency and productivity of the user. Not to mention the added benefit of no longer needing to remember all the passwords used for each "secure" application." Thompson at 2:11-29. "A variety of access control systems and devices presently exist, however; these access control systems do not interface or coordinate with PDA devices. Specifically, a user attempting to gain access to various resources within a company is often required to carry an access card, an access key, or an I.D. access badge. The user may be required to know an access number, a PIN number, a combination, a password, or to provide a computer authorization number. In addition to these standard electronic and mechanical access control devices, some high security areas require an individual to provide specific biometric information such as fingerprint verification or a retinal scan. A system that provides all of the necessary access control information using a PDA device as a substitute for the aforementioned keys, cards, or passwords would considerably lessen the security delays and inefficiencies created by the multiple verification devices presently required to obtain site access authorization, not to mention the additional benefit of drastically reducing the extent and magnitude of security access devices necessary for any one individual to carry with them." Thompson at 2:30-3:8. "PDA device to selectively retrieve the information for service controllers or security outlets. The user may also enter the access control information directly to the PDA device through an interface device. The access control information includes access control codes used to enable the boot-up process for a

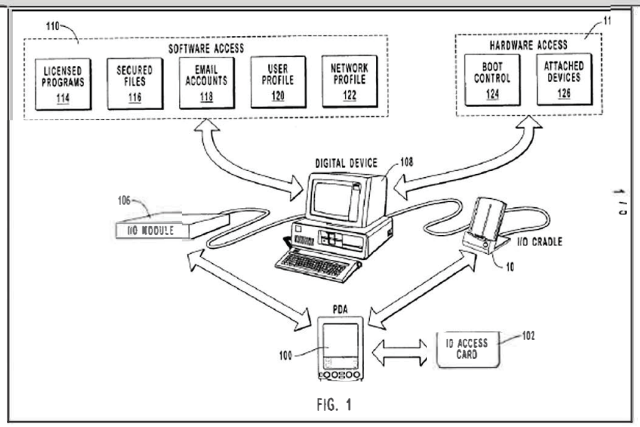
'619 Patent – Claim 25	Thompson
	connected digital device. These codes may also be used to authorize the transfer of funds in a commercial transaction. Access control codes can instruct the PDA device to produce the enabling or disabling signal for an electronic lock on items as diverse as a door and a secured computer file. Just as there are many different types of access control codes, there are multiple methods of delivering the codes to a service controller or security outlet. One method is through the I O cradle attached to the PDA device and the digital device. I/O cradles are usually attached to either the serial RS-232 port or the parallel port. Another interface method is between a PDA Infra-Red (IR) port and an I/O module attached to the digital device with a IR interface. A preferred embodiment of the present invention utilizes wireless transceiver, built into the PDA device to communicate with a receiver. Finally traditional interface parts, coils, or transmissions may be effectively used. These interfaces include RF, Wegand, magnetic, USB, or laser communication. A final potential embodiment includes integrating an IC chip into the digital device providing access control codes faster." Thompson at 3:34-4:17. "In one embodiment, the system and method of the present invention provides all the file, user, network, or licensing authentication necessary for a particular user. Once the PDA device is plugged into an I/O cradle, all of the necessary password verification or authentication is supplied by the PDA device. A less memory intensive approach calls for the storage of a solitary password within the PDA access control database which downloads a user profile from a network location. Additional security checks could be implemented to verify that the PDA device holder is the actual user without negatively affecting the efficiency and productivity of the user because of the overall reduction in the number of access control codes. Another embodiment maintains communication between the PDA device and the digital device through an I/O module, such as a wireless transceiver or IR port. If a wireless transceiver is used, the PDA device can download information from the user's workstation at any time or from any location. The wireless PDA device embodiment could alert a user when someone is attempting unauthorized access to the user's

'619 Patent – Claim 25	Thompson
	computer. Another embodiment utilizes the PDA device to provide the access control codes for a user and then retrieves a customized user desktop setting for the user specified by the PDA device. This feature allows an individual user to attach to any computer within a company's network and obtain their customized desktop. This feature allows for incredible flexibility and versatility, not to mention the added benefit of no longer needing to remember all the passwords used for each "secure" application." Thompson at 4:18-36. "Figure 1 provides an overview illustrating the use of a PDA device to control software and hardware access electronically connected to a digital device. A PDA 100 interfaces with an I.D. access card 102. The I.D. access card 102 may be in permanent, removable, or flexible communication with the PDA 100. A permanent connection is demonstrated by the addition of a chip which is installed within the PDA 100. The chip method has been established in other applications, but it has not been applied to PDA devices specifically in regards to access control or security features. If an IC chip is added to the PDA 100, the IC chip will have access to the PDA interfaces to the outside world through the PDA's processor. One embodiment would use the PDA's processor to read access numbers from the security chip and transmit the number to the device making the query. The querying device could then compare the transmitted number to its database to see if it was an acceptable number. Upon comparison of the devices the querying device could either accept or refuse access to its function e.g., building entry, computer access, transactional support, or purchasing. Removable communication generally involves attaching the I.D. access card 102 to an interface on the PDA 100 for a limited time period to either download access control database or to program an access control extension. Examples would include serial cables, PDA cradles, hard coded memory cards, PCMCIA cards, disks, Wegand devices, or other encoding equipment. Once the I.D. access card 102 contacts the PDA 100, it provides either secured data structures or an encrypted I.D. database that can be verified later by local controller access points. One embodiment uses the I.D. access card 102 by attaching the card or similar device to the PDA 100 through a clip-

'619 Patent – Claim 25	Thompson
	on method. Appropriate hardware and software could be added so that when a query was made on the interface to the outside world, the PDA's processor would read the number from the security card and transmit to the device making the query. The querying device could authorize the PDA request based on a successful comparison of the transmitted number to the querying device's database. Examples of some PDA access control requests include: building entry, computer access, car entry, purchasing transactions, goods, etc." Thompson at 7:6-19. "In addition to receiving information from an I.D. access card 102, the PDA interface devices can be used to facilitate communication between the PDA 100 and a digital device 108. Various PDA interface devices are employed to communicate with devices in the outside world including, but not limited to, the standard serial RS-232 port, a parallel port, an IR port, a PDA cradle connection, a RF bandwidth transceiver, Wegand device, magnetic coding or sensor, bar code reader, USB, wireless transceiver, and laser communication. Once an interface device is selected by the PDA 100, it can either interface with an I/O module 106 or with a PDA cradle 104. These interface input/output transceivers are in electronic communication with digital device 108. Once the digital device 108 has access to the PDA 100, it can verify whether access should be granted to a user for software access 110 or hardware access 112." Thompson at 8:7-17. "1. A method for authorizing access control to digital resources of a digital device using a person digital assistant (PDA), said method comprising of the steps of: initializing a database controlled by said PDA with access control codes; requesting access to said digital resources of said digital device; relaying said access control codes upon request to said digital device; selectively authorizing access by PDA to said digital resources based on said access control codes. 2. A method as recited in claim 1, where said digital resources include: licensed

'619 Patent – Claim 25	Thompson
	executable programs, secured data files, e-mail accounts, user profiles, network profiles, and attached peripheral devices. 3. A method as recited in claim 1, wherein said access control codes are automatically relayed between the digital device and the PDA when the PDA is electronically connected with at least one of a I/O cradle or an I/O module. 4. A method as recited in claim 3, wherein said I/O module comprises at least one of a serial port, a parallel port, an IR port, a PDA cradle connection interface, an RF transceiver, a Wegand interface, 2 magnetic sensor, a bar code render, a modem, a NIC, a USB, or 2 laser communication devices." Thompson at 15:1-20. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

'619 Patent – Claim 26	Thompson
[26] The device of claim 24, wherein the off-line communication prevents eavesdropping of the service activation code.	Thompson discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22pre]-[22h] and [24], ***above***.

’619 Patent – Claim 26	Thompson
	 FIG. 1 Thompson, Fig. 1. *See also*, Figs. 2-5. “An access control system combining PDA functionality with user authentication so that only the authorized user or users may obtain access control codes from a PDA device for an access control point. The access control point can be a computer terminal (108) , a computer file, a door, a checkstand, a visa authorization point, a gate, or other situation wherein high security is desirable. In a preferred embodiment, the access control system attaches to a computer (108) via a PDA cradle (104) and transmits access control codes that include a series of authentication codes or identification codes having encoded data stored within a PDA database. In another form of the invention, user authentication is obtained by comparing biometric data such as a fingerprint with digitally stored data of the authorized user. A decision to grant access affects the release, an electronic release or electronic strike, or electronic software hold. If desired, a write feature can be included into the system whereby each access control point accessed or attempted to be accessed

'619 Patent – Claim 26	Thompson
	by a PDA user will be recorded on the PDA to determine where access has been attempted. Additional records could be maintained along with the authentication I.D. including checking account information, credit card information, membership information, network information, user profile information (120), e-mail information (118), and personal information." Thompson at ABSTRACT. "Examples of computer data felt to require access control include secure files, personalized e-mail accounts, specific user profiles, specific network profiles, and access to licensed programs. A secure file may be created by a user encrypting the file with a password. E-mail accounts obtain limited security by archiving data into personalized data structures or by password protecting e-mail access. Access to specific user profiles and network profiles are often controlled by operating system passwords. Many licensed programs require that only a specific quantity of users within a company be granted access and that additional users are not allowed access to these program. This regulation is generally accomplished by either assigning an access control code to each authorized user or the licensed program may regulate a hard quantity limitation on the total number of copies of the program that can be running from a server at any one time. By focusing on access control mechanisms surrounding the files, productivity and efficiency are reduced. These problems are enhanced if an individual user regularly switches work station locations to different access points within the company. Hence, a portable system which provides all file, user, network, or licensing authentication for a particular user would be useful for a corporation in managing its computer usage or license usages and would increase the efficiency and productivity of the user. Not to mention the added benefit of no longer needing to remember all the passwords used for each "secure" application." Thompson at 2:11-29. "A variety of access control systems and devices presently exist, however; these access control systems do not interface or coordinate with PDA devices. Specifically, a user attempting to gain access to various resources within a

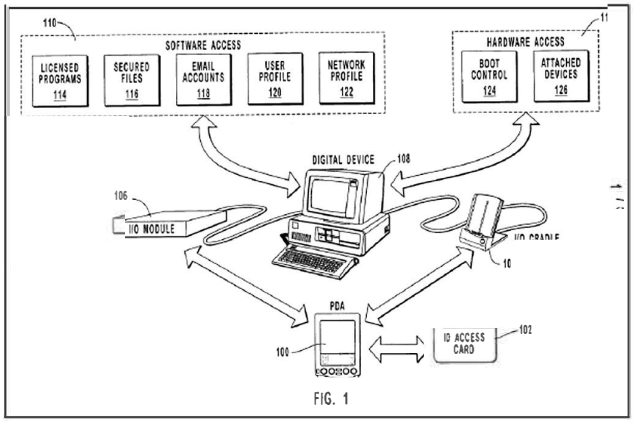
'619 Patent – Claim 26	Thompson
	company is often required to carry an access card, an access key, or an I.D. access badge. The user may be required to know an access number, a PIN number, a combination, a password, or to provide a computer authorization number. In addition to these standard electronic and mechanical access control devices, some high security areas require an individual to provide specific biometric information such as fingerprint verification or a retinal scan. A system that provides all of the necessary access control information using a PDA device as a substitute for the aforementioned keys, cards, or passwords would considerably lessen the security delays and inefficiencies created by the multiple verification devices presently required to obtain site access authorization, not to mention the additional benefit of drastically reducing the extent and magnitude of security access devices necessary for any one individual to carry with them." Thompson at 2:30-3:8. "PDA device to selectively retrieve the information for service controllers or security outlets. The user may also enter the access control information directly to the PDA device through an interface device. The access control information includes access control codes used to enable the boot-up process for a connected digital device. These codes may also be used to authorize the transfer of funds in a commercial transaction. Access control codes can instruct the PDA device to produce the enabling or disabling signal for an electronic lock on items as diverse as a door and a secured computer file. Just as there are many different types of access control codes, there are multiple methods of delivering the codes to a service controller or security outlet. One method is through the I O cradle attached to the PDA device and the digital device. I/O cradles are usually attached to either the serial RS-232 port or the parallel port. Another interface method is between a PDA Infra-Red (IR) port and an I/O module attached to the digital device with a IR interface. A preferred embodiment of the present invention utilizes wireless transceiver, built into the PDA device to communicate with a receiver. Finally traditional interface parts, coils, or transmissions may be effectively used. These interfaces include RF, Wegand, magnetic, USB, or laser communication. A final potential

'619 Patent – Claim 26	Thompson
	embodiment includes integrating an IC chip into the digital device providing access control codes faster." Thompson at 3:34-4:17. "In one embodiment, the system and method of the present invention provides all the file, user, network, or licensing authentication necessary for a particular user. Once the PDA device is plugged into an I/O cradle, all of the necessary password verification or authentication is supplied by the PDA device. A less memory intensive approach calls for the storage of a solitary password within the PDA access control database which downloads a user profile from a network location. Additional security checks could be implemented to verify that the PDA device holder is the actual user without negatively affecting the efficiency and productivity of the user because of the overall reduction in the number of access control codes. Another embodiment maintains communication between the PDA device and the digital device through an I/O module, such as a wireless transceiver or IR port. If a wireless transceiver is used, the PDA device can download information from the user's workstation at any time or from any location. The wireless PDA device embodiment could alert a user when someone is attempting unauthorized access to the user's computer. Another embodiment utilizes the PDA device to provide the access control codes for a user and then retrieves a customized user desktop setting for the user specified by the PDA device. This feature allows an individual user to attach to any computer within a company's network and obtain their customized desktop. This feature allows for incredible flexibility and versatility, not to mention the added benefit of no longer needing to remember all the passwords used for each "secure" application." Thompson at 4:18-36. "Figure 1 provides an overview illustrating the use of a PDA device to control software and hardware access electronically connected to a digital device. A PDA 100 interfaces with an I.D. access card 102. The I.D. access card 102 may be in permanent, removable, or flexible communication with the PDA 100. A permanent connection is demonstrated by the addition of a chip which is installed within the PDA 100. The chip method has been established in other

'619 Patent – Claim 26	Thompson
	applications, but it has not been applied to PDA devices specifically in regards to access control or security features. If an IC chip is added to the PDA 100, the IC chip will have access to the PDA interfaces to the outside world through the PDA's processor. One embodiment would use the PDA's processor to read access numbers from the security chip and transmit the number to the device making the query. The querying device could then compare the transmitted number to its database to see if it was an acceptable number. Upon comparison of the devices the querying device could either accept or refuse access to its function e.g., building entry, computer access, transactional support, or purchasing. Removable communication generally involves attaching the I.D. access card 102 to an interface on the PDA 100 for a limited time period to either download access control database or to program an access control extension. Examples would include serial cables, PDA cradles, hard coded memory cards, PCMCIA cards, disks, Wegand devices, or other encoding equipment. Once the I.D. access card 102 contacts the PDA 100, it provides either secured data structures or an encrypted I.D. database that can be verified later by local controller access points. One embodiment uses the I.D. access card 102 by attaching the card or similar device to the PDA 100 through a clip-on method. Appropriate hardware and software could be added so that when a query was made on the interface to the outside world, the PDA's processor would read the number from the security card and transmit to the device making the query. The querying device could authorize the PDA request based on a successful comparison of the transmitted number to the querying device's database. Examples of some PDA access control requests include: building entry, computer access, car entry, purchasing transactions, goods, etc." Thompson at 7:6-19. "In addition to receiving information from an I.D. access card 102, the PDA interface devices can be used to facilitate communication between the PDA 100 and a digital device 108. Various PDA interface devices are employed to communicate with devices in the outside world including, but not limited to, the standard serial RS-232 port, a parallel port, an IR port, a PDA cradle

'619 Patent – Claim 26	Thompson
	connection, a RF bandwidth transceiver, Wegand device, magnetic coding or sensor, bar code reader, USB, wireless transceiver, and laser communication. Once an interface device is selected by the PDA 100, it can either interface with an I/O module 106 or with a PDA cradle 104. These interface input/output transceivers are in electronic communication with digital device 108. Once the digital device 108 has access to the PDA 100, it can verify whether access should be granted to a user for software access 110 or hardware access 112." Thompson at 8:7-17. "1. A method for authorizing access control to digital resources of a digital device using a person digital assistant (PDA), said method comprising of the steps of: initializing a database controlled by said PDA with access control codes; requesting access to said digital resources of said digital device; relaying said access control codes upon request to said digital device; selectively authorizing access by PDA to said digital resources based on said access control codes. 2. A method as recited in claim 1, where said digital resources include: licensed executable programs, secured data files, e-mail accounts, user profiles, network profiles, and attached peripheral devices. 3. A method as recited in claim 1, wherein said access control codes are automatically relayed between the digital device and the PDA when the PDA is electronically connected with at least one of a I/O cradle or an I/O module. 4. A method as recited in claim 3, wherein said I/O module comprises at least one of a serial port, a parallel port, an IR port, a PDA cradle connection interface, an RF transceiver, a Wegand interface, 2 magnetic sensor, a bar code render, a modem, a NIC, a USB, or 2 laser communication devices." Thompson at 15:1-20. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in

’619 Patent – Claim 26	Thompson
	Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

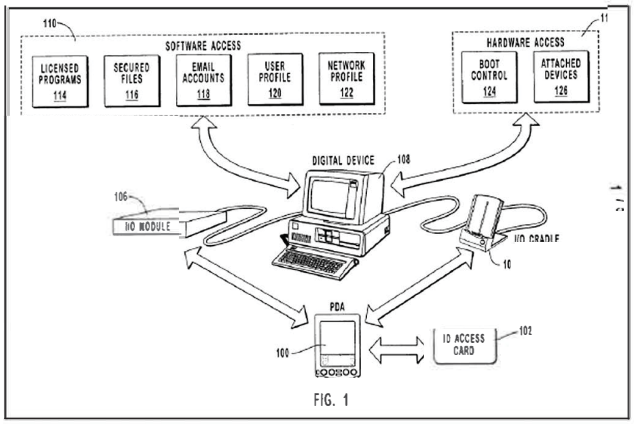
’619 Patent – Claim 27	Thompson
[27] The device of claim 22, wherein the authentication of the device relies on the authentication of the messaging account.	Thompson discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22pre]-[22h], ***above***.  FIG. 1

'619 Patent – Claim 27	Thompson
	Thompson, Fig. 1. *See also*, Figs. 2-5. "An access control system combining PDA functionality with user authentication so that only the authorized user or users may obtain access control codes from a PDA device for an access control point. The access control point can be a computer terminal (108) , a computer file, a door, a checkstand, a visa authorization point, a gate, or other situation wherein high security is desirable. In a preferred embodiment, the access control system attaches to a computer (108) via a PDA cradle (104) and transmits access control codes that include a series of authentication codes or identification codes having encoded data stored within a PDA database. In another form of the invention, user authentication is obtained by comparing biometric data such as a fingerprint with digitally stored data of the authorized user. A decision to grant access affects the release, an electronic release or electronic strike, or electronic software hold. If desired, a write feature can be included into the system whereby each access control point accessed or attempted to be accessed by a PDA user will be recorded on the PDA to determine where access has been attempted. Additional records could be maintained along with the authentication I.D. including checking account information, credit card information, membership information, network information, user profile information (120), e-mail information (118), and personal information." Thompson at ABSTRACT. "In one embodiment, special booting software is installed on a computer so that if the PDA device is not in the cradle, the computer can not be accessed. An access card code interface could also be used for protecting e-mail and communications between computers by requiring the PDA device to be in its cradle or near its receptor before access control would be allowed. This system would add security by controlling access to all things controlled or accessed by the PDA device, without requiring unnecessary security to impede the process. Various software access 110 features include inquiring whether the individual has approval to use licensed programs 114, whether approval exists to secured

'619 Patent – Claim 27	Thompson
	files 116, whether access should be granted to personal e-mail accounts 118, whether a specific user profile 120 should replace the standard desktop profile, and if a network profile 122 exists for a particular user. The network profile 122 could be stored on a central computer and, upon verification of a PDA 100 within an I/O cradle 108 at a particular digital device 108 access and rights and privileges to network, drives, data, and resources could be granted to the individual user, thereby allowing him to use local printers, fax machines, and other local facilities but also providing him with access to printers at his home location. In essence, the user would only need to plug his PDA 100 into I/O cradle 104 or interface with I/O module 106 to obtain personalized access throughout a company's LAN or WAN network." Thompson at 8:18-35. "Figure 3 is a block diagram of an access control protocol that can be applied to software or hardware access. The access control protocol is initiated in execution block 300 whenever there is a request to access of an access control protocol that can be applied to software or hardware access. A protected software or hardware resource, such as e- mail or a protected file. At this point, a subprotocol initiates the security confirmation protocol which prevents the program from providing access or from loading further until the PDA has been verified. In decision block 302, the protocol discovers whether the PDA is connected. If the authorized PDA is not connected, execution block 304 prompts the user to connected the appropriate PDA to the computer. Once the PDA is connected, execution block 306 exchanges of identification information. Decision block 308 determines whether the exchanged identification information is valid. If the information is valid, then execution block 310 allows access to the file, e-mail, or other computer software or hardware resource. If it is not valid, then the access control protocol ends without giving access to the file. This access control protocol allows users to access their files on a common computer shared with multiple users. E-mail files are optionally loaded directly down to the PDA once the identification authorization has been made. Additionally, a user could use a traveling work station in which he was only required to carry his PDA containing the

'619 Patent – Claim 27	Thompson
	appropriate identification information to request from the network server the user's standard desktop and access to the user's e-mail files. As a result, a traveler could go to a foreign office or another work site location, plug his PDA into the control port and be granted access to the computer with the same restrictions and limitations that he may have had at his workstation at home." Thompson at 9:30-10:15. "1. A method for authorizing access control to digital resources of a digital device using a person digital assistant (PDA), said method comprising of the steps of: initializing a database controlled by said PDA with access control codes; requesting access to said digital resources of said digital device; relaying said access control codes upon request to said digital device; selectively authorizing access by PDA to said digital resources based on said access control codes. 2. A method as recited in claim 1, where said digital resources include: licensed executable programs, secured data files, e-mail accounts, user profiles, network profiles, and attached peripheral devices. 3. A method as recited in claim 1, wherein said access control codes are automatically relayed between the digital device and the PDA when the PDA is electronically connected with at least one of a I/O cradle or an I/O module. 4. A method as recited in claim 3, wherein said I/O module comprises at least one of a serial port, a parallel port, an IR port, a PDA cradle connection interface, an RF transceiver, a Wegand interface, 2 magnetic sensor, a bar code render, a modem, a NIC, a USB, or 2 laser communication devices." Thompson at 15:1-20. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person

'619 Patent – Claim 27	Thompson
	of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

'619 Patent – Claim 28	Thompson
[28] The device of claim 27, wherein the authentication of the messaging account includes a username and password.	Thompson discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22pre]-[22h] and [27], ***above***.  FIG. 1 Thompson, Fig. 1. *See also*, Figs. 2-5. "An access control system combining PDA functionality with user

'619 Patent – Claim 28	Thompson
	authentication so that only the authorized user or users may obtain access control codes from a PDA device for an access control point. The access control point can be a computer terminal (108) , a computer file, a door, a checkstand, a visa authorization point, a gate, or other situation wherein high security is desirable. In a preferred embodiment, the access control system attaches to a computer (108) via a PDA cradle (104) and transmits access control codes that include a series of authentication codes or identification codes having encoded data stored within a PDA database. In another form of the invention, user authentication is obtained by comparing biometric data such as a fingerprint with digitally stored data of the authorized user. A decision to grant access affects the release, an electronic release or electronic strike, or electronic software hold. If desired, a write feature can be included into the system whereby each access control point accessed or attempted to be accessed by a PDA user will be recorded on the PDA to determine where access has been attempted. Additional records could be maintained along with the authentication I.D. including checking account information, credit card information, membership information, network information, user profile information (120), e-mail information (118), and personal information." Thompson at ABSTRACT. "Examples of computer data felt to require access control include secure files, personalized e-mail accounts, specific user profiles, specific network profiles, and access to licensed programs. A secure file may be created by a user encrypting the file with a password. E-mail accounts obtain limited security by archiving data into personalized data structures or by password protecting e-mail access. Access to specific user profiles and network profiles are often controlled by operating system passwords. Many licensed programs require that only a specific quantity of users within a company be granted access and that additional users are not allowed access to these program. This regulation is generally accomplished by either assigning an access control code to each authorized user or the licensed program may regulate a hard quantity limitation on the total number of copies of the program that can be running from a server

'619 Patent – Claim 28	Thompson
	at any one time. By focusing on access control mechanisms surrounding the files, productivity and efficiency are reduced. These problems are enhanced if an individual user regularly switches work station locations to different access points within the company. Hence, a portable system which provides all file, user, network, or licensing authentication for a particular user would be useful for a corporation in managing its computer usage or license usages and would increase the efficiency and productivity of the user. Not to mention the added benefit of no longer needing to remember all the passwords used for each "secure" application." Thompson at 2:11-29. "A variety of access control systems and devices presently exist, however; these access control systems do not interface or coordinate with PDA devices. Specifically, a user attempting to gain access to various resources within a company is often required to carry an access card, an access key, or an I.D. access badge. The user may be required to know an access number, a PIN number, a combination, a password, or to provide a computer authorization number. In addition to these standard electronic and mechanical access control devices, some high security areas require an individual to provide specific biometric information such as fingerprint verification or a retinal scan. A system that provides all of the necessary access control information using a PDA device as a substitute for the aforementioned keys, cards, or passwords would considerably lessen the security delays and inefficiencies created by the multiple verification devices presently required to obtain site access authorization, not to mention the additional benefit of drastically reducing the extent and magnitude of security access devices necessary for any one individual to carry with them." Thompson at 2:30-3:7. "In one embodiment, the system and method of the present invention provides all the file, user, network, or licensing authentication necessary for a particular user. Once the PDA device is plugged into an I/O cradle, all of the necessary password verification or authentication is supplied by the PDA device. A less memory intensive approach calls for the storage of a solitary password within

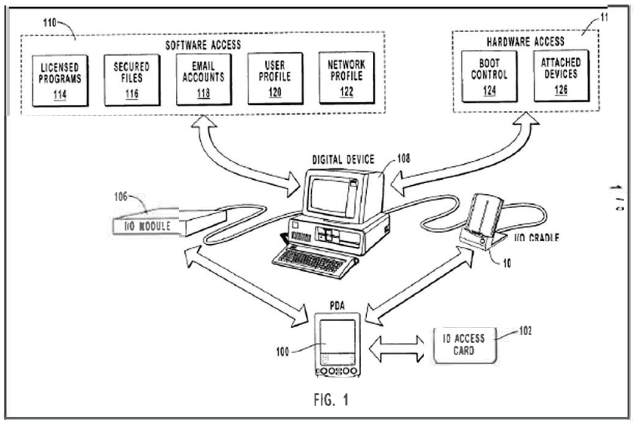
'619 Patent – Claim 28	Thompson
	the PDA access control database which downloads a user profile from a network location. Additional security checks could be implemented to verify that the PDA device holder is the actual user without negatively affecting the efficiency and productivity of the user because of the overall reduction in the number of access control codes. Another embodiment maintains communication between the PDA device and the digital device through an I/O module, such as a wireless transceiver or IR port. If a wireless transceiver is used, the PDA device can download information from the user's workstation at any time or from any location. The wireless PDA device embodiment could alert a user when someone is attempting unauthorized access to the user's computer. Another embodiment utilizes the PDA device to provide the access control codes for a user and then retrieves a customized user desktop setting for the user specified by the PDA device. This feature allows an individual user to attach to any computer within a company's network and obtain their customized desktop. This feature allows for incredible flexibility and versatility, not to mention the added benefit of no longer needing to remember all the passwords used for each "secure" application." Thompson at 4:18-37. "In one embodiment, special booting software is installed on a computer so that if the PDA device is not in the cradle, the computer can not be accessed. An access card code interface could also be used for protecting e-mail and communications between computers by requiring the PDA device to be in its cradle or near its receptor before access control would be allowed. This system would add security by controlling access to all things controlled or accessed by the PDA device, without requiring unnecessary security to impede the process. Various software access 110 features include inquiring whether the individual has approval to use licensed programs 114, whether approval exists to secured files 116, whether access should be granted to personal e-mail accounts 118, whether a specific user profile 120 should replace the standard desktop profile, and if a network profile 122 exists for a particular user. The network profile 122 could be stored on a central computer and, upon verification of a PDA 100 within an I/O cradle 108 at a particular digital device 108 access and rights and

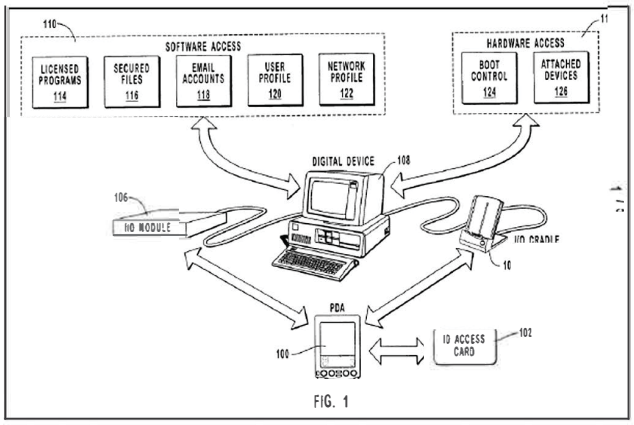
'619 Patent – Claim 28	Thompson
	privileges to network, drives, data, and resources could be granted to the individual user, thereby allowing him to use local printers, fax machines, and other local facilities but also providing him with access to printers at his home location. In essence, the user would only need to plug his PDA 100 into I/O cradle 104 or interface with I/O module 106 to obtain personalized access throughout a company's LAN or WAN network." Thompson at 8:18-35. "Figure 3 is a block diagram of an access control protocol that can be applied to software or hardware access. The access control protocol is initiated in execution block 300 whenever there is a request to access of an access control protocol that can be applied to software or hardware access. A protected software or hardware resource, such as e- mail or a protected file. At this point, a subprotocol initiates the security confirmation protocol which prevents the program from providing access or from loading further until the PDA has been verified. In decision block 302, the protocol discovers whether the PDA is connected. If the authorized PDA is not connected, execution block 304 prompts the user to connected the appropriate PDA to the computer. Once the PDA is connected, execution block 306 exchanges of identification information. Decision block 308 determines whether the exchanged identification information is valid. If the information is valid, then execution block 310 allows access to the file, e-mail, or other computer software or hardware resource. If it is not valid, then the access control protocol ends without giving access to the file. This access control protocol allows users to access their files on a common computer shared with multiple users. E-mail files are optionally loaded directly down to the PDA once the identification authorization has been made. Additionally, a user could use a traveling work station in which he was only required to carry his PDA containing the appropriate identification information to request from the network server the user's standard desktop and access to the user's e-mail files. As a result, a traveler could go to a foreign office or another work site location, plug his PDA into the control port and be granted access to the computer with the same restrictions and limitations that he may have had at his workstation at home."

'619 Patent – Claim 28	Thompson
	Thompson at 9:30-10:15. "1. A method for authorizing access control to digital resources of a digital device using a person digital assistant (PDA), said method comprising of the steps of: initializing a database controlled by said PDA with access control codes; requesting access to said digital resources of said digital device; relaying said access control codes upon request to said digital device; selectively authorizing access by PDA to said digital resources based on said access control codes. 2. A method as recited in claim 1, where said digital resources include: licensed executable programs, secured data files, e-mail accounts, user profiles, network profiles, and attached peripheral devices. 3. A method as recited in claim 1, wherein said access control codes are automatically relayed between the digital device and the PDA when the PDA is electronically connected with at least one of a I/O cradle or an I/O module. 4. A method as recited in claim 3, wherein said I/O module comprises at least one of a serial port, a parallel port, an IR port, a PDA cradle connection interface, an RF transceiver, a Wegand interface, 2 magnetic sensor, a bar code render, a modem, a NIC, a USB, or 2 laser communication devices." Thompson at 15:1-20. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

'619 Patent – Claim 32	Thompson
[32] The device of claim 22, wherein the encryption key is closely related to the service activation code.	Thompson discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22pre]-[22h], *above*. Thompson, Fig. 1. See also, Figs. 2-5. "Examples of computer data felt to require access control include secure files, personalized e-mail accounts, specific user profiles, specific network profiles, and access to licensed programs. A secure file may be created by a user encrypting the file with a password. E-mail accounts obtain limited security by archiving data into personalized data structures or by password protecting e-mail access." Thompson at 2:11-29. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

'619 Patent – Claim 33	Thompson
[33a] The device of claim 22, wherein the device is further operable to:	Thompson discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22pre]-[22h], *above*.

'619 Patent – Claim 33	Thompson
[33b] store an association between at least two of the encryption key, the messaging account, an identifier of the remote device, and the service activation code.	Thompson discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22pre]-[22h], *above*.  FIG. 1 Thompson, Fig. 1. *See also*, Figs. 2-5. "An access control system combining PDA functionality with user authentication so that only the authorized user or users may obtain access control codes from a PDA device for an access control point. The access control point can be a computer terminal (108), a computer file, a door, a checkstand, a visa authorization point, a gate, or other situation wherein high security is desirable. In a preferred embodiment, the access control system attaches to a computer (108) via a PDA cradle (104) and transmits access control codes that include a series of authentication codes or identification codes having encoded data stored within a PDA database. In another form of the invention, user authentication is obtained by comparing biometric data such

'619 Patent – Claim 33	Thompson
	as a fingerprint with digitally stored data of the authorized user. A decision to grant access affects the release, an electronic release or electronic strike, or electronic software hold. If desired, a write feature can be included into the system whereby each access control point accessed or attempted to be accessed by a PDA user will be recorded on the PDA to determine where access has been attempted. Additional records could be maintained along with the authentication I.D. including checking account information, credit card information, membership information, network information, user profile information (120), e-mail information (118), and personal information." Thompson at ABSTRACT.  FIG. 1 Thompson, Fig. 1. *See also*, Figs. 2-5. "An access control system combining PDA functionality with user authentication so that only the authorized user or users may obtain access control codes from a PDA device for an access control point. The access control point can be a computer terminal (108) , a computer file, a door, a

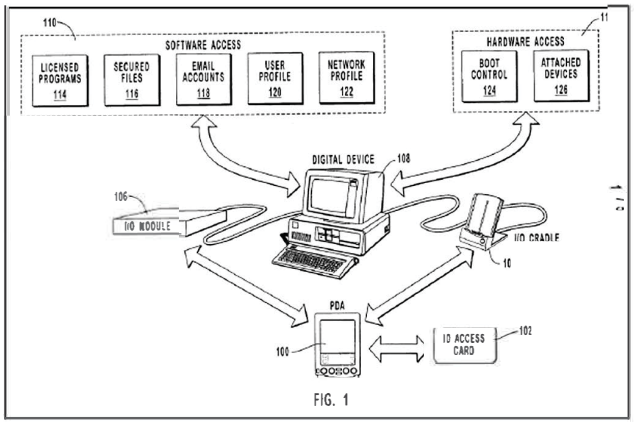
'619 Patent – Claim 33	Thompson
	checkstand, a visa authorization point, a gate, or other situation wherein high security is desirable. In a preferred embodiment, the access control system attaches to a computer (108) via a PDA cradle (104) and transmits access control codes that include a series of authentication codes or identification codes having encoded data stored within a PDA database. In another form of the invention, user authentication is obtained by comparing biometric data such as a fingerprint with digitally stored data of the authorized user. A decision to grant access affects the release, an electronic release or electronic strike, or electronic software hold. If desired, a write feature can be included into the system whereby each access control point accessed or attempted to be accessed by a PDA user will be recorded on the PDA to determine where access has been attempted. Additional records could be maintained along with the authentication I.D. including checking account information, credit card information, membership information, network information, user profile information (120), e-mail information (118), and personal information." Thompson at ABSTRACT. "Examples of computer data felt to require access control include secure files, personalized e-mail accounts, specific user profiles, specific network profiles, and access to licensed programs. A secure file may be created by a user encrypting the file with a password. E-mail accounts obtain limited security by archiving data into personalized data structures or by password protecting e-mail access. Access to specific user profiles and network profiles are often controlled by operating system passwords. Many licensed programs require that only a specific quantity of users within a company be granted access and that additional users are not allowed access to these program. This regulation is generally accomplished by either assigning an access control code to each authorized user or the licensed program may regulate a hard quantity limitation on the total number of copies of the program that can be running from a server at any one time. By focusing on access control mechanisms surrounding the files, productivity and efficiency are reduced. These problems are enhanced if an individual user regularly switches work station locations to different access

'619 Patent – Claim 33	Thompson
	points within the company. Hence, a portable system which provides all file, user, network, or licensing authentication for a particular user would be useful for a corporation in managing its computer usage or license usages and would increase the efficiency and productivity of the user. Not to mention the added benefit of no longer needing to remember all the passwords used for each "secure" application." Thompson at 2:11-29. "A variety of access control systems and devices presently exist, however; these access control systems do not interface or coordinate with PDA devices. Specifically, a user attempting to gain access to various resources within a company is often required to carry an access card, an access key, or an I.D. access badge. The user may be required to know an access number, a PIN number, a combination, a password, or to provide a computer authorization number. In addition to these standard electronic and mechanical access control devices, some high security areas require an individual to provide specific biometric information such as fingerprint verification or a retinal scan. A system that provides all of the necessary access control information using a PDA device as a substitute for the aforementioned keys, cards, or passwords would considerably lessen the security delays and inefficiencies created by the multiple verification devices presently required to obtain site access authorization, not to mention the additional benefit of drastically reducing the extent and magnitude of security access devices necessary for any one individual to carry with them." Thompson at 2:30-3:7. "In one embodiment, the system and method of the present invention provides all the file, user, network, or licensing authentication necessary for a particular user. Once the PDA device is plugged into an I/O cradle, all of the necessary password verification or authentication is supplied by the PDA device. A less memory intensive approach calls for the storage of a solitary password within the PDA access control database which downloads a user profile from a network location. Additional security checks could be implemented to verify that the PDA device holder is the actual user without negatively affecting the

'619 Patent – Claim 33	Thompson
	efficiency and productivity of the user because of the overall reduction in the number of access control codes. Another embodiment maintains communication between the PDA device and the digital device through an I/O module, such as a wireless transceiver or IR port. If a wireless transceiver is used, the PDA device can download information from the user's workstation at any time or from any location. The wireless PDA device embodiment could alert a user when someone is attempting unauthorized access to the user's computer. Another embodiment utilizes the PDA device to provide the access control codes for a user and then retrieves a customized user desktop setting for the user specified by the PDA device. This feature allows an individual user to attach to any computer within a company's network and obtain their customized desktop. This feature allows for incredible flexibility and versatility, not to mention the added benefit of no longer needing to remember all the passwords used for each "secure" application." Thompson at 4:18-37. "In one embodiment, special booting software is installed on a computer so that if the PDA device is not in the cradle, the computer can not be accessed. An access card code interface could also be used for protecting e-mail and communications between computers by requiring the PDA device to be in its cradle or near its receptor before access control would be allowed. This system would add security by controlling access to all things controlled or accessed by the PDA device, without requiring unnecessary security to impede the process. Various software access 110 features include inquiring whether the individual has approval to use licensed programs 114, whether approval exists to secured files 116, whether access should be granted to personal e-mail accounts 118, whether a specific user profile 120 should replace the standard desktop profile, and if a network profile 122 exists for a particular user. The network profile 122 could be stored on a central computer and, upon verification of a PDA 100 within an I/O cradle 108 at a particular digital device 108 access and rights and privileges to network, drives, data, and resources could be granted to the individual user, thereby allowing him to use local printers, fax machines, and other local facilities but also providing him with access to printers at his home

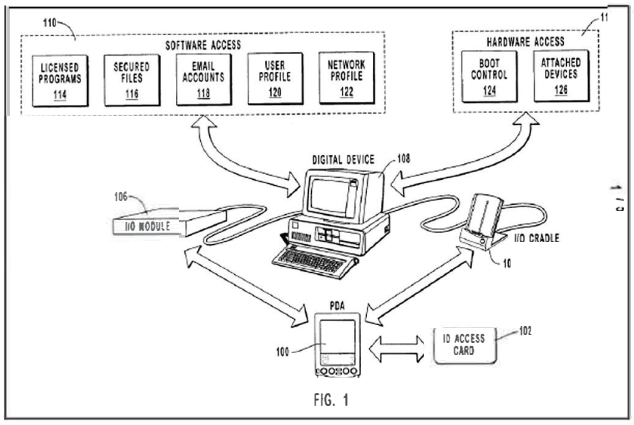
'619 Patent – Claim 33	Thompson
	location. In essence, the user would only need to plug his PDA 100 into I/O cradle 104 or interface with I/O module 106 to obtain personalized access throughout a company's LAN or WAN network." Thompson at 8:18-35. "Figure 3 is a block diagram of an access control protocol that can be applied to software or hardware access. The access control protocol is initiated in execution block 300 whenever there is a request to access of an access control protocol that can be applied to software or hardware access. A protected software or hardware resource, such as e- mail or a protected file. At this point, a subprotocol initiates the security confirmation protocol which prevents the program from providing access or from loading further until the PDA has been verified. In decision block 302, the protocol discovers whether the PDA is connected. If the authorized PDA is not connected, execution block 304 prompts the user to connected the appropriate PDA to the computer. Once the PDA is connected, execution block 306 exchanges of identification information. Decision block 308 determines whether the exchanged identification information is valid. If the information is valid, then execution block 310 allows access to the file, e-mail, or other computer software or hardware resource. If it is not valid, then the access control protocol ends without giving access to the file. This access control protocol allows users to access their files on a common computer shared with multiple users. E-mail files are optionally loaded directly down to the PDA once the identification authorization has been made. Additionally, a user could use a traveling work station in which he was only required to carry his PDA containing the appropriate identification information to request from the network server the user's standard desktop and access to the user's e-mail files. As a result, a traveler could go to a foreign office or another work site location, plug his PDA into the control port and be granted access to the computer with the same restrictions and limitations that he may have had at his workstation at home." Thompson at 9:30-10:15. "1. A method for authorizing access control to digital resources of a digital

'619 Patent – Claim 33	Thompson
	device using a person digital assistant (PDA), said method comprising of the steps of: initializing a database controlled by said PDA with access control codes; requesting access to said digital resources of said digital device; relaying said access control codes upon request to said digital device; selectively authorizing access by PDA to said digital resources based on said access control codes. 2. A method as recited in claim 1, where said digital resources include: licensed executable programs, secured data files, e-mail accounts, user profiles, network profiles, and attached peripheral devices. 3. A method as recited in claim 1, wherein said access control codes are automatically relayed between the digital device and the PDA when the PDA is electronically connected with at least one of a I/O cradle or an I/O module. 4. A method as recited in claim 3, wherein said I/O module comprises at least one of a serial port, a parallel port, an IR port, a PDA cradle connection interface, an RF transceiver, a Wegand interface, 2 magnetic sensor, a bar code render, a modem, a NIC, a USB, or 2 laser communication devices." Thompson at 15:1-20. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

’619 Patent – Claim 36	Thompson
[36] The device of claim 22, wherein a control message is received from the remote device upon user interaction with the message.	Thompson discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22pre]-[22h], *above*.  FIG. 1 Thompson, Fig. 1. *See also*, Figs. 2-5. “An access control system combining PDA functionality with user authentication so that only the authorized user or users may obtain access control codes from a PDA device for an access control point. The access control point can be a computer terminal (108), a computer file, a door, a checkstand, a visa authorization point, a gate, or other situation wherein high security is desirable. In a preferred embodiment, the access control system attaches to a computer (108) via a PDA cradle (104) and transmits access control codes that include a series of authentication codes or identification codes having encoded data stored within a PDA database. In another form of the invention, user authentication is obtained by comparing biometric data such

'619 Patent – Claim 36	Thompson
	as a fingerprint with digitally stored data of the authorized user. A decision to grant access affects the release, an electronic release or electronic strike, or electronic software hold. If desired, a write feature can be included into the system whereby each access control point accessed or attempted to be accessed by a PDA user will be recorded on the PDA to determine where access has been attempted. Additional records could be maintained along with the authentication I.D. including checking account information, credit card information, membership information, network information, user profile information (120), e-mail information (118), and personal information." Thompson at ABSTRACT. "In addition to receiving information from an I.D. access card 102, the PDA interface devices can be used to facilitate communication between the PDA 100 and a digital device 108. Various PDA interface devices are employed to communicate with devices in the outside world including, but not limited to, the standard serial RS-232 port, a parallel port, an IR port, a PDA cradle connection, a RF bandwidth transceiver, Wegand device, magnetic coding or sensor, bar code reader, USB, wireless transceiver, and laser communication. Once an interface device is selected by the PDA 100, it can either interface with an I/O module 106 or with a PDA cradle 104. These interface input/output transceivers are in electronic communication with digital device 108. Once the digital device 108 has access to the PDA 100, it can verify whether access should be granted to a user for software access 110 or hardware access 112." Thompson at 8:7-17. "1. A method for authorizing access control to digital resources of a digital device using a person digital assistant (PDA), said method comprising of the steps of: initializing a database controlled by said PDA with access control codes; requesting access to said digital resources of said digital device; relaying said access control codes upon request to said digital device; selectively authorizing access by PDA to said digital resources based on said access

'619 Patent – Claim 36	Thompson
	control codes. 2. A method as recited in claim 1, where said digital resources include: licensed executable programs, secured data files, e-mail accounts, user profiles, network profiles, and attached peripheral devices. 3. A method as recited in claim 1, wherein said access control codes are automatically relayed between the digital device and the PDA when the PDA is electronically connected with at least one of a I/O cradle or an I/O module. 4. A method as recited in claim 3, wherein said I/O module comprises at least one of a serial port, a parallel port, an IR port, a PDA cradle connection interface, an RF transceiver, a Wegand interface, 2 magnetic sensor, a bar code render, a modem, a NIC, a USB, or 2 laser communication devices." Thompson at 15:1-20. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

'619 Patent – Claim 37	Thompson
[37pre] 37. A method for sharing a messaging account, the method comprising:	To the extent the preamble is limiting, Thompson discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:  FIG. 1 Thompson, Fig. 1. *See also*, Figs. 2-5. "An access control system combining PDA functionality with user authentication so that only the authorized user or users may obtain access control codes from a PDA device for an access control point. The access control point can be a computer terminal (108), a computer file, a door, a checkstand, a visa authorization point, a gate, or other situation wherein high security is desirable. In a preferred embodiment, the access control system attaches to a computer (108) via a PDA cradle (104) and transmits access control codes that include a series of authentication codes or identification codes having encoded data stored within a PDA database. In another form of the invention, user authentication is obtained by comparing biometric data such as a fingerprint with digitally stored data of the authorized user. A decision to

'619 Patent – Claim 37	Thompson
	grant access affects the release, an electronic release or electronic strike, or electronic software hold. If desired, a write feature can be included into the system whereby each access control point accessed or attempted to be accessed by a PDA user will be recorded on the PDA to determine where access has been attempted. Additional records could be maintained along with the authentication I.D. including checking account information, credit card information, membership information, network information, user profile information (120), e-mail information (118), and personal information." Thompson at ABSTRACT. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[37a] authenticating a device for access to the messaging account;	Thompson discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22h], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

'619 Patent – Claim 37	Thompson
[37b] optically receiving information including a displayed service activation code from a remote device;	Thompson discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22c], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[37c] registering the remote device for access to the messaging account using the service activation code;	Thompson discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22d], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[37d] receiving a message for the messaging account;	Thompson discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22e], above. Furthermore, this claim element is obvious in light of this reference itself, when

'619 Patent – Claim 37	Thompson
	combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[37e] encrypting the message using an encryption key; and	Thompson discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22f], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[37f] sending the message to the remote device.	Thompson discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22g], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine

'619 Patent – Claim 37	Thompson
	references and additional details may be found in the Cover Pleading and Exhibit 619-B.

'619 Patent – Claim 38	Thompson
[38] The method of claim 37, wherein the information including the service activation code is received by the device in response to user input at the remote device.	Thompson discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [23], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

'619 Patent – Claim 39	Thompson
[39] The method of claim 38, wherein the information including the service activation code is received by the device in an off-line communication.	Thompson discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [24], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill

'619 Patent – Claim 39	Thompson
	in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

'619 Patent – Claim 40	Thompson
[40] The method of claim 39, wherein the off-line communication prevents eavesdropping of the service activation code.	Thompson discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [26], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

'619 Patent – Claim 41	Thompson
[41] The method of claim 37, wherein the authentication of the device relies on the authentication of the messaging system.	Thompson discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [27], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in

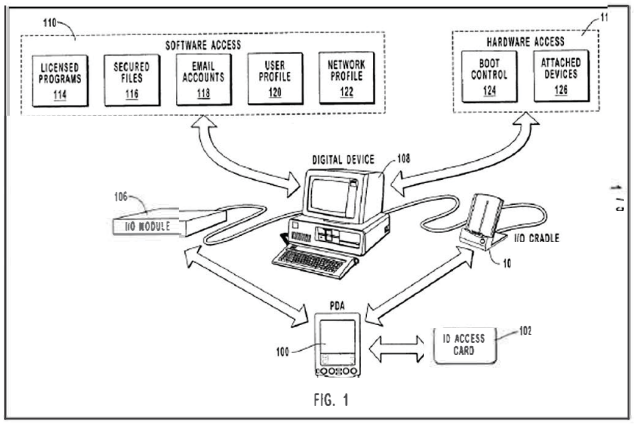
'619 Patent – Claim 41	Thompson
	Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

'619 Patent – Claim 42	Thompson
[42] The method of claim 41, wherein the authentication of the messaging system includes a username and password.	Thompson discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [28], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

'619 Patent – Claim 46	Thompson
[46] The method of claim 37, wherein the encryption key is closely related to the service activation code.	Thompson discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:

'619 Patent – Claim 46	Thompson
	See [32], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

'619 Patent – Claim 50	Thompson
[50] The method of claim 37, wherein a control message is received from the remote device upon user interaction with the message.	Thompson discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [36], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

'619 Patent – Claim 51	Thompson
[51pre] 51. A non-transient computer-readable medium containing program instructions for causing a device to perform a method, the method comprising:	To the extent the preamble is limiting, Thompson discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:  FIG. 1 Thompson, Fig. 1. *See also*, Figs. 2-5. "An access control system combining PDA functionality with user authentication so that only the authorized user or users may obtain access control codes from a PDA device for an access control point. The access control point can be a computer terminal (108), a computer file, a door, a checkstand, a visa authorization point, a gate, or other situation wherein high security is desirable. In a preferred embodiment, the access control system attaches to a computer (108) via a PDA cradle (104) and transmits access control codes that include a series of authentication codes or identification codes having encoded data stored within a PDA database. In another form of the invention, user authentication is obtained by comparing biometric data such as a fingerprint with digitally stored data of the authorized user. A decision to

'619 Patent – Claim 51	Thompson
	grant access affects the release, an electronic release or electronic strike, or electronic software hold. If desired, a write feature can be included into the system whereby each access control point accessed or attempted to be accessed by a PDA user will be recorded on the PDA to determine where access has been attempted. Additional records could be maintained along with the authentication I.D. including checking account information, credit card information, membership information, network information, user profile information (120), e-mail information (118), and personal information." Thompson at ABSTRACT. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[51a] optically receiving information including a displayed service activation code from a remote device;	Thompson discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22c], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

'619 Patent – Claim 51	Thompson
[51b] registering the remote device for access to a messaging account using the service activation code;	Thompson discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22d], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[51c] receiving a message for the messaging account;	Thompson discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22e], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[51d] encrypting the message using an encryption key; and	Thompson discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22f], above. Furthermore, this claim element is obvious in light of this reference itself, when

'619 Patent – Claim 51	Thompson
	combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[51e] sending the message to the remote device,	Thompson discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22g], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[51f] wherein the device is authenticated to access the messaging account.	Thompson discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22h], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine

’619 Patent – Claim 51	Thompson
	references and additional details may be found in the Cover Pleading and Exhibit 619-B.

’619 Patent – Claim 52	Thompson
[52] The method of claim 51, wherein a control message is received from the remote device upon user interaction with the message.	Thompson discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [36], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

EXHIBIT 619-A02

Invalidity Contentions for U.S. Patent No. 10,027,619 ("the '619 patent")

Based on: U.S. Patent No. 7,984,488 to Cross et al. ("Cross")

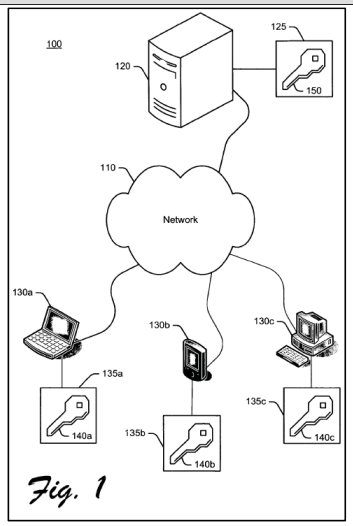
Based on SEVEN's apparent positions as to the scope of the patent's claims, as best they can be deciphered, the reference(s) charted below anticipate(s) or at least render(s) obvious the identified claims. The portions of the prior art reference cited below are not exhaustive but are exemplary in nature. Where Apple identifies a portion of the prior art reference's text, the identification should be understood as referencing any corresponding figure or diagram, and vice versa.

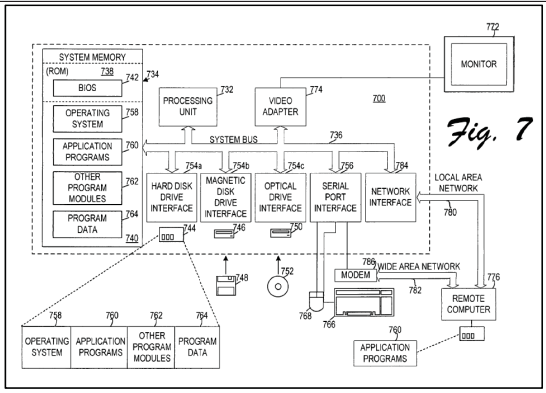
This disclosure is not an admission that Apple concedes any claim construction implied or suggested by SEVEN's apparent positions as to the scope of the patent's claims, nor is it an admission by Apple that any of its products are covered by or infringe the patent's claims, particularly when they are properly construed and applied. Apple is not taking any claim construction positions through this disclosure, including whether the preamble is a limitation.

Apple reserves the right to rely on additional citations or sources of evidence that also may be applicable, or that may become applicable in light of claim construction, changes in SEVEN's infringement contentions, and/or information obtained during discovery as the case progresses. Apple further reserves the right to amend or supplement this claim chart at a later date as more fully set forth in the Invalidity Contentions.

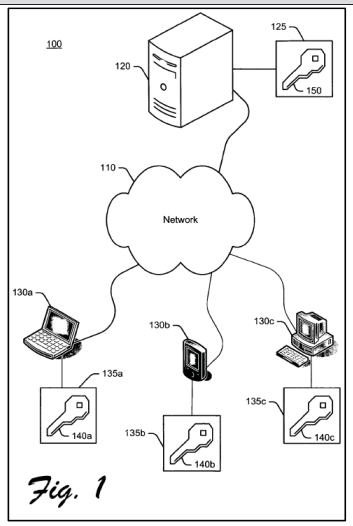
Cross qualifies as prior art under at least pre-AIA 35 U.S.C. §§ 102(a) and/or (e). Cross is a U.S. Patent that was filed on April 9, 2004, published on November 17, 2005, and issued on July 19, 2011.

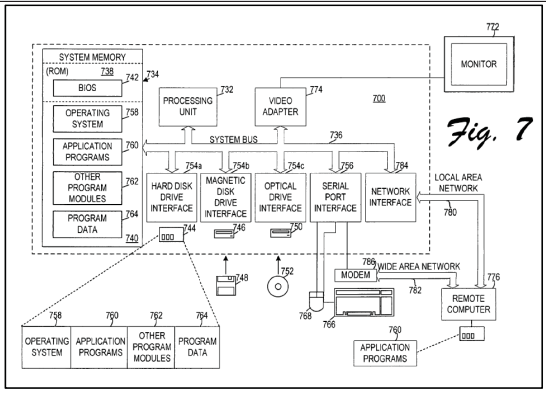
'619 Patent – Claim 22	Cross
[22pre] A device comprising:	To the extent the preamble is limiting, Cross discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:

’619 Patent – Claim 22	Cross
	 Cross, Fig. 1.

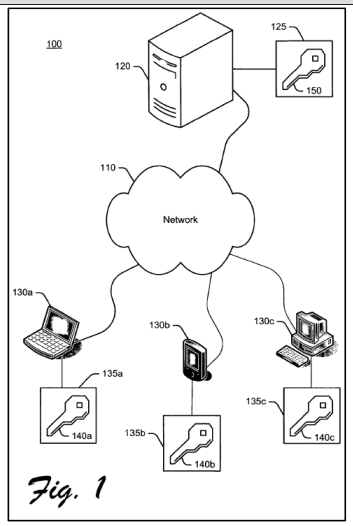
’619 Patent – Claim 22	Cross
	 Fig. 7 Cross Fig. 7. “FIG. 1 is a schematic illustration of an exemplary networked computing system 100 in which credential roaming may be implemented. The networked computer system 100 may include one or more communication networks 110, such as local area network (LAN) and/or wide area network (WAN). One or more hosts 120 and one or more clients 130 a-c may be communicatively coupled over the communication network(s) 110. Host 120 and clients 130 a-c (hereinafter generally referred to as clients 130) may connect to a network via a communication connection such as, e.g., an Ethernet connection. Although there are no theoretical limits on the number of devices that can be included in a network such as networked computing system 100, the number of devices are limited primarily by the connectivity implemented in the communication network. The terms “host” and “client” both refer to the hardware and software (the entire computer system) used to perform various computing services. For

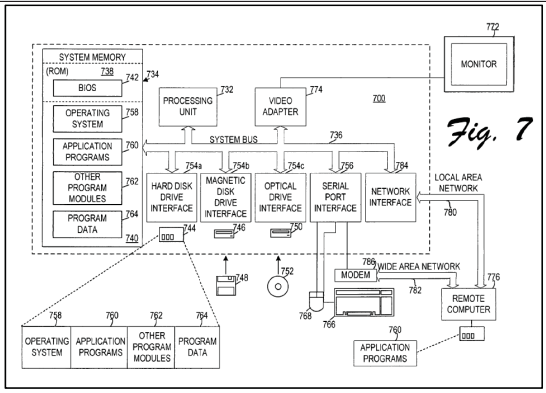
’619 Patent – Claim 22	Cross
	example, a host may be implemented as a server computer that is dedicated to server applications or that also runs other applications. A client may be implemented as a stand-alone desktop or laptop personal computer (PC), workstation, personal digital assistant (PDA), or any of a wide variety of electronic appliances, to name only a few examples.” Cross at 3:13-37. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[22a] a radio;	Cross discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:

’619 Patent – Claim 22	Cross
	 Fig. 1 Cross, Fig. 1.

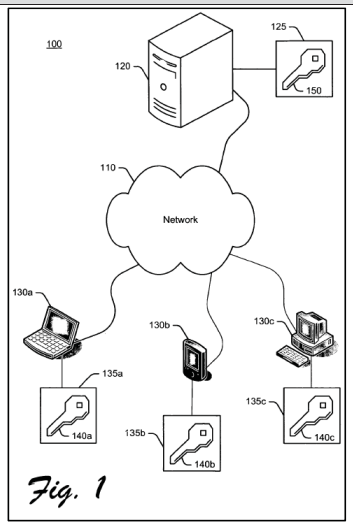
’619 Patent – Claim 22	Cross
	 Cross Fig. 7. “FIG. 7 is a schematic illustration of an exemplary computing device 700 that can be utilized to implement credential roaming. Computing device 700 includes one or more processors or processing units 732, a system memory 734, and a bus 736 that couples various system components including the system memory 734 to processors 732. The bus 736 represents one or more of any of several types of bus structures, including a memory bus or memory controller, a peripheral bus, an accelerated graphics port, and a processor or local bus using any of a variety of bus architectures. The system memory 734 includes read only memory (ROM) 738 and random access memory (RAM) 740. A basic input/output system (BIOS) 742, containing the basic routines that help to transfer information between elements within computing device 700, such as during start-up, is stored in ROM 738.” Cross at 10:47-61. “A number of program modules may be stored on the hard disk 744, magnetic disk 748, optical disk 752, ROM 738, or RAM 740, including an operating system 758, one or more application programs 760, other program into

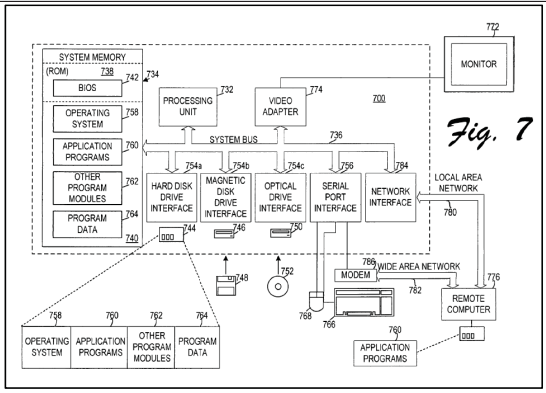
’619 Patent – Claim 22	Cross
	computing device 700 through input devices such as a keyboard 766 and a pointing device 768. Other input devices (not shown) may include a microphone, joystick, game pad, satellite dish, scanner, or the like. These and other input devices are connected to the processing unit 732 through an interface 756 that is coupled to the bus 736. A monitor 772 or other type of display device is also connected to the bus 736 via an interface, such as a video adapter 774.” Cross at 11:14-25. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[22b] a processor and memory containing instructions executable by the processor whereby the device is operable to:	Cross discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:

’619 Patent – Claim 22	Cross
	 Fig. 1 Cross, Fig. 1.

’619 Patent – Claim 22	Cross
	 Cross Fig. 7. “FIG. 7 is a schematic illustration of an exemplary computing device 700 that can be utilized to implement credential roaming. Computing device 700 includes one or more processors or processing units 732, a system memory 734, and a bus 736 that couples various system components including the system memory 734 to processors 732. The bus 736 represents one or more of any of several types of bus structures, including a memory bus or memory controller, a peripheral bus, an accelerated graphics port, and a processor or local bus using any of a variety of bus architectures. The system memory 734 includes read only memory (ROM) 738 and random access memory (RAM) 740. A basic input/output system (BIOS) 742, containing the basic routines that help to transfer information between elements within computing device 700, such as during start-up, is stored in ROM 738.” Cross at 10:47-61. “Generally, the data processors of computing device 700 are programmed by means of instructions stored at different times in the various computer-readable storage media of the computer. Programs and operating systems may be

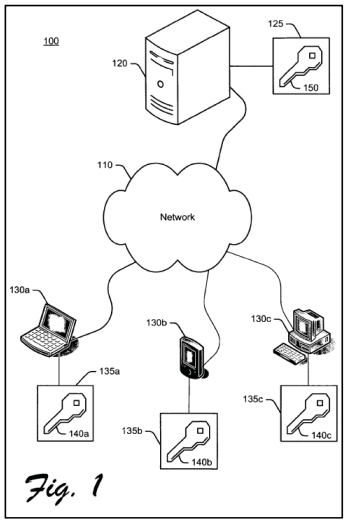
'619 Patent – Claim 22	Cross
	distributed, for example, on floppy disks, CD-ROMs, or electronically, and are installed or loaded into the secondary memory of a computer. At execution, the programs are loaded at least partially into the computer's primary electronic memory." Cross at 11:26-33. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[22c] optically receive information including a displayed service activation code from a remote device;	Cross discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:

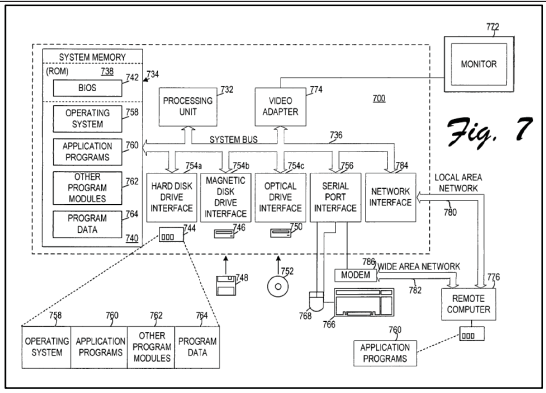
’619 Patent – Claim 22	Cross
	 Fig. 1 Cross, Fig. 1.

’619 Patent – Claim 22	Cross
	 *Fig. 7* Cross Fig. 7. “An exemplary system enabling credential roaming among a plurality of different computing devices may include an event handler to receive event notifications such as, e.g., a client logon. The event handler may invoke a management service in response to receiving an event notification. The management service may include a synchronizing module to synchronize a user's credentials with a remote directory service, such as, e.g., Active Directory, so that the user's credentials are available from any of a number of different computing devices.” Cross at Abstract. “FIG. 1 is a schematic illustration of an exemplary networked computing system 100 in which credential roaming may be implemented. The networked computer system 100 may include one or more communication networks 110, such as local area network (LAN) and/or wide area network (WAN). One or more hosts 120 and one or more clients 130 a-c may be communicatively coupled over the communication network(s) 110.

’619 Patent – Claim 22	Cross
	Host 120 and clients 130 a-c (hereinafter generally referred to as clients 130) may connect to a network via a communication connection such as, e.g., an Ethernet connection. Although there are no theoretical limits on the number of devices that can be included in a network such as networked computing system 100, the number of devices are limited primarily by the connectivity implemented in the communication network. The terms “host” and “client” both refer to the hardware and software (the entire computer system) used to perform various computing services. For example, a host may be implemented as a server computer that is dedicated to server applications or that also runs other applications. A client may be implemented as a stand-alone desktop or laptop personal computer (PC), workstation, personal digital assistant (PDA), or any of a wide variety of electronic appliances, to name only a few examples.” Cross at 3:13-37. “Credentials 140 a-c (hereinafter generally referred to as credentials 140) may be provided at one or more of the clients 130. Credentials may be provided, for example, for symmetric and/or asymmetric encryption/decryption of data for secure communication over network 110, to apply a digital signature to content, or to authenticate to a system, to name only a few examples. Any number of credentials 140 may be stored in a local cache 135 a-c (hereinafter generally referred to as local cache 135). Local cache 135 may include a user profile or other repository (e.g., for user settings and credentials) although other implementations are also contemplated. It is noted that the credentials 140 may include any of a wide variety of different types of credentials, such as, e.g., symmetric encryption keys, asymmetric encryption key pairs, X.509 certificates, XrML licenses, tokens, and authentication/authorization credentials to name only a few exemplary credentials. Of course credentials 140 are not limited to these examples and may include other types of credentials now known or later developed.” Cross at 3:40-57.

'619 Patent – Claim 22	Cross
	"In an exemplary implementation, local credentials 140 may be synchronized with remote credentials 150 provided at a remote cache 125, e.g., at one or more hosts 120 or a shared cache at another client 130 in a workgroup environment. Accordingly, the user has available a current and complete set of credentials when the user logs onto other clients 130. Remote cache 125 may be implemented as a directory service, such as a distributed lightweight directory access protocol (LDAP) or X.500 directory service. The directory service may be monolithic, or it may be distributed as a multi-master implementation or master-slave implementation. Remote cache 125 may stored in a protected or encrypted state so that the remote credentials 150 are not exposed to compromise, theft, or exploit by unauthorized users." Cross at 4:4-19. "Computing device 700 further includes a hard disk drive 744 for reading from and writing to a hard disk (not shown), and may include a magnetic disk drive 746 for reading from and writing to a removable magnetic disk 748, and an optical disk drive 750 for reading from or writing to a removable optical disk 752 such as a CD ROM or other optical media. The hard disk drive 744, magnetic disk drive 746, and optical disk drive 750 are connected to the bus 736 by appropriate interfaces 754 a, 754 b, and 754 c. The drives and their associated computer-readable media provide nonvolatile storage of computer-readable instructions, data structures, program modules and other data for computing device 700. Although the exemplary environment described herein employs a hard disk, a removable magnetic disk 748 and a removable optical disk 752, other types of computer-readable media such as magnetic cassettes, flash memory cards, digital video disks, random access memories (RAMs), read only memories (ROMs), and the like, may also be used in the exemplary operating environment." Cross at 10:63-11:13. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in

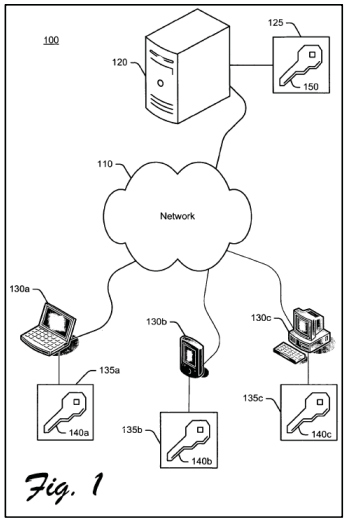
’619 Patent – Claim 22	Cross
	Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[22d] register the remote device for access to a messaging account using the service activation code;	Cross discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:  Cross, Fig. 1.

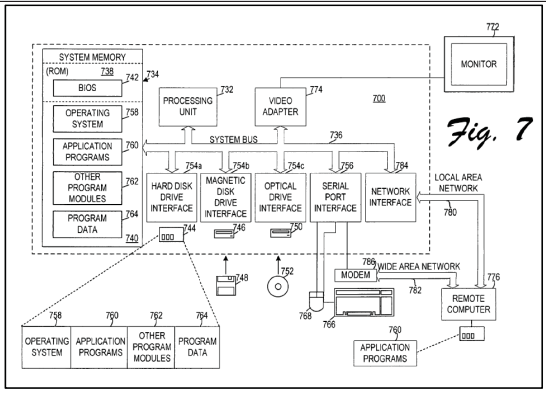
’619 Patent – Claim 22	Cross
	 *Fig. 7* Cross Fig. 7. “Various types of encryption schemes are widely used to secure data (e.g., an email message or file) for communication over a network. For example, in symmetric encryption, both the user that is encrypting data and the user that is decrypting the data need copies of the same encryption key. Asymmetric encryption, also known as public key encryption, uses key pairs (e.g., a public key and a private key). In asymmetric encryption the public keys may be shared but the private keys are not.” Cross at 1:18-26. “Briefly, credential roaming may be implemented to synchronize local credentials (encryption keys, certificates, tokens, etc.) at any number (n) of computing devices. For purposes of illustration, a user may change, modify, add and/or remove credentials at his or her laptop or desktop computer. When the user logs out of the laptop or desktop computer, a management service synchronizes the local credentials with a remote cache. The remote cache may be implemented as a remote directory service, such as, e.g., Active Directory available for the Microsoft WINDOWS® operating environment.

’619 Patent – Claim 22	Cross
	Alternatively, the management service may synchronize in response to other events. For example, real-time synchronizing may occur in response to one or more credentials being added, removed and/or modified. Later, the user may use his or her personal digital assistant (PDA) or mobile phone to retrieve email messages. When the user logs onto the mobile device, the user's credentials are synchronized with the remote directory service so that the user has available a current and complete set of credentials, such as, e.g., encryption credentials for sending/receiving email messages.” Cross at 2:46-67. “An exemplary system enabling credential roaming among a plurality of different computing devices may include an event handler to receive event notifications such as, e.g., a client logon. The event handler may invoke a management service in response to receiving an event notification. The management service may include a synchronizing module to synchronize a user's credentials with a remote directory service, such as, e.g., Active Directory, so that the user's credentials are available from any of a number of different computing devices.” Cross at Abstract. “FIG. 1 is a schematic illustration of an exemplary networked computing system 100 in which credential roaming may be implemented. The networked computer system 100 may include one or more communication networks 110, such as local area network (LAN) and/or wide area network (WAN). One or more hosts 120 and one or more clients 130 a-c may be communicatively coupled over the communication network(s) 110. Host 120 and clients 130 a-c (hereinafter generally referred to as clients 130) may connect to a network via a communication connection such as, e.g., an Ethernet connection. Although there are no theoretical limits on the number of devices that can be included in a network such as networked computing system 100, the number of devices are limited primarily by the connectivity implemented in the communication network.

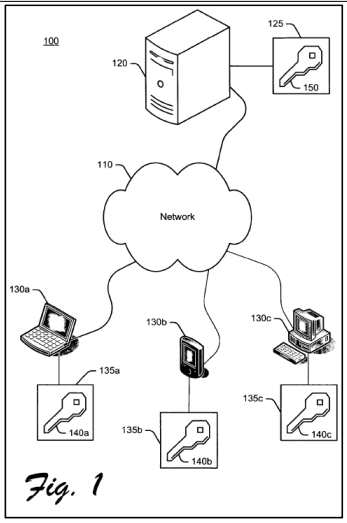
'619 Patent – Claim 22	Cross
	The terms "host" and "client" both refer to the hardware and software (the entire computer system) used to perform various computing services. For example, a host may be implemented as a server computer that is dedicated to server applications or that also runs other applications. A client may be implemented as a stand-alone desktop or laptop personal computer (PC), workstation, personal digital assistant (PDA), or any of a wide variety of electronic appliances, to name only a few examples." Cross at 3:13-37. "Credentials 140 a-c (hereinafter generally referred to as credentials 140) may be provided at one or more of the clients 130. Credentials may be provided, for example, for symmetric and/or asymmetric encryption/decryption of data for secure communication over network 110, to apply a digital signature to content, or to authenticate to a system, to name only a few examples. Any number of credentials 140 may be stored in a local cache 135 a-c (hereinafter generally referred to as local cache 135). Local cache 135 may include a user profile or other repository (e.g., for user settings and credentials) although other implementations are also contemplated. It is noted that the credentials 140 may include any of a wide variety of different types of credentials, such as, e.g., symmetric encryption keys, asymmetric encryption key pairs, X.509 certificates, XrML licenses, tokens, and authentication/authorization credentials to name only a few exemplary credentials. Of course credentials 140 are not limited to these examples and may include other types of credentials now known or later developed." Cross at 3:40-57. "In an exemplary implementation, local credentials 140 may be synchronized with remote credentials 150 provided at a remote cache 125, e.g., at one or more hosts 120 or a shared cache at another client 130 in a workgroup environment. Accordingly, the user has available a current and complete set of credentials when the user logs onto other clients 130. Remote cache 125 may be implemented as a directory service, such as a

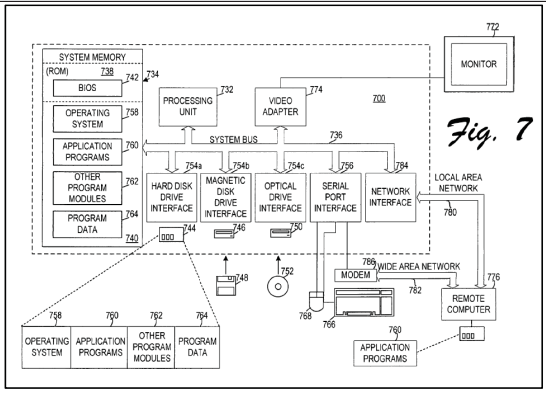
’619 Patent – Claim 22	Cross
	distributed lightweight directory access protocol (LDAP) or X.500 directory service. The directory service may be monolithic, or it may be distributed as a multi-master implementation or master-slave implementation. Remote cache 125 may stored in a protected or encrypted state so that the remote credentials 150 are not exposed to compromise, theft, or exploit by unauthorized users.” Cross at 4:4-19. “Computing device 700 further includes a hard disk drive 744 for reading from and writing to a hard disk (not shown), and may include a magnetic disk drive 746 for reading from and writing to a removable magnetic disk 748, and an optical disk drive 750 for reading from or writing to a removable optical disk 752 such as a CD ROM or other optical media. The hard disk drive 744, magnetic disk drive 746, and optical disk drive 750 are connected to the bus 736 by appropriate interfaces 754 a, 754 b, and 754 c. The drives and their associated computer-readable media provide nonvolatile storage of computer-readable instructions, data structures, program modules and other data for computing device 700. Although the exemplary environment described herein employs a hard disk, a removable magnetic disk 748 and a removable optical disk 752, other types of computer-readable media such as magnetic cassettes, flash memory cards, digital video disks, random access memories (RAMs), read only memories (ROMs), and the like, may also be used in the exemplary operating environment.” Cross at 10:63-11:13. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

’619 Patent – Claim 22	Cross
[22e] receive a message for the messaging account;	Cross discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:  Cross, Fig. 1.

’619 Patent – Claim 22	Cross
	 *Fig. 7* Cross Fig. 7. “Various types of encryption schemes are widely used to secure data (e.g., an email message or file) for communication over a network. For example, in symmetric encryption, both the user that is encrypting data and the user that is decrypting the data need copies of the same encryption key. Asymmetric encryption, also known as public key encryption, uses key pairs (e.g., a public key and a private key). In asymmetric encryption the public keys may be shared but the private keys are not.” Cross at 1:18-26. “Briefly, credential roaming may be implemented to synchronize local credentials (encryption keys, certificates, tokens, etc.) at any number (n) of computing devices. For purposes of illustration, a user may change, modify, add and/or remove credentials at his or her laptop or desktop computer. When the user logs out of the laptop or desktop computer, a management service synchronizes the local credentials with a remote cache. The remote cache may be implemented as a remote directory service, such as, e.g., Active Directory available for the Microsoft WINDOWS® operating environment.

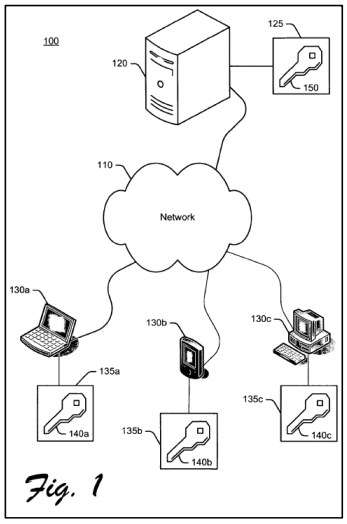
’619 Patent – Claim 22	Cross
	Alternatively, the management service may synchronize in response to other events. For example, real-time synchronizing may occur in response to one or more credentials being added, removed and/or modified. Later, the user may use his or her personal digital assistant (PDA) or mobile phone to retrieve email messages. When the user logs onto the mobile device, the user's credentials are synchronized with the remote directory service so that the user has available a current and complete set of credentials, such as, e.g., encryption credentials for sending/receiving email messages.” Cross at 2:46-67. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[22f] encrypt the message using an encryption key; and	Cross discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:

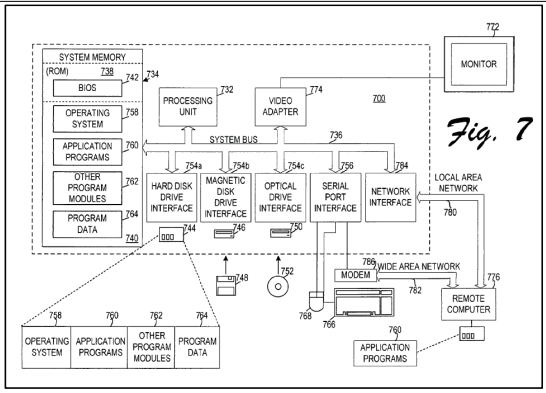
’619 Patent – Claim 22	Cross
	 Cross, Fig. 1.

’619 Patent – Claim 22	Cross
	 *Fig. 7* Cross Fig. 7. “Various types of encryption schemes are widely used to secure data (e.g., an email message or file) for communication over a network. For example, in symmetric encryption, both the user that is encrypting data and the user that is decrypting the data need copies of the same encryption key. Asymmetric encryption, also known as public key encryption, uses key pairs (e.g., a public key and a private key). In asymmetric encryption the public keys may be shared but the private keys are not.” Cross at 1:18-26. “Briefly, credential roaming may be implemented to synchronize local credentials (encryption keys, certificates, tokens, etc.) at any number (n) of computing devices. For purposes of illustration, a user may change, modify, add and/or remove credentials at his or her laptop or desktop computer. When the user logs out of the laptop or desktop computer, a management service synchronizes the local credentials with a remote cache. The remote cache may be implemented as a remote directory service, such as, e.g., Active Directory available for the Microsoft WINDOWS® operating environment.

’619 Patent – Claim 22	Cross
	Alternatively, the management service may synchronize in response to other events. For example, real-time synchronizing may occur in response to one or more credentials being added, removed and/or modified. Later, the user may use his or her personal digital assistant (PDA) or mobile phone to retrieve email messages. When the user logs onto the mobile device, the user's credentials are synchronized with the remote directory service so that the user has available a current and complete set of credentials, such as, e.g., encryption credentials for sending/receiving email messages.” Cross at 2:46-67. “FIG. 1 is a schematic illustration of an exemplary networked computing system 100 in which credential roaming may be implemented. The networked computer system 100 may include one or more communication networks 110, such as local area network (LAN) and/or wide area network (WAN). One or more hosts 120 and one or more clients 130 a-c may be communicatively coupled over the communication network(s) 110. Host 120 and clients 130 a-c (hereinafter generally referred to as clients 130) may connect to a network via a communication connection such as, e.g., an Ethernet connection. Although there are no theoretical limits on the number of devices that can be included in a network such as networked computing system 100, the number of devices are limited primarily by the connectivity implemented in the communication network. The terms “host” and “client” both refer to the hardware and software (the entire computer system) used to perform various computing services. For example, a host may be implemented as a server computer that is dedicated to server applications or that also runs other applications. A client may be implemented as a stand-alone desktop or laptop personal computer (PC), workstation, personal digital assistant (PDA), or any of a wide variety of electronic appliances, to name only a few examples.” Cross at 3:13-37. “Credentials 140 a-c (hereinafter generally referred to as credentials 140) may

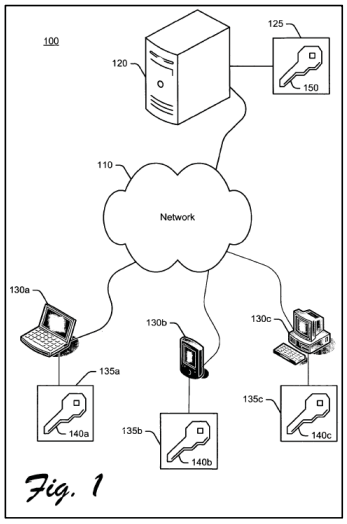
’619 Patent – Claim 22	Cross
	be provided at one or more of the clients 130. Credentials may be provided, for example, for symmetric and/or asymmetric encryption/decryption of data for secure communication over network 110, to apply a digital signature to content, or to authenticate to a system, to name only a few examples. Any number of credentials 140 may be stored in a local cache 135 a-c (hereinafter generally referred to as local cache 135). Local cache 135 may include a user profile or other repository (e.g., for user settings and credentials) although other implementations are also contemplated. It is noted that the credentials 140 may include any of a wide variety of different types of credentials, such as, e.g., symmetric encryption keys, asymmetric encryption key pairs, X.509 certificates, XrML licenses, tokens, and authentication/authorization credentials to name only a few exemplary credentials. Of course credentials 140 are not limited to these examples and may include other types of credentials now known or later developed.” Cross at 3:40-57. “In an exemplary implementation, local credentials 140 may be synchronized with remote credentials 150 provided at a remote cache 125, e.g., at one or more hosts 120 or a shared cache at another client 130 in a workgroup environment. Accordingly, the user has available a current and complete set of credentials when the user logs onto other clients 130. Remote cache 125 may be implemented as a directory service, such as a distributed lightweight directory access protocol (LDAP) or X.500 directory service. The directory service may be monolithic, or it may be distributed as a multi-master implementation or master-slave implementation. Remote cache 125 may stored in a protected or encrypted state so that the remote credentials 150 are not exposed to compromise, theft, or exploit by unauthorized users.” Cross at 4:4-19. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in

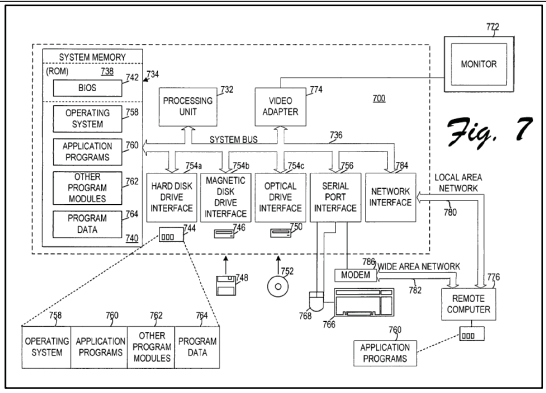
’619 Patent – Claim 22	Cross
	Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[22g] send the message to the remote device,	Cross discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:  Cross, Fig. 1.

’619 Patent – Claim 22	Cross
	 *Fig. 7* Cross Fig. 7. “Various types of encryption schemes are widely used to secure data (e.g., an email message or file) for communication over a network. For example, in symmetric encryption, both the user that is encrypting data and the user that is decrypting the data need copies of the same encryption key. Asymmetric encryption, also known as public key encryption, uses key pairs (e.g., a public key and a private key). In asymmetric encryption the public keys may be shared but the private keys are not.” Cross at 1:18-26. “Briefly, credential roaming may be implemented to synchronize local credentials (encryption keys, certificates, tokens, etc.) at any number (n) of computing devices. For purposes of illustration, a user may change, modify, add and/or remove credentials at his or her laptop or desktop computer. When the user logs out of the laptop or desktop computer, a management service synchronizes the local credentials with a remote cache. The remote cache may be implemented as a remote directory service, such as, e.g., Active Directory available for the Microsoft WINDOWS® operating environment.

’619 Patent – Claim 22	Cross
	Alternatively, the management service may synchronize in response to other events. For example, real-time synchronizing may occur in response to one or more credentials being added, removed and/or modified. Later, the user may use his or her personal digital assistant (PDA) or mobile phone to retrieve email messages. When the user logs onto the mobile device, the user's credentials are synchronized with the remote directory service so that the user has available a current and complete set of credentials, such as, e.g., encryption credentials for sending/receiving email messages.” Cross at 2:46-67. “FIG. 1 is a schematic illustration of an exemplary networked computing system 100 in which credential roaming may be implemented. The networked computer system 100 may include one or more communication networks 110, such as local area network (LAN) and/or wide area network (WAN). One or more hosts 120 and one or more clients 130 a-c may be communicatively coupled over the communication network(s) 110. Host 120 and clients 130 a-c (hereinafter generally referred to as clients 130) may connect to a network via a communication connection such as, e.g., an Ethernet connection. Although there are no theoretical limits on the number of devices that can be included in a network such as networked computing system 100, the number of devices are limited primarily by the connectivity implemented in the communication network. The terms “host” and “client” both refer to the hardware and software (the entire computer system) used to perform various computing services. For example, a host may be implemented as a server computer that is dedicated to server applications or that also runs other applications. A client may be implemented as a stand-alone desktop or laptop personal computer (PC), workstation, personal digital assistant (PDA), or any of a wide variety of electronic appliances, to name only a few examples.” Cross at 3:13-37. “Credentials 140 a-c (hereinafter generally referred to as credentials 140) may

’619 Patent – Claim 22	Cross
	be provided at one or more of the clients 130. Credentials may be provided, for example, for symmetric and/or asymmetric encryption/decryption of data for secure communication over network 110, to apply a digital signature to content, or to authenticate to a system, to name only a few examples. Any number of credentials 140 may be stored in a local cache 135 a-c (hereinafter generally referred to as local cache 135). Local cache 135 may include a user profile or other repository (e.g., for user settings and credentials) although other implementations are also contemplated. It is noted that the credentials 140 may include any of a wide variety of different types of credentials, such as, e.g., symmetric encryption keys, asymmetric encryption key pairs, X.509 certificates, XrML licenses, tokens, and authentication/authorization credentials to name only a few exemplary credentials. Of course credentials 140 are not limited to these examples and may include other types of credentials now known or later developed.” Cross at 3:40-57. “In an exemplary implementation, local credentials 140 may be synchronized with remote credentials 150 provided at a remote cache 125, e.g., at one or more hosts 120 or a shared cache at another client 130 in a workgroup environment. Accordingly, the user has available a current and complete set of credentials when the user logs onto other clients 130. Remote cache 125 may be implemented as a directory service, such as a distributed lightweight directory access protocol (LDAP) or X.500 directory service. The directory service may be monolithic, or it may be distributed as a multi-master implementation or master-slave implementation. Remote cache 125 may stored in a protected or encrypted state so that the remote credentials 150 are not exposed to compromise, theft, or exploit by unauthorized users.” Cross at 4:4-19. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in

’619 Patent – Claim 22	Cross
	Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[22h] wherein the device is authenticated to access the messaging account.	Cross discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:  Cross, Fig. 1.

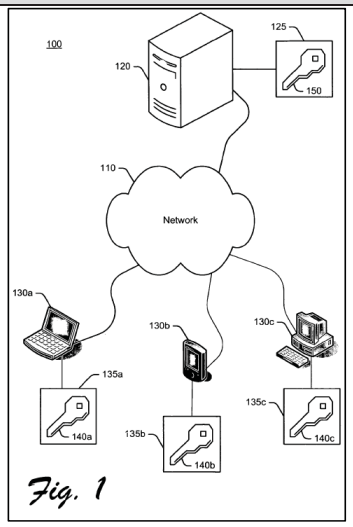
’619 Patent – Claim 22	Cross
	 *Fig. 7* Cross Fig. 7. “Various types of encryption schemes are widely used to secure data (e.g., an email message or file) for communication over a network. For example, in symmetric encryption, both the user that is encrypting data and the user that is decrypting the data need copies of the same encryption key. Asymmetric encryption, also known as public key encryption, uses key pairs (e.g., a public key and a private key). In asymmetric encryption the public keys may be shared but the private keys are not.” Cross at 1:18-26. “Briefly, credential roaming may be implemented to synchronize local credentials (encryption keys, certificates, tokens, etc.) at any number (n) of computing devices. For purposes of illustration, a user may change, modify, add and/or remove credentials at his or her laptop or desktop computer. When the user logs out of the laptop or desktop computer, a management service synchronizes the local credentials with a remote cache. The remote cache may be implemented as a remote directory service, such as, e.g., Active Directory available for the Microsoft WINDOWS® operating environment.

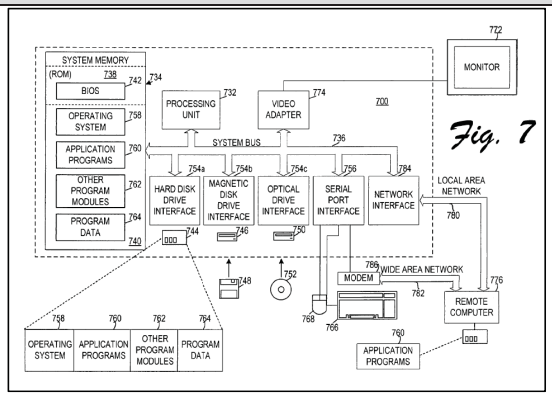
’619 Patent – Claim 22	Cross
	Alternatively, the management service may synchronize in response to other events. For example, real-time synchronizing may occur in response to one or more credentials being added, removed and/or modified. Later, the user may use his or her personal digital assistant (PDA) or mobile phone to retrieve email messages. When the user logs onto the mobile device, the user's credentials are synchronized with the remote directory service so that the user has available a current and complete set of credentials, such as, e.g., encryption credentials for sending/receiving email messages.” Cross at 2:46-67. “FIG. 1 is a schematic illustration of an exemplary networked computing system 100 in which credential roaming may be implemented. The networked computer system 100 may include one or more communication networks 110, such as local area network (LAN) and/or wide area network (WAN). One or more hosts 120 and one or more clients 130 a-c may be communicatively coupled over the communication network(s) 110. Host 120 and clients 130 a-c (hereinafter generally referred to as clients 130) may connect to a network via a communication connection such as, e.g., an Ethernet connection. Although there are no theoretical limits on the number of devices that can be included in a network such as networked computing system 100, the number of devices are limited primarily by the connectivity implemented in the communication network. The terms “host” and “client” both refer to the hardware and software (the entire computer system) used to perform various computing services. For example, a host may be implemented as a server computer that is dedicated to server applications or that also runs other applications. A client may be implemented as a stand-alone desktop or laptop personal computer (PC), workstation, personal digital assistant (PDA), or any of a wide variety of electronic appliances, to name only a few examples.” Cross at 3:13-37. “Credentials 140 a-c (hereinafter generally referred to as credentials 140) may

’619 Patent – Claim 22	Cross
	be provided at one or more of the clients 130. Credentials may be provided, for example, for symmetric and/or asymmetric encryption/decryption of data for secure communication over network 110, to apply a digital signature to content, or to authenticate to a system, to name only a few examples. Any number of credentials 140 may be stored in a local cache 135 a-c (hereinafter generally referred to as local cache 135). Local cache 135 may include a user profile or other repository (e.g., for user settings and credentials) although other implementations are also contemplated. It is noted that the credentials 140 may include any of a wide variety of different types of credentials, such as, e.g., symmetric encryption keys, asymmetric encryption key pairs, X.509 certificates, XrML licenses, tokens, and authentication/authorization credentials to name only a few exemplary credentials. Of course credentials 140 are not limited to these examples and may include other types of credentials now known or later developed.” Cross at 3:40-57. “In an exemplary implementation, local credentials 140 may be synchronized with remote credentials 150 provided at a remote cache 125, e.g., at one or more hosts 120 or a shared cache at another client 130 in a workgroup environment. Accordingly, the user has available a current and complete set of credentials when the user logs onto other clients 130. Remote cache 125 may be implemented as a directory service, such as a distributed lightweight directory access protocol (LDAP) or X.500 directory service. The directory service may be monolithic, or it may be distributed as a multi-master implementation or master-slave implementation. Remote cache 125 may stored in a protected or encrypted state so that the remote credentials 150 are not exposed to compromise, theft, or exploit by unauthorized users.” Cross at 4:4-19. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in

’619 Patent – Claim 22	Cross
	Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

’619 Patent – Claim 23	Cross
[23] The device of claim 22, wherein the information including the service activation code is received by the device in response to user input at the remote device.	Cross discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22pre]-[22h], *above*.

’619 Patent – Claim 23	Cross
	 Fig. 1 Cross, Fig. 1.

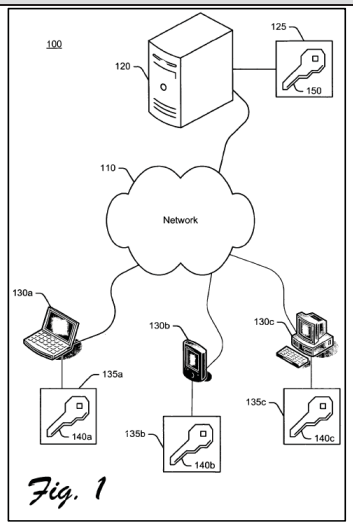
’619 Patent – Claim 23	Cross
	 Fig. 7 Cross Fig. 7. “Various types of encryption schemes are widely used to secure data (e.g., an email message or file) for communication over a network. For example, in symmetric encryption, both the user that is encrypting data and the user that is decrypting the data need copies of the same encryption key. Asymmetric encryption, also known as public key encryption, uses key pairs (e.g., a public key and a private key). In asymmetric encryption the public keys may be shared but the private keys are not.” Cross at 1:18-26. “Briefly, credential roaming may be implemented to synchronize local credentials (encryption keys, certificates, tokens, etc.) at any number (n) of computing devices. For purposes of illustration, a user may change, modify, add and/or remove credentials at his or her laptop or desktop computer. When the user logs out of the laptop or desktop computer, a management service synchronizes the local credentials with a remote cache. The remote cache may be implemented as a remote directory service, such as, e.g., Active Directory available for the Microsoft WINDOWS® operating environment.

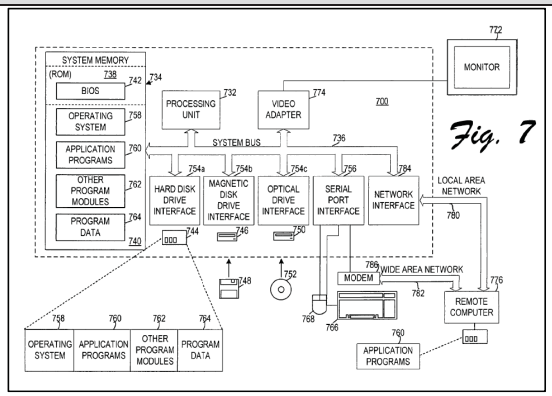
’619 Patent – Claim 23	Cross
	Alternatively, the management service may synchronize in response to other events. For example, real-time synchronizing may occur in response to one or more credentials being added, removed and/or modified. Later, the user may use his or her personal digital assistant (PDA) or mobile phone to retrieve email messages. When the user logs onto the mobile device, the user's credentials are synchronized with the remote directory service so that the user has available a current and complete set of credentials, such as, e.g., encryption credentials for sending/receiving email messages.” Cross at 2:46-67. “FIG. 1 is a schematic illustration of an exemplary networked computing system 100 in which credential roaming may be implemented. The networked computer system 100 may include one or more communication networks 110, such as local area network (LAN) and/or wide area network (WAN). One or more hosts 120 and one or more clients 130 a-c may be communicatively coupled over the communication network(s) 110. Host 120 and clients 130 a-c (hereinafter generally referred to as clients 130) may connect to a network via a communication connection such as, e.g., an Ethernet connection. Although there are no theoretical limits on the number of devices that can be included in a network such as networked computing system 100, the number of devices are limited primarily by the connectivity implemented in the communication network. The terms “host” and “client” both refer to the hardware and software (the entire computer system) used to perform various computing services. For example, a host may be implemented as a server computer that is dedicated to server applications or that also runs other applications. A client may be implemented as a stand-alone desktop or laptop personal computer (PC), workstation, personal digital assistant (PDA), or any of a wide variety of electronic appliances, to name only a few examples.” Cross at 3:13-37. “Credentials 140 a-c (hereinafter generally referred to as credentials 140) may

’619 Patent – Claim 23	Cross
	be provided at one or more of the clients 130. Credentials may be provided, for example, for symmetric and/or asymmetric encryption/decryption of data for secure communication over network 110, to apply a digital signature to content, or to authenticate to a system, to name only a few examples. Any number of credentials 140 may be stored in a local cache 135 a-c (hereinafter generally referred to as local cache 135). Local cache 135 may include a user profile or other repository (e.g., for user settings and credentials) although other implementations are also contemplated. It is noted that the credentials 140 may include any of a wide variety of different types of credentials, such as, e.g., symmetric encryption keys, asymmetric encryption key pairs, X.509 certificates, XrML licenses, tokens, and authentication/authorization credentials to name only a few exemplary credentials. Of course credentials 140 are not limited to these examples and may include other types of credentials now known or later developed.” Cross at 3:40-57. “In an exemplary implementation, local credentials 140 may be synchronized with remote credentials 150 provided at a remote cache 125, e.g., at one or more hosts 120 or a shared cache at another client 130 in a workgroup environment. Accordingly, the user has available a current and complete set of credentials when the user logs onto other clients 130. Remote cache 125 may be implemented as a directory service, such as a distributed lightweight directory access protocol (LDAP) or X.500 directory service. The directory service may be monolithic, or it may be distributed as a multi-master implementation or master-slave implementation. Remote cache 125 may stored in a protected or encrypted state so that the remote credentials 150 are not exposed to compromise, theft, or exploit by unauthorized users.” Cross at 4:4-19. Furthermore, this claim element is obvious in light of this reference itself, when

’619 Patent – Claim 23	Cross
	combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

’619 Patent – Claim 24	Cross
[24] The device of claim 22, wherein the information including the service activation code is received by the device in an off-line communication.	Cross discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22pre]-[22h], *above*.

’619 Patent – Claim 24	Cross
	 Fig. 1 Cross, Fig. 1.

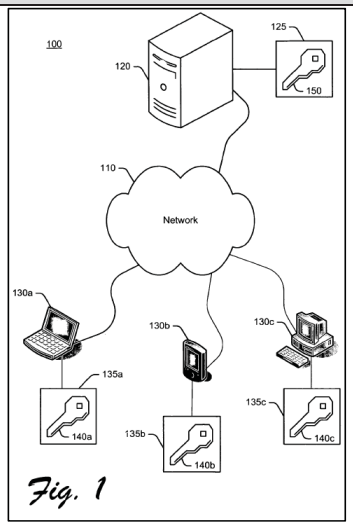
’619 Patent – Claim 24	Cross
	 Fig. 7 Cross Fig. 7. “Various types of encryption schemes are widely used to secure data (e.g., an email message or file) for communication over a network. For example, in symmetric encryption, both the user that is encrypting data and the user that is decrypting the data need copies of the same encryption key. Asymmetric encryption, also known as public key encryption, uses key pairs (e.g., a public key and a private key). In asymmetric encryption the public keys may be shared but the private keys are not.” Cross at 1:18-26. “Briefly, credential roaming may be implemented to synchronize local credentials (encryption keys, certificates, tokens, etc.) at any number (n) of computing devices. For purposes of illustration, a user may change, modify, add and/or remove credentials at his or her laptop or desktop computer. When the user logs out of the laptop or desktop computer, a management service synchronizes the local credentials with a remote cache. The remote cache may be implemented as a remote directory service, such as, e.g., Active Directory available for the Microsoft WINDOWS® operating environment.

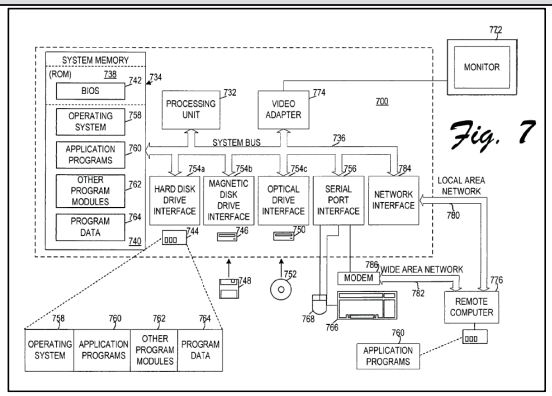
’619 Patent – Claim 24	Cross
	Alternatively, the management service may synchronize in response to other events. For example, real-time synchronizing may occur in response to one or more credentials being added, removed and/or modified. Later, the user may use his or her personal digital assistant (PDA) or mobile phone to retrieve email messages. When the user logs onto the mobile device, the user's credentials are synchronized with the remote directory service so that the user has available a current and complete set of credentials, such as, e.g., encryption credentials for sending/receiving email messages.” Cross at 2:46-67. “FIG. 1 is a schematic illustration of an exemplary networked computing system 100 in which credential roaming may be implemented. The networked computer system 100 may include one or more communication networks 110, such as local area network (LAN) and/or wide area network (WAN). One or more hosts 120 and one or more clients 130 a-c may be communicatively coupled over the communication network(s) 110. Host 120 and clients 130 a-c (hereinafter generally referred to as clients 130) may connect to a network via a communication connection such as, e.g., an Ethernet connection. Although there are no theoretical limits on the number of devices that can be included in a network such as networked computing system 100, the number of devices are limited primarily by the connectivity implemented in the communication network. The terms “host” and “client” both refer to the hardware and software (the entire computer system) used to perform various computing services. For example, a host may be implemented as a server computer that is dedicated to server applications or that also runs other applications. A client may be implemented as a stand-alone desktop or laptop personal computer (PC), workstation, personal digital assistant (PDA), or any of a wide variety of electronic appliances, to name only a few examples.” Cross at 3:13-37. “Credentials 140 a-c (hereinafter generally referred to as credentials 140) may

’619 Patent – Claim 24	Cross
	be provided at one or more of the clients 130. Credentials may be provided, for example, for symmetric and/or asymmetric encryption/decryption of data for secure communication over network 110, to apply a digital signature to content, or to authenticate to a system, to name only a few examples. Any number of credentials 140 may be stored in a local cache 135 a-c (hereinafter generally referred to as local cache 135). Local cache 135 may include a user profile or other repository (e.g., for user settings and credentials) although other implementations are also contemplated. It is noted that the credentials 140 may include any of a wide variety of different types of credentials, such as, e.g., symmetric encryption keys, asymmetric encryption key pairs, X.509 certificates, XrML licenses, tokens, and authentication/authorization credentials to name only a few exemplary credentials. Of course credentials 140 are not limited to these examples and may include other types of credentials now known or later developed.” Cross at 3:40-57. “In an exemplary implementation, local credentials 140 may be synchronized with remote credentials 150 provided at a remote cache 125, e.g., at one or more hosts 120 or a shared cache at another client 130 in a workgroup environment. Accordingly, the user has available a current and complete set of credentials when the user logs onto other clients 130. Remote cache 125 may be implemented as a directory service, such as a distributed lightweight directory access protocol (LDAP) or X.500 directory service. The directory service may be monolithic, or it may be distributed as a multi-master implementation or master-slave implementation. Remote cache 125 may stored in a protected or encrypted state so that the remote credentials 150 are not exposed to compromise, theft, or exploit by unauthorized users.” Cross at 4:4-19. Furthermore, this claim element is obvious in light of this reference itself, when

’619 Patent – Claim 24	Cross
	combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

’619 Patent – Claim 25	Cross
[25] The device of claim 24, wherein the off-line communication involves a local connection.	Cross discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22pre]-[22h] and [24], *above*.

’619 Patent – Claim 25	Cross
	 Fig. 1 Cross, Fig. 1.

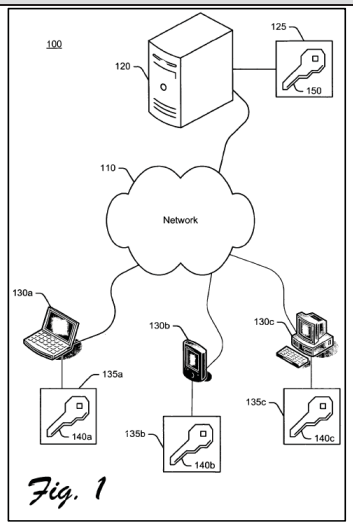
’619 Patent – Claim 25	Cross
	 Fig. 7 Cross Fig. 7. “Various types of encryption schemes are widely used to secure data (e.g., an email message or file) for communication over a network. For example, in symmetric encryption, both the user that is encrypting data and the user that is decrypting the data need copies of the same encryption key. Asymmetric encryption, also known as public key encryption, uses key pairs (e.g., a public key and a private key). In asymmetric encryption the public keys may be shared but the private keys are not.” Cross at 1:18-26. “Briefly, credential roaming may be implemented to synchronize local credentials (encryption keys, certificates, tokens, etc.) at any number (n) of computing devices. For purposes of illustration, a user may change, modify, add and/or remove credentials at his or her laptop or desktop computer. When the user logs out of the laptop or desktop computer, a management service synchronizes the local credentials with a remote cache. The remote cache may be implemented as a remote directory service, such as, e.g., Active Directory available for the Microsoft WINDOWS® operating environment.

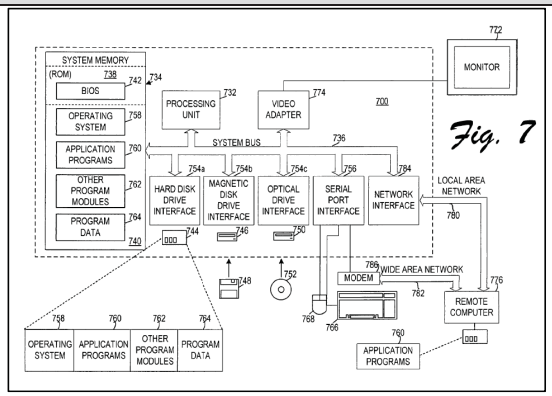
’619 Patent – Claim 25	Cross
	Alternatively, the management service may synchronize in response to other events. For example, real-time synchronizing may occur in response to one or more credentials being added, removed and/or modified. Later, the user may use his or her personal digital assistant (PDA) or mobile phone to retrieve email messages. When the user logs onto the mobile device, the user's credentials are synchronized with the remote directory service so that the user has available a current and complete set of credentials, such as, e.g., encryption credentials for sending/receiving email messages.” Cross at 2:46-67. “FIG. 1 is a schematic illustration of an exemplary networked computing system 100 in which credential roaming may be implemented. The networked computer system 100 may include one or more communication networks 110, such as local area network (LAN) and/or wide area network (WAN). One or more hosts 120 and one or more clients 130 a-c may be communicatively coupled over the communication network(s) 110. Host 120 and clients 130 a-c (hereinafter generally referred to as clients 130) may connect to a network via a communication connection such as, e.g., an Ethernet connection. Although there are no theoretical limits on the number of devices that can be included in a network such as networked computing system 100, the number of devices are limited primarily by the connectivity implemented in the communication network. The terms “host” and “client” both refer to the hardware and software (the entire computer system) used to perform various computing services. For example, a host may be implemented as a server computer that is dedicated to server applications or that also runs other applications. A client may be implemented as a stand-alone desktop or laptop personal computer (PC), workstation, personal digital assistant (PDA), or any of a wide variety of electronic appliances, to name only a few examples.” Cross at 3:13-37. “Credentials 140 a-c (hereinafter generally referred to as credentials 140) may

’619 Patent – Claim 25	Cross
	be provided at one or more of the clients 130. Credentials may be provided, for example, for symmetric and/or asymmetric encryption/decryption of data for secure communication over network 110, to apply a digital signature to content, or to authenticate to a system, to name only a few examples. Any number of credentials 140 may be stored in a local cache 135 a-c (hereinafter generally referred to as local cache 135). Local cache 135 may include a user profile or other repository (e.g., for user settings and credentials) although other implementations are also contemplated. It is noted that the credentials 140 may include any of a wide variety of different types of credentials, such as, e.g., symmetric encryption keys, asymmetric encryption key pairs, X.509 certificates, XrML licenses, tokens, and authentication/authorization credentials to name only a few exemplary credentials. Of course credentials 140 are not limited to these examples and may include other types of credentials now known or later developed.” Cross at 3:40-57. “In an exemplary implementation, local credentials 140 may be synchronized with remote credentials 150 provided at a remote cache 125, e.g., at one or more hosts 120 or a shared cache at another client 130 in a workgroup environment. Accordingly, the user has available a current and complete set of credentials when the user logs onto other clients 130. Remote cache 125 may be implemented as a directory service, such as a distributed lightweight directory access protocol (LDAP) or X.500 directory service. The directory service may be monolithic, or it may be distributed as a multi-master implementation or master-slave implementation. Remote cache 125 may stored in a protected or encrypted state so that the remote credentials 150 are not exposed to compromise, theft, or exploit by unauthorized users.” Cross at 4:4-19. Furthermore, this claim element is obvious in light of this reference itself, when

’619 Patent – Claim 25	Cross
	combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

’619 Patent – Claim 26	Cross
[26] The device of claim 24, wherein the off-line communication prevents eavesdropping of the service activation code.	Cross discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22pre]-[22h] and [24], *above*.

’619 Patent – Claim 26	Cross
	 Cross, Fig. 1.

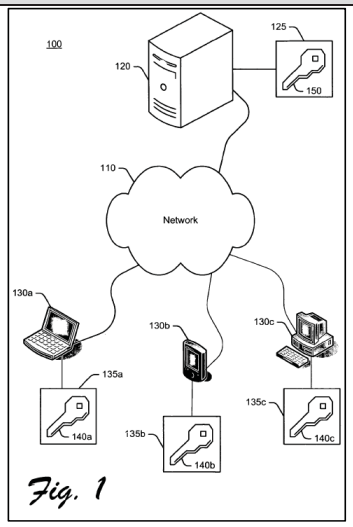
’619 Patent – Claim 26	Cross
	 *Fig. 7* Cross Fig. 7. “Various types of encryption schemes are widely used to secure data (e.g., an email message or file) for communication over a network. For example, in symmetric encryption, both the user that is encrypting data and the user that is decrypting the data need copies of the same encryption key. Asymmetric encryption, also known as public key encryption, uses key pairs (e.g., a public key and a private key). In asymmetric encryption the public keys may be shared but the private keys are not.” Cross at 1:18-26. “Briefly, credential roaming may be implemented to synchronize local credentials (encryption keys, certificates, tokens, etc.) at any number (n) of computing devices. For purposes of illustration, a user may change, modify, add and/or remove credentials at his or her laptop or desktop computer. When the user logs out of the laptop or desktop computer, a management service synchronizes the local credentials with a remote cache. The remote cache may be implemented as a remote directory service, such as, e.g., Active Directory available for the Microsoft WINDOWS® operating environment.

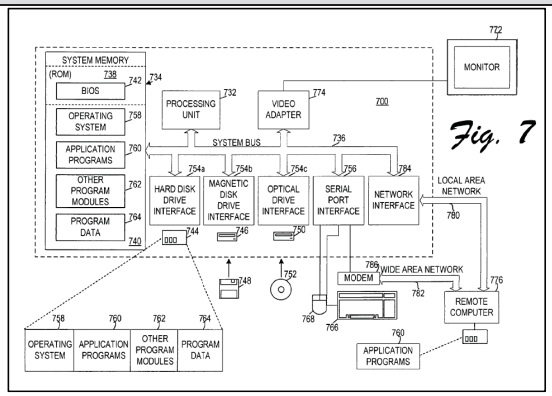
’619 Patent – Claim 26	Cross
	Alternatively, the management service may synchronize in response to other events. For example, real-time synchronizing may occur in response to one or more credentials being added, removed and/or modified. Later, the user may use his or her personal digital assistant (PDA) or mobile phone to retrieve email messages. When the user logs onto the mobile device, the user's credentials are synchronized with the remote directory service so that the user has available a current and complete set of credentials, such as, e.g., encryption credentials for sending/receiving email messages.” Cross at 2:46-67. “FIG. 1 is a schematic illustration of an exemplary networked computing system 100 in which credential roaming may be implemented. The networked computer system 100 may include one or more communication networks 110, such as local area network (LAN) and/or wide area network (WAN). One or more hosts 120 and one or more clients 130 a-c may be communicatively coupled over the communication network(s) 110. Host 120 and clients 130 a-c (hereinafter generally referred to as clients 130) may connect to a network via a communication connection such as, e.g., an Ethernet connection. Although there are no theoretical limits on the number of devices that can be included in a network such as networked computing system 100, the number of devices are limited primarily by the connectivity implemented in the communication network. The terms “host” and “client” both refer to the hardware and software (the entire computer system) used to perform various computing services. For example, a host may be implemented as a server computer that is dedicated to server applications or that also runs other applications. A client may be implemented as a stand-alone desktop or laptop personal computer (PC), workstation, personal digital assistant (PDA), or any of a wide variety of electronic appliances, to name only a few examples.” Cross at 3:13-37. “Credentials 140 a-c (hereinafter generally referred to as credentials 140) may

’619 Patent – Claim 26	Cross
	be provided at one or more of the clients 130. Credentials may be provided, for example, for symmetric and/or asymmetric encryption/decryption of data for secure communication over network 110, to apply a digital signature to content, or to authenticate to a system, to name only a few examples. Any number of credentials 140 may be stored in a local cache 135 a-c (hereinafter generally referred to as local cache 135). Local cache 135 may include a user profile or other repository (e.g., for user settings and credentials) although other implementations are also contemplated. It is noted that the credentials 140 may include any of a wide variety of different types of credentials, such as, e.g., symmetric encryption keys, asymmetric encryption key pairs, X.509 certificates, XrML licenses, tokens, and authentication/authorization credentials to name only a few exemplary credentials. Of course credentials 140 are not limited to these examples and may include other types of credentials now known or later developed.” Cross at 3:40-57. “In an exemplary implementation, local credentials 140 may be synchronized with remote credentials 150 provided at a remote cache 125, e.g., at one or more hosts 120 or a shared cache at another client 130 in a workgroup environment. Accordingly, the user has available a current and complete set of credentials when the user logs onto other clients 130. Remote cache 125 may be implemented as a directory service, such as a distributed lightweight directory access protocol (LDAP) or X.500 directory service. The directory service may be monolithic, or it may be distributed as a multi-master implementation or master-slave implementation. Remote cache 125 may stored in a protected or encrypted state so that the remote credentials 150 are not exposed to compromise, theft, or exploit by unauthorized users.” Cross at 4:4-19. Furthermore, this claim element is obvious in light of this reference itself, when

’619 Patent – Claim 26	Cross
	combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

’619 Patent – Claim 27	Cross
[27] The device of claim 22, wherein the authentication of the device relies on the authentication of the messaging account.	Cross discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22pre]-[22h], *above*.

’619 Patent – Claim 27	Cross
	 Fig. 1 Cross, Fig. 1.

’619 Patent – Claim 27	Cross
	 Fig. 7 Cross Fig. 7. “Various types of encryption schemes are widely used to secure data (e.g., an email message or file) for communication over a network. For example, in symmetric encryption, both the user that is encrypting data and the user that is decrypting the data need copies of the same encryption key. Asymmetric encryption, also known as public key encryption, uses key pairs (e.g., a public key and a private key). In asymmetric encryption the public keys may be shared but the private keys are not.” Cross at 1:18-26. “Briefly, credential roaming may be implemented to synchronize local credentials (encryption keys, certificates, tokens, etc.) at any number (n) of computing devices. For purposes of illustration, a user may change, modify, add and/or remove credentials at his or her laptop or desktop computer. When the user logs out of the laptop or desktop computer, a management service synchronizes the local credentials with a remote cache. The remote cache may be implemented as a remote directory service, such as, e.g., Active Directory available for the Microsoft WINDOWS® operating environment.

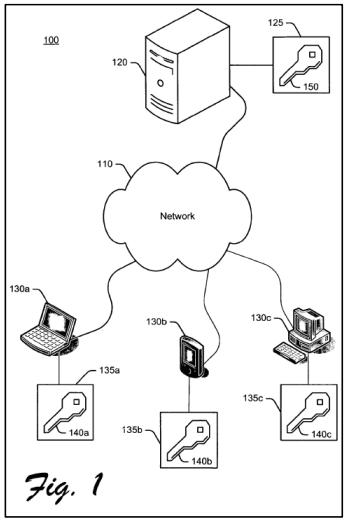
’619 Patent – Claim 27	Cross
	Alternatively, the management service may synchronize in response to other events. For example, real-time synchronizing may occur in response to one or more credentials being added, removed and/or modified. Later, the user may use his or her personal digital assistant (PDA) or mobile phone to retrieve email messages. When the user logs onto the mobile device, the user's credentials are synchronized with the remote directory service so that the user has available a current and complete set of credentials, such as, e.g., encryption credentials for sending/receiving email messages.” Cross at 2:46-67. “FIG. 1 is a schematic illustration of an exemplary networked computing system 100 in which credential roaming may be implemented. The networked computer system 100 may include one or more communication networks 110, such as local area network (LAN) and/or wide area network (WAN). One or more hosts 120 and one or more clients 130 a-c may be communicatively coupled over the communication network(s) 110. Host 120 and clients 130 a-c (hereinafter generally referred to as clients 130) may connect to a network via a communication connection such as, e.g., an Ethernet connection. Although there are no theoretical limits on the number of devices that can be included in a network such as networked computing system 100, the number of devices are limited primarily by the connectivity implemented in the communication network. The terms “host” and “client” both refer to the hardware and software (the entire computer system) used to perform various computing services. For example, a host may be implemented as a server computer that is dedicated to server applications or that also runs other applications. A client may be implemented as a stand-alone desktop or laptop personal computer (PC), workstation, personal digital assistant (PDA), or any of a wide variety of electronic appliances, to name only a few examples.” Cross at 3:13-37. “Credentials 140 a-c (hereinafter generally referred to as credentials 140) may

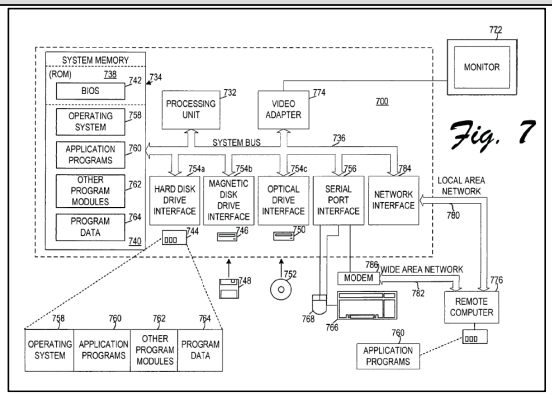
’619 Patent – Claim 27	Cross
	be provided at one or more of the clients 130. Credentials may be provided, for example, for symmetric and/or asymmetric encryption/decryption of data for secure communication over network 110, to apply a digital signature to content, or to authenticate to a system, to name only a few examples. Any number of credentials 140 may be stored in a local cache 135 a-c (hereinafter generally referred to as local cache 135). Local cache 135 may include a user profile or other repository (e.g., for user settings and credentials) although other implementations are also contemplated. It is noted that the credentials 140 may include any of a wide variety of different types of credentials, such as, e.g., symmetric encryption keys, asymmetric encryption key pairs, X.509 certificates, XrML licenses, tokens, and authentication/authorization credentials to name only a few exemplary credentials. Of course credentials 140 are not limited to these examples and may include other types of credentials now known or later developed.” Cross at 3:40-57. “In an exemplary implementation, local credentials 140 may be synchronized with remote credentials 150 provided at a remote cache 125, e.g., at one or more hosts 120 or a shared cache at another client 130 in a workgroup environment. Accordingly, the user has available a current and complete set of credentials when the user logs onto other clients 130. Remote cache 125 may be implemented as a directory service, such as a distributed lightweight directory access protocol (LDAP) or X.500 directory service. The directory service may be monolithic, or it may be distributed as a multi-master implementation or master-slave implementation. Remote cache 125 may stored in a protected or encrypted state so that the remote credentials 150 are not exposed to compromise, theft, or exploit by unauthorized users.” Cross at 4:4-19. Furthermore, this claim element is obvious in light of this reference itself, when

’619 Patent – Claim 27	Cross
	combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

’619 Patent – Claim 28	Cross
[28] The device of claim 27, wherein the authentication of the messaging account includes a username and password.	Cross discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22pre]-[22h] and [27], *above*. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

’619 Patent – Claim 32	Cross
[32] The device of claim 22, wherein the encryption key is closely related to the service activation code.	Cross discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:

’619 Patent – Claim 32	Cross
	See [22pre]-[22h], *above*.  Cross, Fig. 1.

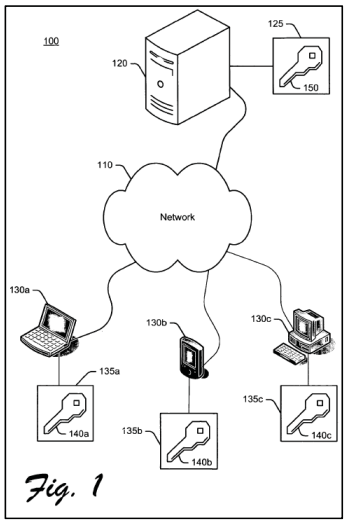
’619 Patent – Claim 32	Cross
	 *Fig. 7* Cross Fig. 7. “Various types of encryption schemes are widely used to secure data (e.g., an email message or file) for communication over a network. For example, in symmetric encryption, both the user that is encrypting data and the user that is decrypting the data need copies of the same encryption key. Asymmetric encryption, also known as public key encryption, uses key pairs (e.g., a public key and a private key). In asymmetric encryption the public keys may be shared but the private keys are not.” Cross at 1:18-26. “Briefly, credential roaming may be implemented to synchronize local credentials (encryption keys, certificates, tokens, etc.) at any number (n) of computing devices. For purposes of illustration, a user may change, modify, add and/or remove credentials at his or her laptop or desktop computer. When the user logs out of the laptop or desktop computer, a management service synchronizes the local credentials with a remote cache. The remote cache may be implemented as a remote directory service, such as, e.g., Active Directory available for the Microsoft WINDOWS® operating environment.

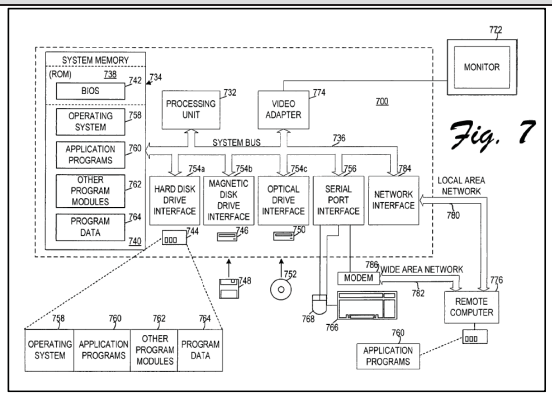
’619 Patent – Claim 32	Cross
	Alternatively, the management service may synchronize in response to other events. For example, real-time synchronizing may occur in response to one or more credentials being added, removed and/or modified. Later, the user may use his or her personal digital assistant (PDA) or mobile phone to retrieve email messages. When the user logs onto the mobile device, the user's credentials are synchronized with the remote directory service so that the user has available a current and complete set of credentials, such as, e.g., encryption credentials for sending/receiving email messages.” Cross at 2:46-67. “FIG. 1 is a schematic illustration of an exemplary networked computing system 100 in which credential roaming may be implemented. The networked computer system 100 may include one or more communication networks 110, such as local area network (LAN) and/or wide area network (WAN). One or more hosts 120 and one or more clients 130 a-c may be communicatively coupled over the communication network(s) 110. Host 120 and clients 130 a-c (hereinafter generally referred to as clients 130) may connect to a network via a communication connection such as, e.g., an Ethernet connection. Although there are no theoretical limits on the number of devices that can be included in a network such as networked computing system 100, the number of devices are limited primarily by the connectivity implemented in the communication network. The terms “host” and “client” both refer to the hardware and software (the entire computer system) used to perform various computing services. For example, a host may be implemented as a server computer that is dedicated to server applications or that also runs other applications. A client may be implemented as a stand-alone desktop or laptop personal computer (PC), workstation, personal digital assistant (PDA), or any of a wide variety of electronic appliances, to name only a few examples.” Cross at 3:13-37. “Credentials 140 a-c (hereinafter generally referred to as credentials 140) may

’619 Patent – Claim 32	Cross
	be provided at one or more of the clients 130. Credentials may be provided, for example, for symmetric and/or asymmetric encryption/decryption of data for secure communication over network 110, to apply a digital signature to content, or to authenticate to a system, to name only a few examples. Any number of credentials 140 may be stored in a local cache 135 a-c (hereinafter generally referred to as local cache 135). Local cache 135 may include a user profile or other repository (e.g., for user settings and credentials) although other implementations are also contemplated. It is noted that the credentials 140 may include any of a wide variety of different types of credentials, such as, e.g., symmetric encryption keys, asymmetric encryption key pairs, X.509 certificates, XrML licenses, tokens, and authentication/authorization credentials to name only a few exemplary credentials. Of course credentials 140 are not limited to these examples and may include other types of credentials now known or later developed.” Cross at 3:40-57. “It is noted that the credentials 140 may include any of a wide variety of different types of credentials, such as, e.g., symmetric encryption keys, asymmetric encryption key pairs, X.509 certificates, XrML licenses, tokens, and authentication/authorization credentials to name only a few exemplary credentials. Of course credentials 140 are not limited to these examples and may include other types of credentials now known or later developed.” Cross at 3:51-58. “In an exemplary implementation, local credentials 140 may be synchronized with remote credentials 150 provided at a remote cache 125, e.g., at one or more hosts 120 or a shared cache at another client 130 in a workgroup environment. Accordingly, the user has available a current and complete set of credentials when the user logs onto other clients 130. Remote cache 125 may be implemented as a directory service, such as a

'619 Patent – Claim 32	Cross
	distributed lightweight directory access protocol (LDAP) or X.500 directory service. The directory service may be monolithic, or it may be distributed as a multi-master implementation or master-slave implementation. Remote cache 125 may stored in a protected or encrypted state so that the remote credentials 150 are not exposed to compromise, theft, or exploit by unauthorized users." Cross at 4:4-19. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

'619 Patent – Claim 33	Cross
[33a] The device of claim 22, wherein the device is further operable to:	Cross discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22pre]-[22h], *above*. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

’619 Patent – Claim 33	Cross
[33b] store an association between at least two of the encryption key, the messaging account, an identifier of the remote device, and the service activation code.	Cross discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22pre]-[22h], *above*.  Cross, Fig. 1.

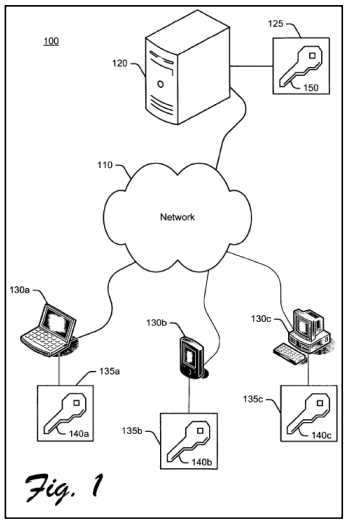
’619 Patent – Claim 33	Cross
	 Fig. 7 Cross Fig. 7. “Various types of encryption schemes are widely used to secure data (e.g., an email message or file) for communication over a network. For example, in symmetric encryption, both the user that is encrypting data and the user that is decrypting the data need copies of the same encryption key. Asymmetric encryption, also known as public key encryption, uses key pairs (e.g., a public key and a private key). In asymmetric encryption the public keys may be shared but the private keys are not.” Cross at 1:18-26. “Briefly, credential roaming may be implemented to synchronize local credentials (encryption keys, certificates, tokens, etc.) at any number (n) of computing devices. For purposes of illustration, a user may change, modify, add and/or remove credentials at his or her laptop or desktop computer. When the user logs out of the laptop or desktop computer, a management service synchronizes the local credentials with a remote cache. The remote cache may be implemented as a remote directory service, such as, e.g., Active Directory available for the Microsoft WINDOWS® operating environment.

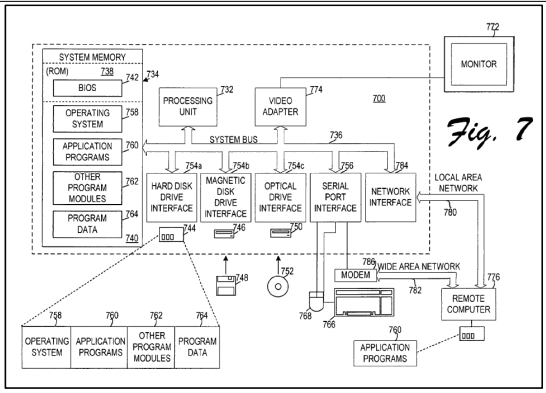
’619 Patent – Claim 33	Cross
	Alternatively, the management service may synchronize in response to other events. For example, real-time synchronizing may occur in response to one or more credentials being added, removed and/or modified. Later, the user may use his or her personal digital assistant (PDA) or mobile phone to retrieve email messages. When the user logs onto the mobile device, the user's credentials are synchronized with the remote directory service so that the user has available a current and complete set of credentials, such as, e.g., encryption credentials for sending/receiving email messages.” Cross at 2:46-67. “FIG. 1 is a schematic illustration of an exemplary networked computing system 100 in which credential roaming may be implemented. The networked computer system 100 may include one or more communication networks 110, such as local area network (LAN) and/or wide area network (WAN). One or more hosts 120 and one or more clients 130 a-c may be communicatively coupled over the communication network(s) 110. Host 120 and clients 130 a-c (hereinafter generally referred to as clients 130) may connect to a network via a communication connection such as, e.g., an Ethernet connection. Although there are no theoretical limits on the number of devices that can be included in a network such as networked computing system 100, the number of devices are limited primarily by the connectivity implemented in the communication network. The terms “host” and “client” both refer to the hardware and software (the entire computer system) used to perform various computing services. For example, a host may be implemented as a server computer that is dedicated to server applications or that also runs other applications. A client may be implemented as a stand-alone desktop or laptop personal computer (PC), workstation, personal digital assistant (PDA), or any of a wide variety of electronic appliances, to name only a few examples.” Cross at 3:13-37. “Credentials 140 a-c (hereinafter generally referred to as credentials 140) may

’619 Patent – Claim 33	Cross
	be provided at one or more of the clients 130. Credentials may be provided, for example, for symmetric and/or asymmetric encryption/decryption of data for secure communication over network 110, to apply a digital signature to content, or to authenticate to a system, to name only a few examples. Any number of credentials 140 may be stored in a local cache 135 a-c (hereinafter generally referred to as local cache 135). Local cache 135 may include a user profile or other repository (e.g., for user settings and credentials) although other implementations are also contemplated. It is noted that the credentials 140 may include any of a wide variety of different types of credentials, such as, e.g., symmetric encryption keys, asymmetric encryption key pairs, X.509 certificates, XrML licenses, tokens, and authentication/authorization credentials to name only a few exemplary credentials. Of course credentials 140 are not limited to these examples and may include other types of credentials now known or later developed.” Cross at 3:40-57. “It is noted that the credentials 140 may include any of a wide variety of different types of credentials, such as, e.g., symmetric encryption keys, asymmetric encryption key pairs, X.509 certificates, XrML licenses, tokens, and authentication/authorization credentials to name only a few exemplary credentials. Of course credentials 140 are not limited to these examples and may include other types of credentials now known or later developed.” Cross at 3:51-58. “In an exemplary implementation, local credentials 140 may be synchronized with remote credentials 150 provided at a remote cache 125, e.g., at one or more hosts 120 or a shared cache at another client 130 in a workgroup environment. Accordingly, the user has available a current and complete set of credentials when the user logs onto other clients 130. Remote cache 125 may be implemented as a directory service, such as a

'619 Patent – Claim 33	Cross
	distributed lightweight directory access protocol (LDAP) or X.500 directory service. The directory service may be monolithic, or it may be distributed as a multi-master implementation or master-slave implementation. Remote cache 125 may stored in a protected or encrypted state so that the remote credentials 150 are not exposed to compromise, theft, or exploit by unauthorized users." Cross at 4:4-19. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

'619 Patent – Claim 36	Cross
[36] The device of claim 22, wherein a control message is received from the remote device upon user interaction with the message.	Cross discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22pre]-[22h], *above*. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

’619 Patent – Claim 37	Cross
[37pre] 37. A method for sharing a messaging account, the method comprising:	To the extent the preamble is limiting, Cross discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:  Fig. 1 Cross, Fig. 1.

’619 Patent – Claim 37	Cross
	 Cross Fig. 7. “FIG. 1 is a schematic illustration of an exemplary networked computing system 100 in which credential roaming may be implemented. The networked computer system 100 may include one or more communication networks 110, such as local area network (LAN) and/or wide area network (WAN). One or more hosts 120 and one or more clients 130 a-c may be communicatively coupled over the communication network(s) 110. Host 120 and clients 130 a-c (hereinafter generally referred to as clients 130) may connect to a network via a communication connection such as, e.g., an Ethernet connection. Although there are no theoretical limits on the number of devices that can be included in a network such as networked computing system 100, the number of devices are limited primarily by the connectivity implemented in the communication network. The terms “host” and “client” both refer to the hardware and software (the entire computer system) used to perform various computing services. For

'619 Patent – Claim 37	Cross
	example, a host may be implemented as a server computer that is dedicated to server applications or that also runs other applications. A client may be implemented as a stand-alone desktop or laptop personal computer (PC), workstation, personal digital assistant (PDA), or any of a wide variety of electronic appliances, to name only a few examples." Cross at 3:13-37. "Described herein are exemplary methods for implementing encryption credential roaming. The methods described herein may be embodied as logic instructions on one or more computer-readable medium. When executed on a processor, the logic instructions cause a general purpose computing device to be programmed as a special-purpose machine that implements the described methods. In the following exemplary operations, the components and connections depicted in the figures may be used to implement encryption credential roaming." Cross at 7:58-67. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[37a] authenticating a device for access to the messaging account;	Cross discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22h], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person

’619 Patent – Claim 37	Cross
	of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[37b] optically receiving information including a displayed service activation code from a remote device;	Cross discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22c], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[37c] registering the remote device for access to the messaging account using the service activation code;	Cross discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22d], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

’619 Patent – Claim 37	Cross
[37d] receiving a message for the messaging account;	Cross discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22e], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[37e] encrypting the message using an encryption key; and	Cross discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22f], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[37f] sending the message to the remote device.	Cross discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22g], above. Furthermore, this claim element is obvious in light of this reference itself, when

'619 Patent – Claim 37	Cross
	combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

'619 Patent – Claim 38	Cross
[38] The method of claim 37, wherein the information including the service activation code is received by the device in response to user input at the remote device.	Cross discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [23], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

'619 Patent – Claim 39	Cross
[39] The method of claim 38, wherein the information including the service activation code is received by the device in an off-line	Cross discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:

'619 Patent – Claim 39	Cross
communication.	*See* [24], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

'619 Patent – Claim 40	Cross
[40] The method of claim 39, wherein the off-line communication prevents eavesdropping of the service activation code.	Cross discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [26], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

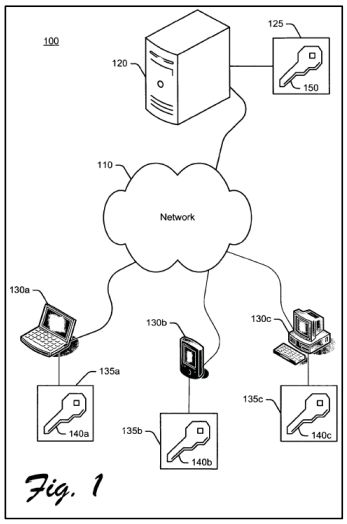
'619 Patent – Claim 41	Cross
[41] The method of claim 37, wherein the authentication of the device relies on the	Cross discloses this claim limitation. For example, see the following passages

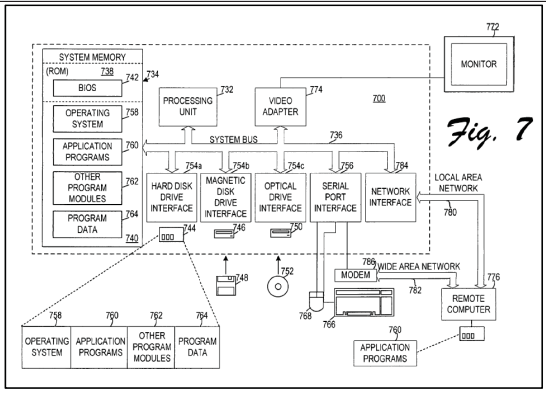
’619 Patent – Claim 41	Cross
authentication of the messaging system.	and/or figures, as well as all related disclosures: *See* [27], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

’619 Patent – Claim 42	Cross
[42] The method of claim 41, wherein the authentication of the messaging system includes a username and password.	Cross discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [28], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

’619 Patent – Claim 46	Cross
[46] The method of claim 37, wherein the encryption key is closely related to the service activation code.	Cross discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [32], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

’619 Patent – Claim 50	Cross
[50] The method of claim 37, wherein a control message is received from the remote device upon user interaction with the message.	Cross discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [36], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

’619 Patent – Claim 51	Cross
[51pre] 51. A non-transient computer-readable medium containing program instructions for causing a device to perform a method, the method comprising:	To the extent the preamble is limiting, Cross discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:  Cross, Fig. 1.

’619 Patent – Claim 51	Cross
	 *Fig. 7* Cross Fig. 7. “FIG. 1 is a schematic illustration of an exemplary networked computing system 100 in which credential roaming may be implemented. The networked computer system 100 may include one or more communication networks 110, such as local area network (LAN) and/or wide area network (WAN). One or more hosts 120 and one or more clients 130 a-c may be communicatively coupled over the communication network(s) 110. Host 120 and clients 130 a-c (hereinafter generally referred to as clients 130) may connect to a network via a communication connection such as, e.g., an Ethernet connection. Although there are no theoretical limits on the number of devices that can be included in a network such as networked computing system 100, the number of devices are limited primarily by the connectivity implemented in the communication network. The terms “host” and “client” both refer to the hardware and software (the entire computer system) used to perform various computing services. For

’619 Patent – Claim 51	Cross
	example, a host may be implemented as a server computer that is dedicated to server applications or that also runs other applications. A client may be implemented as a stand-alone desktop or laptop personal computer (PC), workstation, personal digital assistant (PDA), or any of a wide variety of electronic appliances, to name only a few examples.” Cross at 3:13-37. “Described herein are exemplary methods for implementing encryption credential roaming. The methods described herein may be embodied as logic instructions on one or more computer-readable medium. When executed on a processor, the logic instructions cause a general purpose computing device to be programmed as a special-purpose machine that implements the described methods. In the following exemplary operations, the components and connections depicted in the figures may be used to implement encryption credential roaming.” Cross at 7:58-67. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[51a] optically receiving information including a displayed service activation code from a remote device;	Cross discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22c], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person

'619 Patent – Claim 51	Cross
	of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[51b] registering the remote device for access to a messaging account using the service activation code;	Cross discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22d], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[51c] receiving a message for the messaging account;	Cross discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22e], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

'619 Patent – Claim 51	Cross
[51d] encrypting the message using an encryption key; and	Cross discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22f], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[51e] sending the message to the remote device,	Cross discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22g], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[51f] wherein the device is authenticated to access the messaging account.	Cross discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22h], above. Furthermore, this claim element is obvious in light of this reference itself, when

’619 Patent – Claim 51	Cross
	combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

’619 Patent – Claim 52	Cross
[52] The method of claim 51, wherein a control message is received from the remote device upon user interaction with the message.	Cross discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [36], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

EXHIBIT 619-A03

Invalidity Contentions for U.S. Patent No. 10,027,619 ("the '619 patent")

Based on: U.S. Patent No. 7,603,556 to Brown et al. ("Brown")

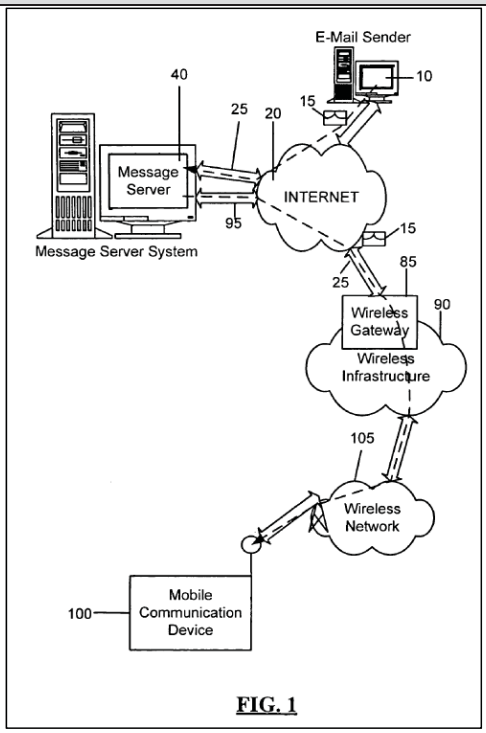
Based on SEVEN's apparent positions as to the scope of the patent's claims, as best they can be deciphered, the reference(s) charted below anticipate(s) or at least render(s) obvious the identified claims. The portions of the prior art reference cited below are not exhaustive but are exemplary in nature. Where Apple identifies a portion of the prior art reference's text, the identification should be understood as referencing any corresponding figure or diagram, and vice versa.

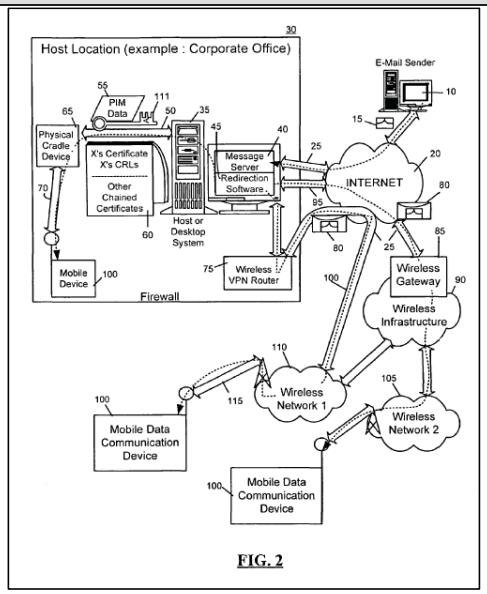
This disclosure is not an admission that Apple concedes any claim construction implied or suggested by SEVEN's apparent positions as to the scope of the patent's claims, nor is it an admission by Apple that any of its products are covered by or infringe the patent's claims, particularly when they are properly construed and applied. Apple is not taking any claim construction positions through this disclosure, including whether the preamble is a limitation.

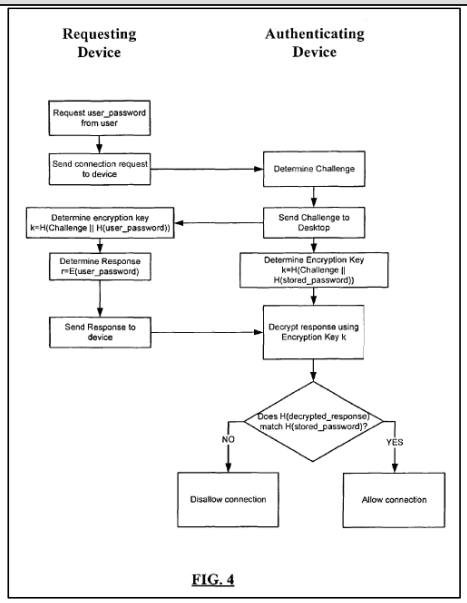
Apple reserves the right to rely on additional citations or sources of evidence that also may be applicable, or that may become applicable in light of claim construction, changes in SEVEN's infringement contentions, and/or information obtained during discovery as the case progresses. Apple further reserves the right to amend or supplement this claim chart at a later date as more fully set forth in the Invalidity Contentions.

Brown qualifies as prior art under at least pre-AIA 35 U.S.C. §§ 102(a) and/or (e). Brown is a U.S. Patent that was filed on November 26, 2004, published on November 10, 2005, and issued on October 13, 2009.

'619 Patent – Claim 22	Brown
[22pre] A device comprising:	To the extent the preamble is limiting, Brown discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:

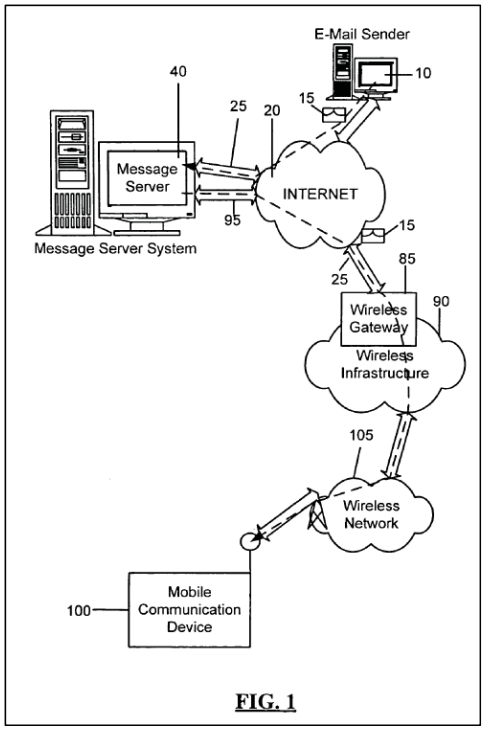
’619 Patent – Claim 22	Brown
	 FIG. 1 Brown, Fig. 1.

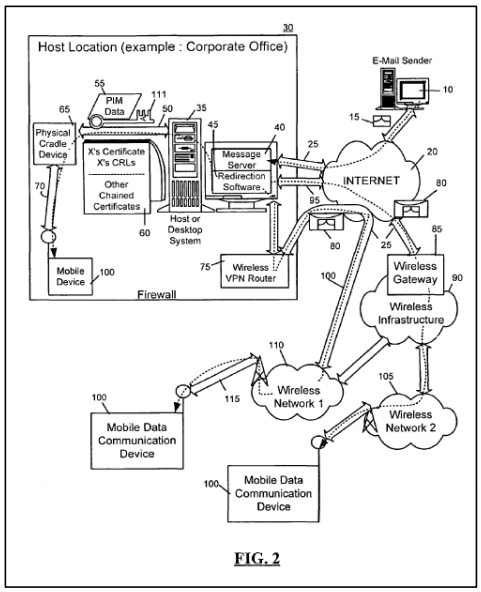
’619 Patent – Claim 22	Brown
	 Brown, Fig. 2.

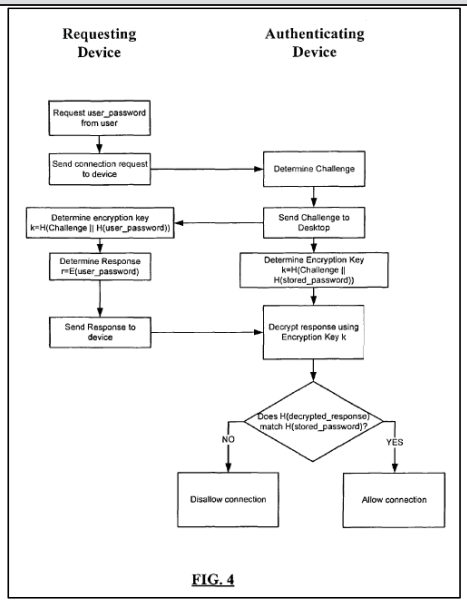
’619 Patent – Claim 22	Brown
	 FIG. 4 Brown, Fig. 4. “A challenge response scheme authenticates a requesting device by an authenticating device. The authenticating device generates and issues a challenge to the requesting device. The requesting device combines the challenge with a hash of a password provided by a user, and the combination is further hashed in order to generate a requesting encryption key used to encrypt the user supplied password. The encrypted user supplied password is sent to the authenticating device as a response to the issued challenge. The authenticating device generates an authenticating encryption key by generating the hash of a

’619 Patent – Claim 22	Brown
	combination of the challenge and a stored hash of an authenticating device password. The authenticating encryption key is used to decrypt the response in order to retrieve the user-supplied password. If the user-supplied password hash matches the stored authenticating device password hash, the requesting device is authenticated and the authenticating device is in possession of the password.” Brown at ABSTRACT. “FIG. 1 is an overview of an example communication system in which a wireless communication device may be used. One skilled in the art will appreciate that there may be hundreds of different topologies, but the system shown in FIG. 1 helps demonstrate the operation of the encoded message processing systems and methods described in the present application. There may also be many message senders and recipients. The simple system shown in FIG. 1 is for illustrative purposes only, and shows perhaps the most prevalent Internet e-mail environment where security is not generally used. FIG. 1 shows an e-mail sender 10, the Internet 20, a message server system 40, a wireless gateway 85, wireless infrastructure 90, a wireless network 105 and a mobile communication device 100.” Brown at 4:49-62. “FIG. 2 is a block diagram of a further example communication system including multiple networks and multiple mobile communication devices. The system of FIG. 2 is substantially similar to the FIG. 1 system, but includes a host system 30 , a redirection program 45, a mobile device cradle 65, a wireless virtual private network (VPN) router 75, an additional wireless network 110 and multiple mobile communication devices 100. As described above in conjunction with FIG. 1, FIG. 2 represents an overview of a sample network topology. Although the encoded message processing systems and methods described herein may be applied to networks having many different topologies, the network of FIG. 2 is useful in understanding an automatic e-mail redirection system mentioned briefly above.” Brown at 6:15-27. “The central host system 30 will typically be a corporate office or other LAN,

’619 Patent – Claim 22	Brown
	but may instead be a home office computer or some other private system where mail messages are being exchanged. Within the host system 30 is the message server 40, running on some computer within the firewall of the host system, that acts as the main interface for the host system to exchange e-mail with the Internet 20. In the system of FIG. 2, the redirection program 45 enables redirection of data items from the server 40 to a mobile communication device 100. Although the redirection program 45 is shown to reside on the same machine as the message server 40 for ease of presentation, there is no requirement that it must reside on the message server. The redirection program 45 and the message server 40 are designed to co-operate and interact to allow the pushing of information to mobile devices 100. In this installation, the redirection program 45 takes confidential and non-confidential corporate information for a specific user and redirects it out through the corporate firewall to mobile devices 100.” Brown at 6:29-47. “As another example, the systems and methods disclosed herein may be used with many different computers and devices, such as a wireless mobile communications device shown in FIG. 5. With reference to FIG. 5, the mobile device 100 is a dual-mode mobile device and includes a transceiver 311, a microprocessor 338, a display 322, non-volatile memory 324, random access memory (RAM) 326, one or more auxiliary input/output (I/O) devices 328, a serial port 330, a keyboard 332, a speaker 334, a microphone 336, a short-range wireless communications sub-system 340, and other device sub-systems 342.” Brown at 9:46-56. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and

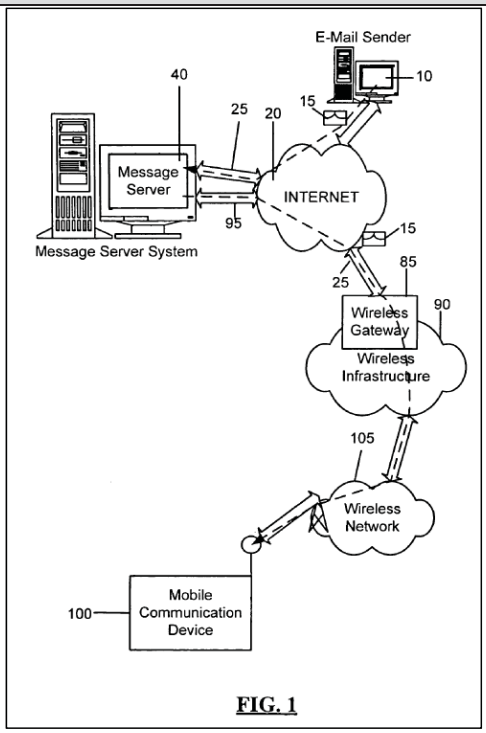
’619 Patent – Claim 22	Brown
	Exhibit 619-B.
[22a] a radio;	Brown discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:  FIG. 1

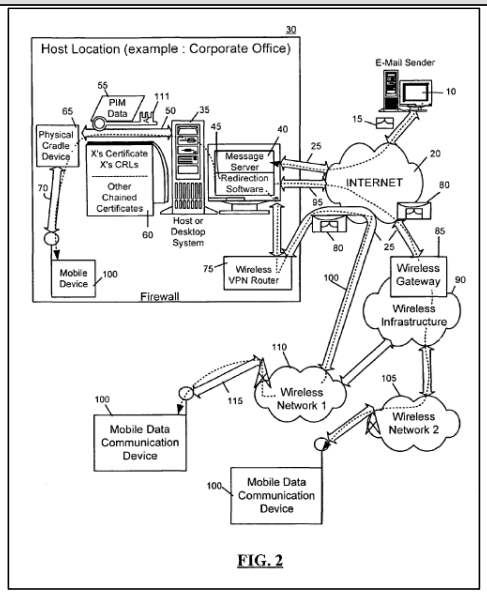
’619 Patent – Claim 22	Brown
	Brown, Fig. 1.  Brown, Fig. 2.

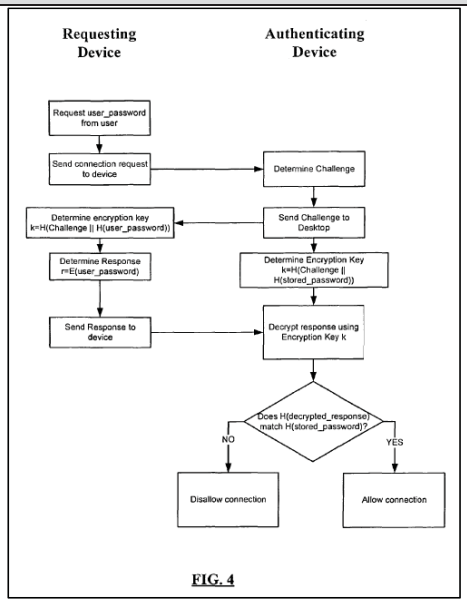
’619 Patent – Claim 22	Brown
	 FIG. 4 Brown, Fig. 4. “The wireless gateway 85 and infrastructure 90 provide a link between the Internet 20 and wireless network 105. The wireless infrastructure 90 determines the most likely network for locating a given user and tracks the user as they roam between countries or networks. A message is then delivered to the mobile device 100 via wireless transmission, typically at a radio frequency (RF), from a base station in the wireless network 105 to the mobile device 100. The particular network 105 may be virtually any wireless network over which messages may be exchanged with a mobile communication device.” Brown at

’619 Patent – Claim 22	Brown
	5:26-36. “With reference to FIG. 5, the mobile device 100 is a dual-mode mobile device and includes a transceiver 311, a microprocessor 338, a display 322, non-volatile memory 324, random access memory (RAM) 326, one or more auxiliary input/output (I/O) devices 328, a serial port 330, a keyboard 332, a speaker 334, a microphone 336, a short-range wireless communications sub-system 340, and other device sub-systems 342. The transceiver 311 includes a receiver 312, a transmitter 314, antennas 316 and 318, one or more local oscillators 313, and a digital signal processor (DSP) 320. The antennas 316 and 318 may be antenna elements of a multiple-element antenna, and are preferably embedded antennas. However, the systems and methods described herein are in no way restricted to a particular type of antenna, or even to wireless communication devices.” Brown at 9:49-64. “Regardless of the specific mechanism controlling the forwarding of messages to the mobile device 100, the message 15, or possibly a translated or reformatted version thereof, is sent to the wireless gateway 85. The wireless infrastructure 90 includes a series of connections to wireless network 105. These connections could be Integrated Services Digital Network (ISDN), Frame Relay or T1 connections using the TCP/IP protocol used throughout the Internet. As used herein, the term “wireless network” is intended to include three different types of networks, those being (1) data-centric wireless networks, (2) voice-centric wireless networks and (3) dual-mode networks that can support both voice and data communications over the same physical base stations. Combined dual-mode networks include, but are not limited to, (1) Code Division Multiple Access (CDMA) networks, (2) the Groupe Special Mobile or the Global System for Mobile Communications (GSM) and the General Packet Radio Service (GPRS) networks, and (3) future third-generation (3G) networks like Enhanced Data-rates for Global Evolution (EDGE) and Universal Mobile Telecommunications Systems (UMTS). Some older examples of data-centric network include the Mobitex™ Radio Network

’619 Patent – Claim 22	Brown
	and the DataTAC™ Radio Network. Examples of older voice-centric data networks include Personal Communication Systems (PCS) networks like GSM, and TDMA systems.” Brown at 5:57-6:14. “A short-range communications subsystem 340 is also included in the mobile device 100. The subsystem 340 may include an infrared device and associated circuits and components, or a short-range RF communication module such as a BLUETOOTH® module or an 802.11 module, for example, to provide for communication with similarly-enabled systems and devices. Those skilled in the art will appreciate that “BLUETOOTH” and “802.11” refer to sets of specifications, available from the Institute of Electrical and Electronics Engineers, relating to wireless personal area networks and wireless local area networks, respectively.” Brown at 13:43-54. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[22b] a processor and memory containing instructions executable by the processor whereby the device is operable to:	Brown discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:

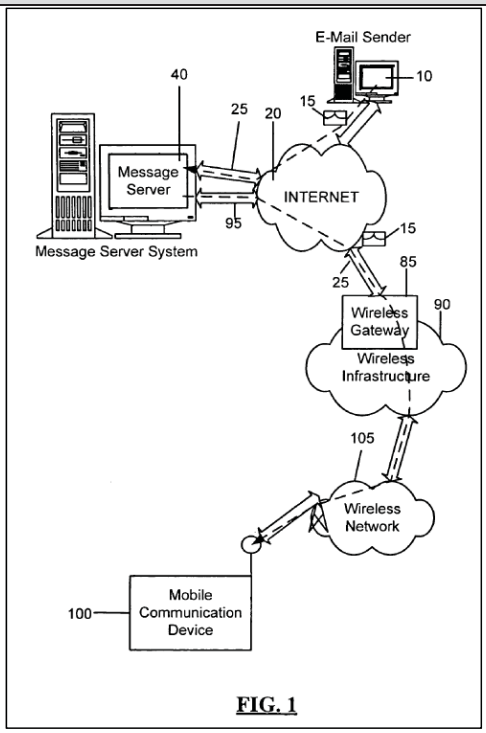
’619 Patent – Claim 22	Brown
	 FIG. 1 Brown, Fig. 1.

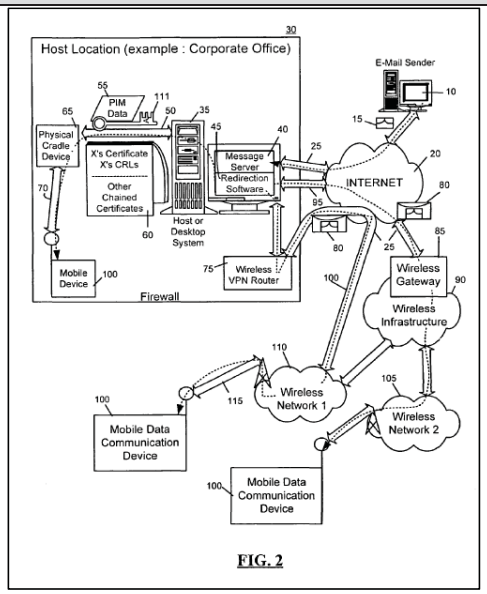
’619 Patent – Claim 22	Brown
	 Brown, Fig. 2.

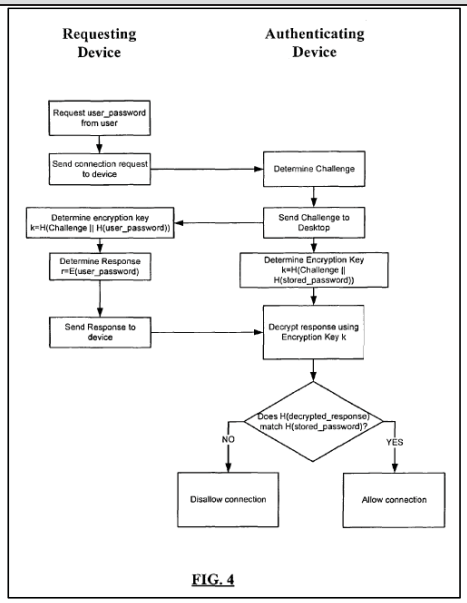
’619 Patent – Claim 22	Brown
	 FIG. 4 Brown, Fig. 4. “The systems' and methods' data may be stored in one or more data stores. The data stores can be of many different types of storage devices and programming constructs, such as RAM, ROM, Flash memory, programming data structures, programming variables, etc. It is noted that data structures describe formats for use in organizing and storing data in databases, programs, memory, or other computer-readable media for use by a computer program. The systems and methods may be provided on many different types of

’619 Patent – Claim 22	Brown
	computer-readable media including computer storage mechanisms (e.g., CD-ROM, diskette, RAM, flash memory, computer's hard drive, etc.) that contain instructions for use in execution by a processor to perform the methods' operations and implement the systems described herein. The computer components, software modules, functions and data structures described herein may be connected directly or indirectly to each other in order to allow the flow of data needed for their operations. It is also noted that a module or processor includes but is not limited to a unit of code that performs a software operation, and can be implemented for example as a subroutine unit of code, or as a software function unit of code, or as an object (as in an object-oriented paradigm), or as an applet, or in a computer script language, or as another type of computer code.” Brown at 13:55-14:13. “The central host system 30 will typically be a corporate office or other LAN, but may instead be a home office computer or some other private system where mail messages are being exchanged. Within the host system 30 is the message server 40, running on some computer within the firewall of the host system, that acts as the main interface for the host system to exchange e-mail with the Internet 20. In the system of FIG. 2, the redirection program 45 enables redirection of data items from the server 40 to a mobile communication device 100. Although the redirection program 45 is shown to reside on the same machine as the message server 40 for ease of presentation, there is no requirement that it must reside on the message server. The redirection program 45 and the message server 40 are designed to co-operate and interact to allow the pushing of information to mobile devices 100. In this installation, the redirection program 45 takes confidential and non-confidential corporate information for a specific user and redirects it out through the corporate firewall to mobile devices 100.” Brown at 6:29-47. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in

’619 Patent – Claim 22	Brown
	Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[22c] optically receive information including a displayed service activation code from a remote device;	Brown discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:

’619 Patent – Claim 22	Brown
	 FIG. 1 Brown, Fig. 1.

’619 Patent – Claim 22	Brown
	 FIG. 2 Brown, Fig. 2.

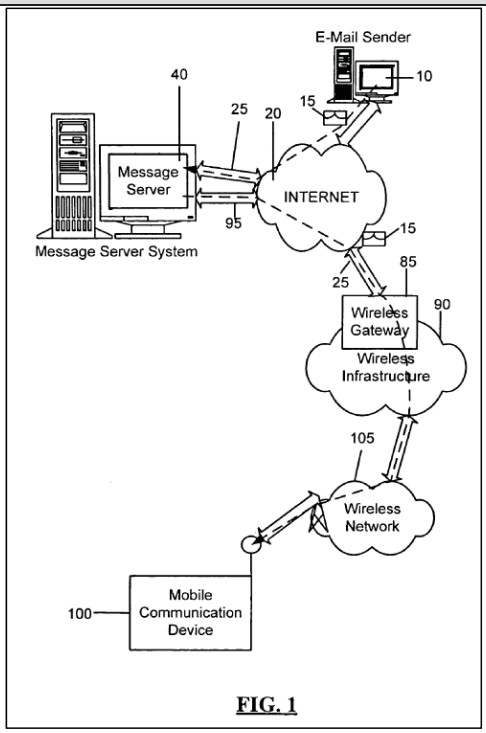
’619 Patent – Claim 22	Brown
	 FIG. 4 Brown, Fig. 4. “A challenge response scheme authenticates a requesting device by an authenticating device. The authenticating device generates and issues a challenge to the requesting device. The requesting device combines the challenge with a hash of a password provided by a user, and the combination is further hashed in order to generate a requesting encryption key used to encrypt the user supplied password. The encrypted user supplied password is sent to the authenticating device as a response to the issued challenge. The authenticating device generates an authenticating encryption key by generating the hash of a

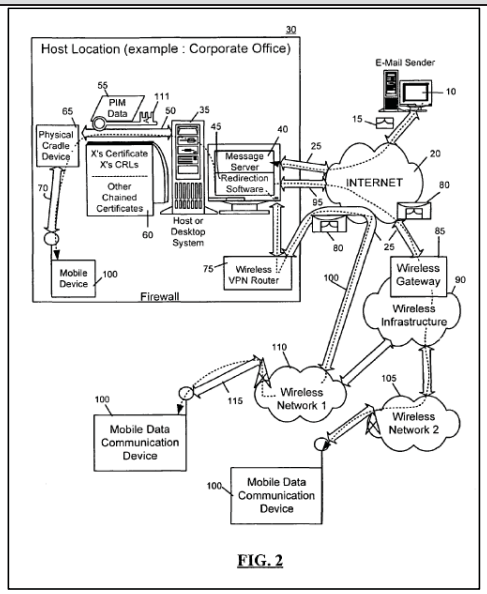
’619 Patent – Claim 22	Brown
	combination of the challenge and a stored hash of an authenticating device password. The authenticating encryption key is used to decrypt the response in order to retrieve the user-supplied password. If the user-supplied password hash matches the stored authenticating device password hash, the requesting device is authenticated and the authenticating device is in possession of the password.” Brown at ABSTRACT; Brown at SUMMARY. “FIG. 4 illustrates a challenge response scheme in accordance with a preferred embodiment of the present invention. In the preferred embodiment, a requesting device, such as the desktop system 35, is connected to an authenticating device, such as mobile device 10, using a communications link, such as a universal serial bus (USB) link, through which the requesting device may send a connection request. The connection request may be in the form of a software request sent to the authenticating device, or the detection of a change in a hardware state of the communications link. The authenticating device detects that a connection is being requested, and proceeds to authenticate the requesting device in accordance with the challenge response scheme described below. It will be understood that the authenticating device may only initiate the challenge response scheme if the authenticating device has been secured by a device password (stored_password). In order to determine if a requesting device needs to be authenticated, the authenticating device may check for the presence of a hash of the device password H(stored_password) in a memory of the authenticating device. In other implementations, the authentication device may check for a flag indicating whether the device has been secured. When the authenticating device detects a connection request, it generates a Challenge c to issue to the requesting device. The Challenge c may be a group of bits that have been randomly generated by the authenticating device. Alternatively, the numbers of bits used in the Challenge c may also be randomized. The authenticating device may use a hardware-based random number generator or a software-based random number generator to generate the

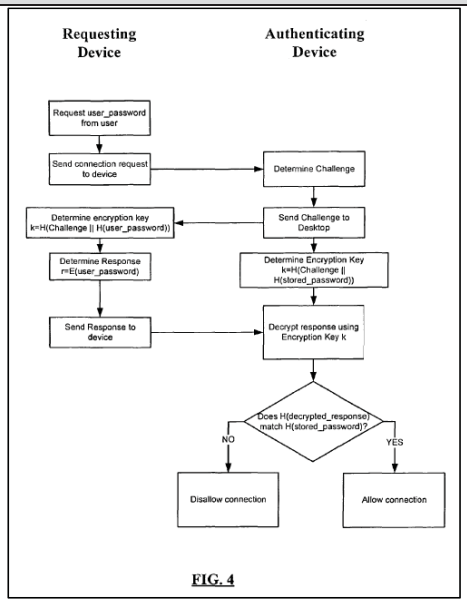
’619 Patent – Claim 22	Brown
	random Challenge c. The requesting device prompts the user of the requesting device for a password user_password. This password is hashed, using known hashing functions such as SHA-1, to create H(user_password) which is then combined with the Challenge c received from the authenticating device. In the preferred embodiment, the Challenge c and the hash of the password H(user_password) are concatenated together. It is understood that there are different ways in which to combine the two values. This combination of the Challenge c and the hash of the password H(user_password) is further hashed in order to generate a requesting encryption key kr=H(c‖H(user_password)) that is used in creating a response r to the challenge issued by the authenticating device. The response r is generated by encrypting the password user_password using known techniques such as AES or TripleDES. In some implementations, the response r may also be generated by applying the XOR function to the requesting encryption key kr and the password user_password. The response r is then transmitted to the authenticating device. The authenticating device determines an authenticating encryption key ka by following a process similar to that followed by the requesting device. The authenticating device combines the stored hash of the device password H(stored_password) with the randomly generated Challenge c, and then generates a hash of the combination, in order to generate the authenticating encryption key ka=H(c‖H(stored_password)). The authenticating encryption key ka is used to decrypt the response r received from the requesting device. A hash of the decrypted response H(decrypted_response) is then compared to the stored hash of the device password H(stored_password). If the two hashes match, then the decrypted response was the correct device password. Thus the authenticating device has authenticated the requesting device. The authenticating device is also in possession of the device password for use in operations that require the device password. If the two hashes do not match, then the user did not provide the correct password, and the authenticating

’619 Patent – Claim 22	Brown
	device rejects the connection request from the requesting device, and thereby disallows the connection. In a further embodiment, the device password is concatenated with a random salt s, then hashed and stored in the memory of the authenticating device together with s. Therefore the authenticating device stores (s, H(s‖stored_password)). When the challenge c is transmitted to the requesting device, the salt s is likewise transmitted, and the requesting device then hashes a concatenation of s and user_password to generate an authenticating encrypting key kr=H(c‖H(s‖user_password)) using the process described above. Once the response r is transmitted to the authenticating device, the authenticating device determines an authenticating encryption key ka=H(c‖H(s‖stored_password)) by following a process similar to that described above. The authenticating encryption key ka is used to decrypt the response r received from the requesting device. A hash of the decrypted response H(decrypted_response) is then compared to the stored hash of the salted device password H(s‖stored_password). If the two hashes match, then the decrypted response was the correct device password.” Brown at 8:16-9:18. “The mobile device 100 may be manually synchronized with a host system by placing the device 100 in an interface cradle, which couples the serial port 330 of the mobile device 100 to the serial port of a computer system or device. The serial port 330 may also be used to enable a user to set preferences through an external device or software application, or to download other application modules 324N for installation. This wired download path may be used to load an encryption key onto the device, which is a more secure method than exchanging encryption information via the wireless network 319. Interfaces for other wired download paths may be provided in the mobile device 100, in addition to or instead of the serial port 330. For example, a USB port would provide an interface to a similarly equipped personal computer.” Brown at 12:46-61.

’619 Patent – Claim 22	Brown
	“A short-range communications subsystem 340 is also included in the mobile device 100. The subsystem 340 may include an infrared device and associated circuits and components, or a short-range RF communication module such as a BLUETOOTH® module or an 802.11 module, for example, to provide for communication with similarly-enabled systems and devices. Those skilled in the art will appreciate that "BLUETOOTH" and "802.11" refer to sets of specifications, available from the Institute of Electrical and Electronics Engineers, relating to wireless personal area networks and wireless local area networks, respectively.” Brown at 13:43-54. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[22d] register the remote device for access to a messaging account using the service activation code;	Brown discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:

’619 Patent – Claim 22	Brown
	 FIG. 1 Brown, Fig. 1.

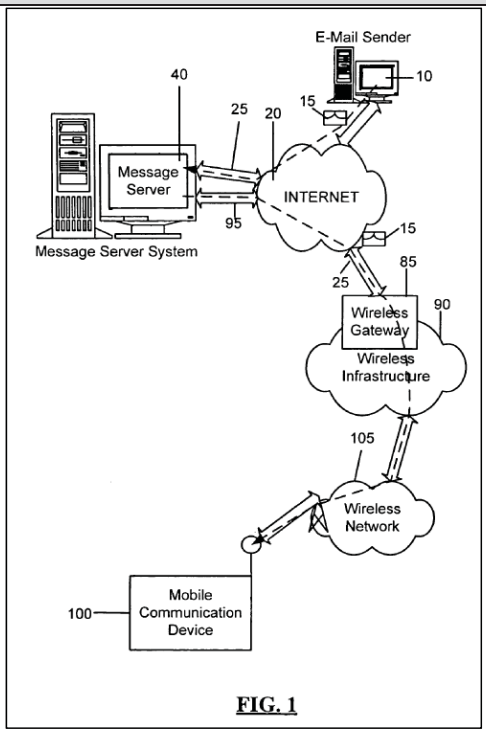
’619 Patent – Claim 22	Brown
	 FIG. 2 Brown, Fig. 2.

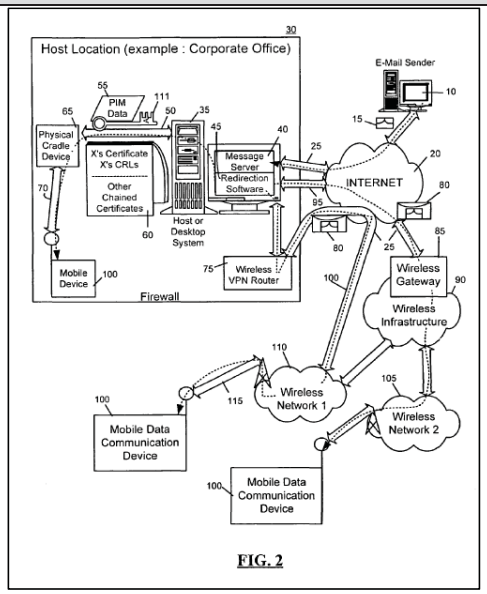
’619 Patent – Claim 22	Brown
	 FIG. 4 Brown, Fig. 4. “The message server 40 may be implemented, for example, on a network computer within the firewall of a corporation, a computer within an ISP or ASP system or the like, and acts as the main interface for e-mail exchange over the Internet 20. Although other messaging systems might not require a message server system 40, a mobile device 100 configured for receiving and possibly sending e-mail will normally be associated with an account on a message server. Perhaps the two most common message servers are MICROSOFT® EXCHANGE and LOTUS DOMINO®. These products are often used in

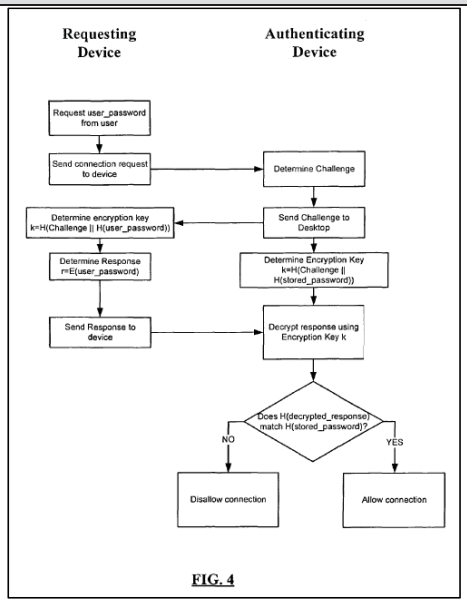
’619 Patent – Claim 22	Brown
	conjunction with Internet mail routers that route and deliver mail. These intermediate components are not shown in FIG. 1, as they do not directly play a role in the secure message processing described below. Message servers such as server 40 typically extend beyond just e-mail sending and receiving; they also include dynamic database storage engines that have predefined database formats for data like calendars, to-do lists, task lists, e-mail and documentation.” Brown at 5:8-25. “As shown in FIG. 1, a composed e-mail message 15 is sent by the e-mail sender 10, located somewhere on the Internet 20. This message 15 is normally fully in the clear and uses traditional Simple Mail Transfer Protocol (SMTP), RFC822 headers and Multipurpose Internet Mail Extension (MIME) body parts to define the format of the mail message. These techniques are all well known to those skilled in the art. The message 15 arrives at the message server 40 and is normally stored in a message store. Most known messaging systems support a so-called “pull” message access scheme, wherein the mobile device 100 must request that stored messages be forwarded by the message server to the mobile device 100. Some systems provide for automatic routing of such messages which are addressed using a specific e-mail address associated with the mobile device 100. In a preferred embodiment described in further detail below, messages addressed to a message server account associated with a host system such as a home computer or office computer which belongs to the user of a mobile device 100 are redirected from the message server 40 to the mobile device 100 as they are received.” Brown at 5:37-56. “In the automatic redirection system of FIG. 2, a composed e-mail message 15 leaving the e-mail sender 10 arrives at the message server 40 and is redirected by the redirection program 45 to the mobile device 100. As this redirection takes place the message 15 is re-enveloped, as indicated at 80, and a possibly proprietary compression and encryption algorithm can then be applied to the original message 15. In this way, messages being read on the mobile device 100 are no less secure than if they were read on a desktop workstation such as

’619 Patent – Claim 22	Brown
	35 within the firewall. All messages exchanged between the redirection program 45 and the mobile device 100 preferably use this message repackaging technique. Another goal of this outer envelope is to maintain the addressing information of the original message except the sender's and the receiver's address. This allows reply messages to reach the appropriate destination, and also allows the “from” field to reflect the mobile user's desktop address. Using the user's e-mail address from the mobile device 100 allows the received message to appear as though the message originated from the user's desktop system 35 rather than the mobile device 100.” Brown at 7:24-43. “After any required network registration or activation procedures have been completed, the mobile device 100 may the send and receive communication signals, including both voice and data signals, over the networks 319. Signals received by the antenna 316 from the communication network 319 are routed to the receiver 312, which provides for signal amplification, frequency down conversion, filtering, channel selection, etc., and may also provide analog to digital conversion. Analog to digital conversion of the received signal allows more complex communication functions, such as digital demodulation and decoding to be performed using the DSP 320. In a similar manner, signals to be transmitted to the network 319 are processed, including modulation and encoding, for example, by the DSP 320 and are then provided to the transmitter 314 for digital to analog conversion, frequency up conversion, filtering, amplification and transmission to the communication network 319 via the antenna 318.” Brown 10:55-11:4. “The non-volatile memory 324 preferably also provides a file system to facilitate storage of PIM data items on the device. The PIM application preferably includes the ability to send and receive data items, either by itself, or in conjunction with the voice and data communication modules 324A, 324B, via the wireless networks 319. The PIM data items are preferably seamlessly integrated, synchronized and updated, via the wireless networks 319, with a corresponding set of data items stored or associated with a host computer

’619 Patent – Claim 22	Brown
	system, thereby creating a mirrored system for data items associated with a particular user.” Brown at 12:19-29. “The mobile device 100 may be manually synchronized with a host system by placing the device 100 in an interface cradle, which couples the serial port 330 of the mobile device 100 to the serial port of a computer system or device. The serial port 330 may also be used to enable a user to set preferences through an external device or software application, or to download other application modules 324N for installation. This wired download path may be used to load an encryption key onto the device, which is a more secure method than exchanging encryption information via the wireless network 319. Interfaces for other wired download paths may be provided in the mobile device 100, in addition to or instead of the serial port 330. For example, a USB port would provide an interface to a similarly equipped personal computer.” Brown at 12:46-61. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[22e] receive a message for the messaging account;	Brown discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:

’619 Patent – Claim 22	Brown
	 FIG. 1 Brown, Fig. 1.

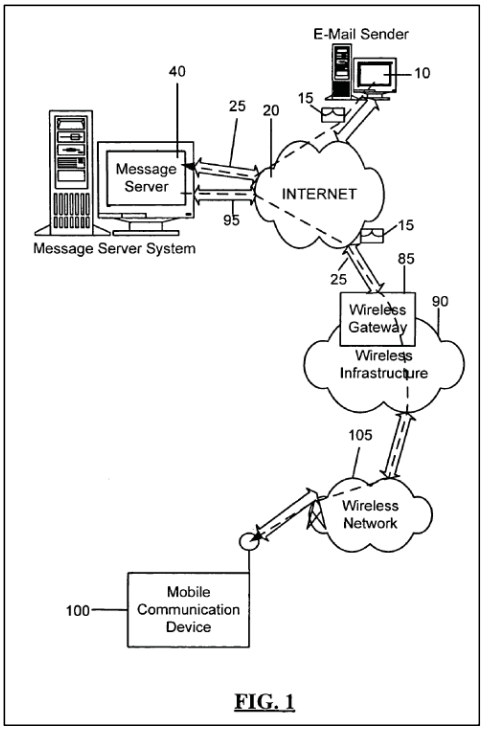
’619 Patent – Claim 22	Brown
	 Brown, Fig. 2.

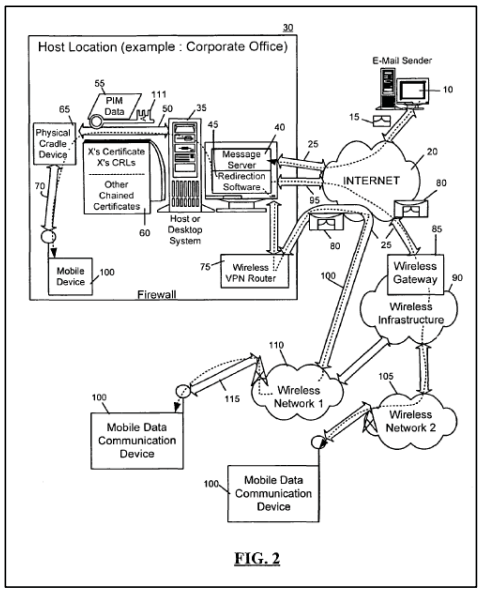
’619 Patent – Claim 22	Brown
	 FIG. 4 Brown, Fig. 4. “The message server 40 may be implemented, for example, on a network computer within the firewall of a corporation, a computer within an ISP or ASP system or the like, and acts as the main interface for e-mail exchange over the Internet 20. Although other messaging systems might not require a message server system 40, a mobile device 100 configured for receiving and possibly sending e-mail will normally be associated with an account on a message server. Perhaps the two most common message servers are MICROSOFT® EXCHANGE and LOTUS DOMINO®. These products are often used in

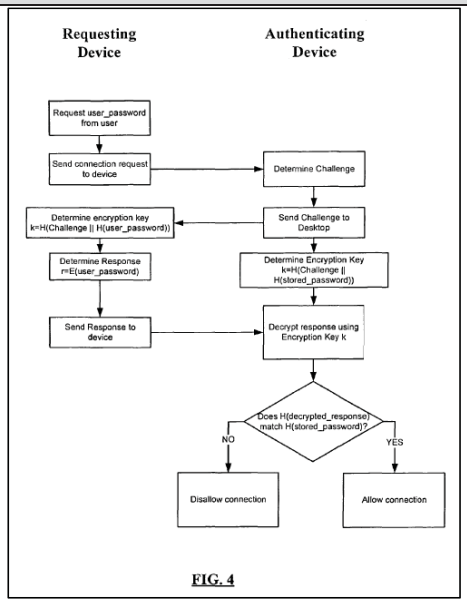
’619 Patent – Claim 22	Brown
	conjunction with Internet mail routers that route and deliver mail. These intermediate components are not shown in FIG. 1, as they do not directly play a role in the secure message processing described below. Message servers such as server 40 typically extend beyond just e-mail sending and receiving; they also include dynamic database storage engines that have predefined database formats for data like calendars, to-do lists, task lists, e-mail and documentation. The wireless gateway 85 and infrastructure 90 provide a link between the Internet 20 and wireless network 105. The wireless infrastructure 90 determines the most likely network for locating a given user and tracks the user as they roam between countries or networks. A message is then delivered to the mobile device 100 via wireless transmission, typically at a radio frequency (RF), from a base station in the wireless network 105 to the mobile device 100. The particular network 105 may be virtually any wireless network over which messages may be exchanged with a mobile communication device.”) Brown 5:8-37. “As shown in FIG. 1, a composed e-mail message 15 is sent by the e-mail sender 10, located somewhere on the Internet 20. This message 15 is normally fully in the clear and uses traditional Simple Mail Transfer Protocol (SMTP), RFC822 headers and Multipurpose Internet Mail Extension (MIME) body parts to define the format of the mail message. These techniques are all well known to those skilled in the art. The message 15 arrives at the message server 40 and is normally stored in a message store. Most known messaging systems support a so-called “pull” message access scheme, wherein the mobile device 100 must request that stored messages be forwarded by the message server to the mobile device 100. Some systems provide for automatic routing of such messages which are addressed using a specific e-mail address associated with the mobile device 100. In a preferred embodiment described in further detail below, messages addressed to a message server account associated with a host system such as a home computer or office computer which belongs to the user of a mobile device 100 are redirected from the message server 40 to the mobile

’619 Patent – Claim 22	Brown
	device 100 as they are received.” Brown at 5:37-56. “The central host system 30 will typically be a corporate office or other LAN, but may instead be a home office computer or some other private system where mail messages are being exchanged. Within the host system 30 is the message server 40, running on some computer within the firewall of the host system, that acts as the main interface for the host system to exchange e-mail with the Internet 20. In the system of FIG. 2, the redirection program 45 enables redirection of data items from the server 40 to a mobile communication device 100. Although the redirection program 45 is shown to reside on the same machine as the message server 40 for ease of presentation, there is no requirement that it must reside on the message server. The redirection program 45 and the message server 40 are designed to co-operate and interact to allow the pushing of information to mobile devices 100. In this installation, the redirection program 45 takes confidential and non-confidential corporate information for a specific user and redirects it out through the corporate firewall to mobile devices 100.” Brown at 6:29-47. “One method for loading information onto the mobile device 100 is through a port designated 50, using a device cradle 65. This method tends to be useful for bulk information updates often performed at initialization of a mobile device 100 with the host system 30 or a computer 35 within the system 30.” Brown at 6:60-66. “In the automatic redirection system of FIG. 2, a composed e-mail message 15 leaving the e-mail sender 10 arrives at the message server 40 and is redirected by the redirection program 45 to the mobile device 100. As this redirection takes place the message 15 is re-enveloped, as indicated at 80, and a possibly proprietary compression and encryption algorithm can then be applied to the original message 15 . In this way, messages being read on the mobile device 100 are no less secure than if they were read on a desktop workstation such as 35 within the firewall. All messages exchanged between the redirection

’619 Patent – Claim 22	Brown
	program 45 and the mobile device 100 preferably use this message repackaging technique. Another goal of this outer envelope is to maintain the addressing information of the original message except the sender's and the receiver's address. This allows reply messages to reach the appropriate destination, and also allows the “from” field to reflect the mobile user's desktop address. Using the user's e-mail address from the mobile device 100 allows the received message to appear as though the message originated from the user's desktop system 35 rather than the mobile device 100.” Brown at 7:24-43. “When the mobile device 100 is operating in a data communication mode, a received signal, such as a text message or a web page download, is processed by the transceiver module 311 and provided to the microprocessor 338, which preferably further processes the received signal in multiple stages as described above, for eventual output to the display 322, or, alternatively, to an auxiliary I/O device 328. A user of mobile device 100 may also compose data items, such as e-mail messages, using the keyboard 332, which is preferably a complete alphanumeric keyboard laid out in the QWERTY style, although other styles of complete alphanumeric keyboards such as the known DVORAK style may also be used. User input to the mobile device 100 is further enhanced with a plurality of auxiliary I/O devices 328, which may include a thumbwheel input device, a touchpad, a variety of switches, a rocker input switch, etc. The composed data items input by the user may then be transmitted over the communication networks 319 via the transceiver module 311.” Brown at 13:8-26. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and

’619 Patent – Claim 22	Brown
	Exhibit 619-B.
[22f] encrypt the message using an encryption key; and	Brown discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:  FIG. 1

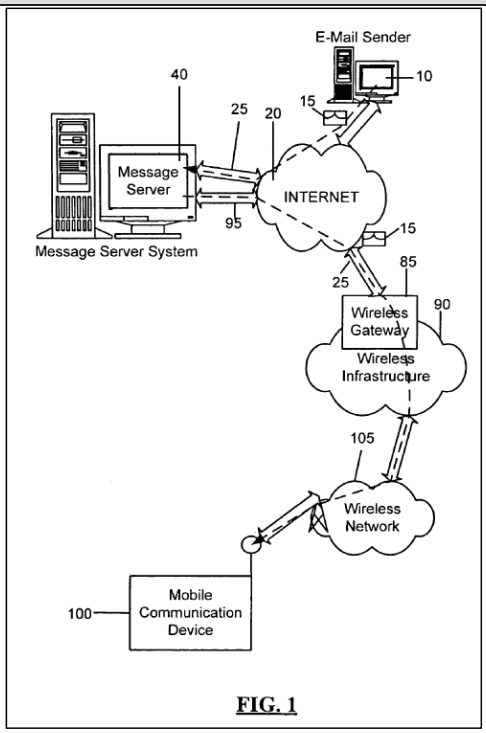
’619 Patent – Claim 22	Brown
	Brown, Fig. 1.  Brown, Fig. 2.

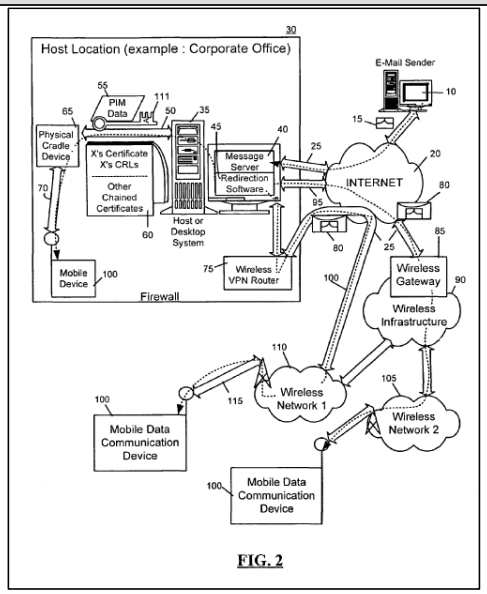
’619 Patent – Claim 22	Brown
	 FIG. 4 Brown, Fig. 4. “A challenge response scheme authenticates a requesting device by an authenticating device. The authenticating device generates and issues a challenge to the requesting device. The requesting device combines the challenge with a hash of a password provided by a user, and the combination is further hashed in order to generate a requesting encryption key used to encrypt the user supplied password. The encrypted user supplied password is sent to the authenticating device as a response to the issued challenge. The authenticating device generates an authenticating encryption key by generating the hash of a

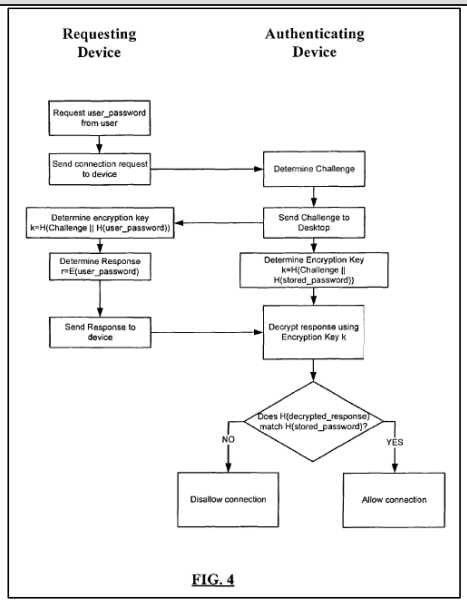
’619 Patent – Claim 22	Brown
	combination of the challenge and a stored hash of an authenticating device password. The authenticating encryption key is used to decrypt the response in order to retrieve the user-supplied password. If the user-supplied password hash matches the stored authenticating device password hash, the requesting device is authenticated and the authenticating device is in possession of the password.” Brown at Abstract. “The central host system 30 will typically be a corporate office or other LAN, but may instead be a home office computer or some other private system where mail messages are being exchanged. Within the host system 30 is the message server 40, running on some computer within the firewall of the host system, that acts as the main interface for the host system to exchange e-mail with the Internet 20. In the system of FIG. 2, the redirection program 45 enables redirection of data items from the server 40 to a mobile communication device 100. Although the redirection program 45 is shown to reside on the same machine as the message server 40 for ease of presentation, there is no requirement that it must reside on the message server. The redirection program 45 and the message server 40 are designed to co-operate and interact to allow the pushing of information to mobile devices 100. In this installation, the redirection program 45 takes confidential and non-confidential corporate information for a specific user and redirects it out through the corporate firewall to mobile devices 100. A more detailed description of the redirection software 45 may be found in the commonly assigned U.S. Pat. No. 6,219,694 (“the '694 Patent”), entitled “System and Method for Pushing Information From A Host System To A Mobile Data Communication Device Having A Shared Electronic Address”, and issued to the assignee of the instant application on Apr. 17, 2001,which is hereby incorporated into the present application by reference. This push technique may use a wireless friendly encoding, compression and encryption technique to deliver all information to a mobile device, thus effectively extending the security firewall to include each mobile device 100 associated with the host system 30.” Brown at 6:29-59.

’619 Patent – Claim 22	Brown
	“In the automatic redirection system of FIG. 2, a composed e-mail message 15 leaving the e-mail sender 10 arrives at the message server 40 and is redirected by the redirection program 45 to the mobile device 100. As this redirection takes place the message 15 is re-enveloped, as indicated at 80, and a possibly proprietary compression and encryption algorithm can then be applied to the original message 15 . In this way, messages being read on the mobile device 100 are no less secure than if they were read on a desktop workstation such as 35 within the firewall. All messages exchanged between the redirection program 45 and the mobile device 100 preferably use this message repackaging technique. Another goal of this outer envelope is to maintain the addressing information of the original message except the sender's and the receiver's address. This allows reply messages to reach the appropriate destination, and also allows the “from” field to reflect the mobile user's desktop address. Using the user's e-mail address from the mobile device 100 allows the received message to appear as though the message originated from the user's desktop system 35 rather than the mobile device 100. With reference back to the port 50 and cradle 65 connectivity to the mobile device 100, this connection path offers many advantages for enabling one-time data exchange of large items. For those skilled in the art of personal digital assistants (PDAs) and synchronization, the most common data exchanged over this link is Personal Information Management (PIM) data 55. When exchanged for the first time this data tends to be large in quantity, bulky in nature and requires a large bandwidth to get loaded onto the mobile device 100 where it can be used on the road. This serial link may also be used for other purposes, including setting up a private security key 111 such as an S/MIME or PGP specific private key, the Certificate (Cert) of the user and their Certificate Revocation Lists (CRLs) 60. The private key is preferably exchanged so that the desktop 35 and mobile device 100 share one personality and one method for accessing all mail. The Cert and CRLs are normally exchanged over such a link because they represent a large amount of the data that is required by the device

'619 Patent – Claim 22	Brown
	for S/MIME, PGP and other public key security methods. " Brown at 7:24-63. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[22g] send the message to the remote device,	Brown discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:

’619 Patent – Claim 22	Brown
	 FIG. 1 Brown, Fig. 1.

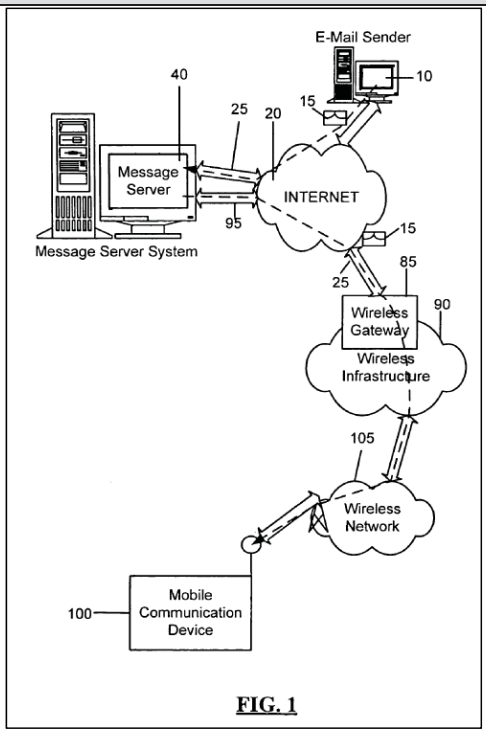
’619 Patent – Claim 22	Brown
	 FIG. 2 Brown, Fig. 2.

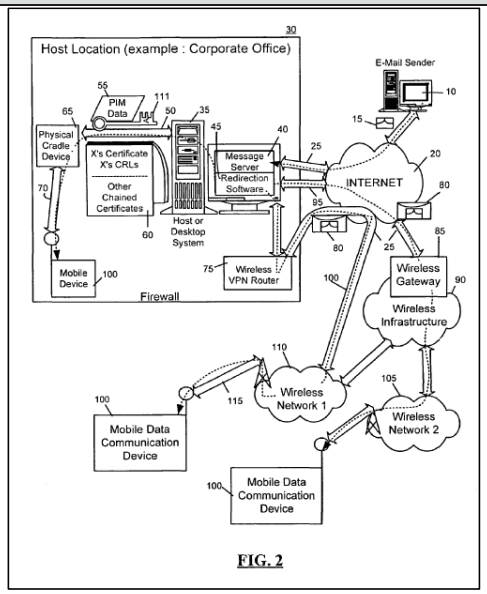
’619 Patent – Claim 22	Brown
	 FIG. 4 Brown, Fig. 4. “The message server 40 may be implemented, for example, on a network computer within the firewall of a corporation, a computer within an ISP or ASP system or the like, and acts as the main interface for e-mail exchange over the Internet 20. Although other messaging systems might not require a message server system 40, a mobile device 100 configured for receiving and possibly sending e-mail will normally be associated with an account on a message server. Perhaps the two most common message servers are MICROSOFT® EXCHANGE and LOTUS DOMINO®. These products are often used in

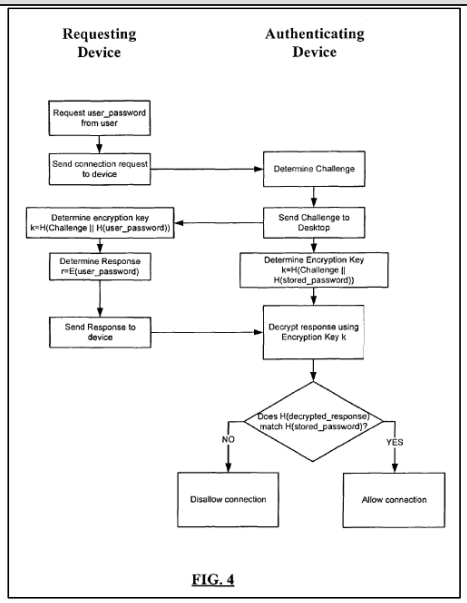
’619 Patent – Claim 22	Brown
	conjunction with Internet mail routers that route and deliver mail. These intermediate components are not shown in FIG. 1, as they do not directly play a role in the secure message processing described below. Message servers such as server 40 typically extend beyond just e-mail sending and receiving; they also include dynamic database storage engines that have predefined database formats for data like calendars, to-do lists, task lists, e-mail and documentation. The wireless gateway 85 and infrastructure 90 provide a link between the Internet 20 and wireless network 105. The wireless infrastructure 90 determines the most likely network for locating a given user and tracks the user as they roam between countries or networks. A message is then delivered to the mobile device 100 via wireless transmission, typically at a radio frequency (RF), from a base station in the wireless network 105 to the mobile device 100. The particular network 105 may be virtually any wireless network over which messages may be exchanged with a mobile communication device.” Brown 5:8-37. “As shown in FIG. 1, a composed e-mail message 15 is sent by the e-mail sender 10, located somewhere on the Internet 20. This message 15 is normally fully in the clear and uses traditional Simple Mail Transfer Protocol (SMTP), RFC822 headers and Multipurpose Internet Mail Extension (MIME) body parts to define the format of the mail message. These techniques are all well known to those skilled in the art. The message 15 arrives at the message server 40 and is normally stored in a message store. Most known messaging systems support a so-called “pull” message access scheme, wherein the mobile device 100 must request that stored messages be forwarded by the message server to the mobile device 100. Some systems provide for automatic routing of such messages which are addressed using a specific e-mail address associated with the mobile device 100. In a preferred embodiment described in further detail below, messages addressed to a message server account associated with a host system such as a home computer or office computer which belongs to the user of a mobile device 100 are redirected from the message server 40 to the mobile

’619 Patent – Claim 22	Brown
	device 100 as they are received.” Brown at 5:37-56. “In the automatic redirection system of FIG. 2, a composed e-mail message 15 leaving the e-mail sender 10 arrives at the message server 40 and is redirected by the redirection program 45 to the mobile device 100. As this redirection takes place the message 15 is re-enveloped, as indicated at 80, and a possibly proprietary compression and encryption algorithm can then be applied to the original message 15 . In this way, messages being read on the mobile device 100 are no less secure than if they were read on a desktop workstation such as 35 within the firewall. All messages exchanged between the redirection program 45 and the mobile device 100 preferably use this message repackaging technique. Another goal of this outer envelope is to maintain the addressing information of the original message except the sender's and the receiver's address. This allows reply messages to reach the appropriate destination, and also allows the “from” field to reflect the mobile user's desktop address. Using the user's e-mail address from the mobile device 100 allows the received message to appear as though the message originated from the user's desktop system 35 rather than the mobile device 100.” Brown at 7:24-43. “When the mobile device 100 is operating in a data communication mode, a received signal, such as a text message or a web page download, is processed by the transceiver module 311 and provided to the microprocessor 338, which preferably further processes the received signal in multiple stages as described above, for eventual output to the display 322, or, alternatively, to an auxiliary I/O device 328. A user of mobile device 100 may also compose data items, such as e-mail messages, using the keyboard 332, which is preferably a complete alphanumeric keyboard laid out in the QWERTY style, although other styles of complete alphanumeric keyboards such as the known DVORAK style may also be used. User input to the mobile device 100 is further enhanced with a plurality of auxiliary I/O devices 328, which may include a thumbwheel input device, a touchpad, a variety of switches, a rocker input switch, etc. The composed data items input by the user may then be transmitted over the

’619 Patent – Claim 22	Brown
	communication networks 319 via the transceiver module 311.” Brown at 13:8-26. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[22h] wherein the device is authenticated to access the messaging account.	Brown discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:

’619 Patent – Claim 22	Brown
	 FIG. 1 Brown, Fig. 1.

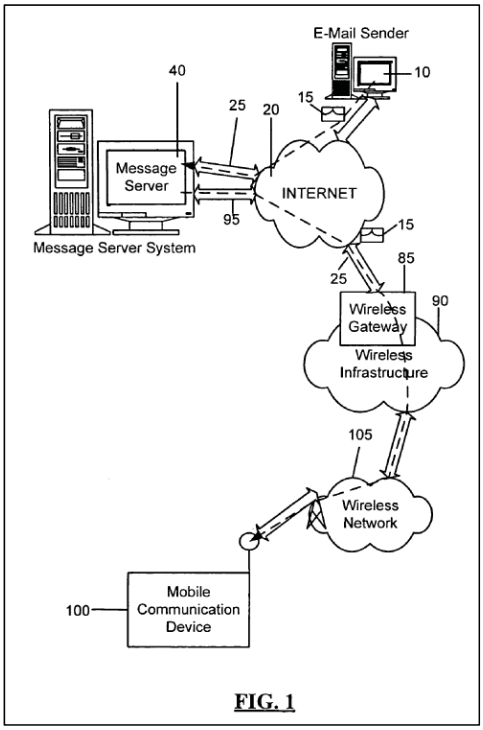
’619 Patent – Claim 22	Brown
	 Brown, Fig. 2.

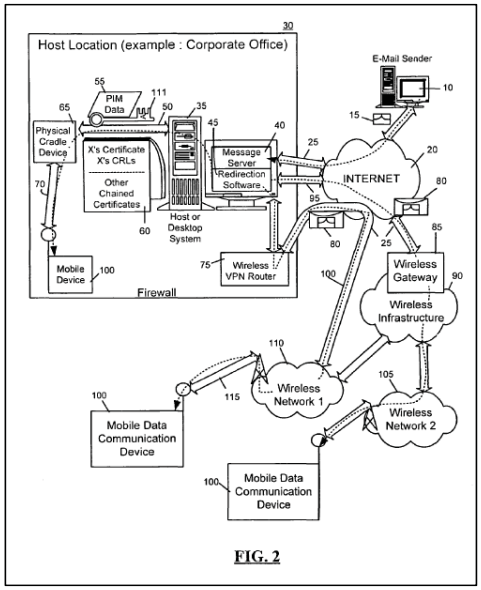
’619 Patent – Claim 22	Brown
	 FIG. 4 Brown, Fig. 4. “The message server 40 may be implemented, for example, on a network computer within the firewall of a corporation, a computer within an ISP or ASP system or the like, and acts as the main interface for e-mail exchange over the Internet 20. Although other messaging systems might not require a message server system 40, a mobile device 100 configured for receiving and possibly sending e-mail will normally be associated with an account on a message server. Perhaps the two most common message servers are MICROSOFT® EXCHANGE and LOTUS DOMINO®. These products are often used in

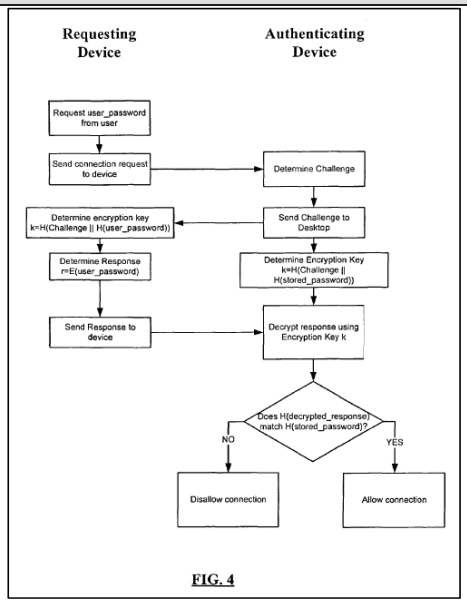
’619 Patent – Claim 22	Brown
	conjunction with Internet mail routers that route and deliver mail. These intermediate components are not shown in FIG. 1, as they do not directly play a role in the secure message processing described below. Message servers such as server 40 typically extend beyond just e-mail sending and receiving; they also include dynamic database storage engines that have predefined database formats for data like calendars, to-do lists, task lists, e-mail and documentation.” Brown at 5:8-25. “As shown in FIG. 1, a composed e-mail message 15 is sent by the e-mail sender 10, located somewhere on the Internet 20. This message 15 is normally fully in the clear and uses traditional Simple Mail Transfer Protocol (SMTP), RFC822 headers and Multipurpose Internet Mail Extension (MIME) body parts to define the format of the mail message. These techniques are all well known to those skilled in the art. The message 15 arrives at the message server 40 and is normally stored in a message store. Most known messaging systems support a so-called “pull” message access scheme, wherein the mobile device 100 must request that stored messages be forwarded by the message server to the mobile device 100. Some systems provide for automatic routing of such messages which are addressed using a specific e-mail address associated with the mobile device 100. In a preferred embodiment described in further detail below, messages addressed to a message server account associated with a host system such as a home computer or office computer which belongs to the user of a mobile device 100 are redirected from the message server 40 to the mobile device 100 as they are received.” Brown at 5:37-56. “In the automatic redirection system of FIG. 2, a composed e-mail message 15 leaving the e-mail sender 10 arrives at the message server 40 and is redirected by the redirection program 45 to the mobile device 100. As this redirection takes place the message 15 is re-enveloped, as indicated at 80, and a possibly proprietary compression and encryption algorithm can then be applied to the original message 15. In this way, messages being read on the mobile device 100 are no less secure than if they were read on a desktop workstation such as

'619 Patent – Claim 22	Brown
	35 within the firewall. All messages exchanged between the redirection program 45 and the mobile device 100 preferably use this message repackaging technique. Another goal of this outer envelope is to maintain the addressing information of the original message except the sender's and the receiver's address. This allows reply messages to reach the appropriate destination, and also allows the "from" field to reflect the mobile user's desktop address. Using the user's e-mail address from the mobile device 100 allows the received message to appear as though the message originated from the user's desktop system 35 rather than the mobile device 100." Brown at 7:24-43. "The private key is preferably exchanged so that the desktop 35 and mobile device 100 share one personality and one method for accessing all mail." Brown at 7:57-59. "After any required network registration or activation procedures have been completed, the mobile device 100 may the send and receive communication signals, including both voice and data signals, over the networks 319. Signals received by the antenna 316 from the communication network 319 are routed to the receiver 312, which provides for signal amplification, frequency down conversion, filtering, channel selection, etc., and may also provide analog to digital conversion. Analog to digital conversion of the received signal allows more complex communication functions, such as digital demodulation and decoding to be performed using the DSP 320. In a similar manner, signals to be transmitted to the network 319 are processed, including modulation and encoding, for example, by the DSP 320 and are then provided to the transmitter 314 for digital to analog conversion, frequency up conversion, filtering, amplification and transmission to the communication network 319 via the antenna 318." Brown 10:55-11:4. "The non-volatile memory 324 preferably also provides a file system to facilitate storage of PIM data items on the device. The PIM application preferably includes the ability to send and receive data items, either by itself, or

’619 Patent – Claim 22	Brown
	in conjunction with the voice and data communication modules 324A, 324B, via the wireless networks 319. The PIM data items are preferably seamlessly integrated, synchronized and updated, via the wireless networks 319, with a corresponding set of data items stored or associated with a host computer system, thereby creating a mirrored system for data items associated with a particular user.” Brown at 12:19-29. “The mobile device 100 may be manually synchronized with a host system by placing the device 100 in an interface cradle, which couples the serial port 330 of the mobile device 100 to the serial port of a computer system or device. The serial port 330 may also be used to enable a user to set preferences through an external device or software application, or to download other application modules 324N for installation. This wired download path may be used to load an encryption key onto the device, which is a more secure method than exchanging encryption information via the wireless network 319. Interfaces for other wired download paths may be provided in the mobile device 100, in addition to or instead of the serial port 330. For example, a USB port would provide an interface to a similarly equipped personal computer.” Brown at 12:46-61. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

’619 Patent – Claim 23	Brown
[23] The device of claim 22, wherein the information including the service activation code is received by the device in response to user input at the remote device.	Brown discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22pre]-[22h], *above*.  **FIG. 1**

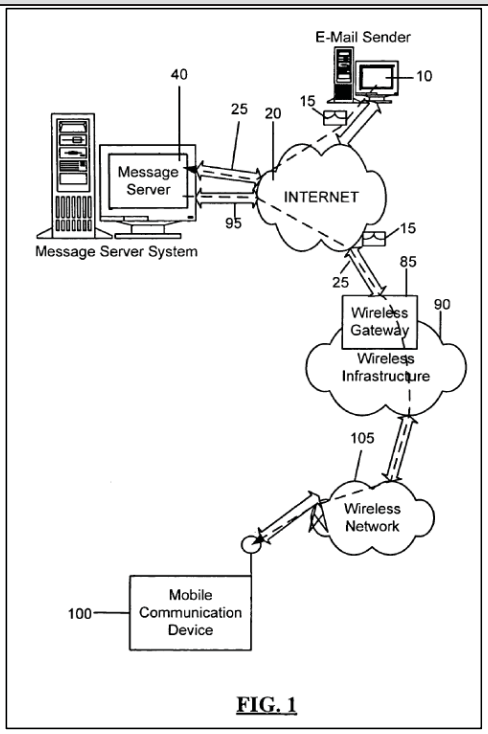
’619 Patent – Claim 23	Brown
	Brown, Fig. 1.  FIG. 2 Brown, Fig. 2.

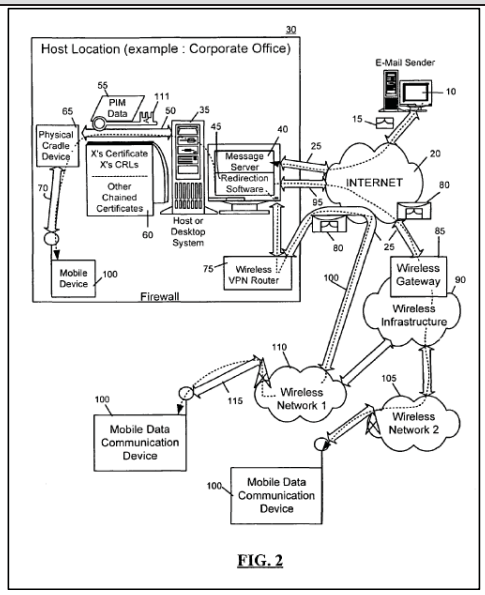
’619 Patent – Claim 23	Brown
	 FIG. 4 Brown, Fig. 4. “When device 10 is connected to the desktop system 35, for instance through a serial link such as a universal serial bus (USB) link, the user of the desktop system 35 is prompted to enter a password in order to authenticate the user to the device 10. The desktop system 35 creates a one-way hash of the password provided by the user, and transmits the hash of the password to the device 10. The device 10 then compares the hash of the password to a stored hash of the device password. If the two values match, then the user is authenticated and the desktop system 35 is allowed to form a connection with the device 10. In this

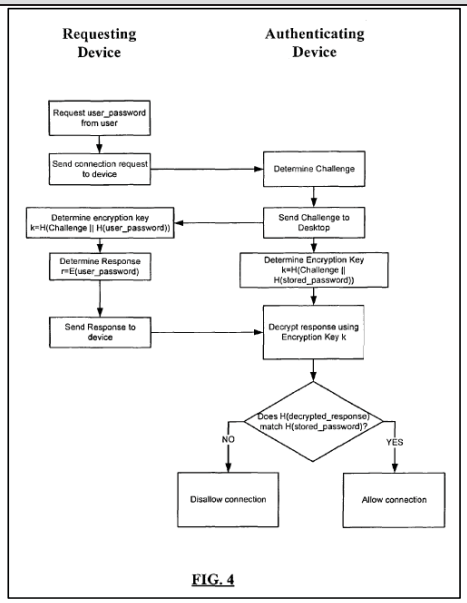
'619 Patent – Claim 23	Brown
	typical challenge response scheme, only the hash of the password is transmitted to the device 10. If the password itself were sent over the communications link, an attacker would be able to intercept the transmission and gain knowledge of the password." Brown at 7:67-8:15. "FIG. 4 illustrates a challenge response scheme in accordance with a preferred embodiment of the present invention. In the preferred embodiment, a requesting device, such as the desktop system 35, is connected to an authenticating device, such as mobile device 10, using a communications link, such as a universal serial bus (USB) link, through which the requesting device may send a connection request. The connection request may be in the form of a software request sent to the authenticating device, or the detection of a change in a hardware state of the communications link. The authenticating device detects that a connection is being requested, and proceeds to authenticate the requesting device in accordance with the challenge response scheme described below. It will be understood that the authenticating device may only initiate the challenge response scheme if the authenticating device has been secured by a device password (stored_password). In order to determine if a requesting device needs to be authenticated, the authenticating device may check for the presence of a hash of the device password H(stored_password) in a memory of the authenticating device. In other implementations, the authentication device may check for a flag indicating whether the device has been secured." Brown at 8:16-37. "The requesting device prompts the user of the requesting device for a password user_password. This password is hashed, using known hashing functions such as SHA-1, to create H(user_password) which is then combined with the 50 Challenge c received from the authenticating device. In the preferred embodiment, the Challenge c and the hash of the password H(user_password) are concatenated together. It is understood that there are different ways in which to combine the two values. This combination of the Challenge c and the 55 hash of the password H(user_password) is further

’619 Patent – Claim 23	Brown
	hashed in order to generate a requesting encryption key kr=H(cllH (user_password)) that is used in creating a response r to the challenge issued by the authenticating device. The response r is generated by encrypting the password user_password using known techniques such as AES or TripleDES. In some implementations, the response r may also be generated by applying the XOR function to the requesting encryption key k, and the password user_password. The response r is then transmitted to the authenticating device.” Brown at 8:46-58. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

’619 Patent – Claim 24	Brown
[24] The device of claim 22, wherein the information including the service activation code is received by the device in an off-line communication.	Brown discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22pre]-[22h], *above*.

’619 Patent – Claim 24	Brown
	 FIG. 1 Brown, Fig. 1.

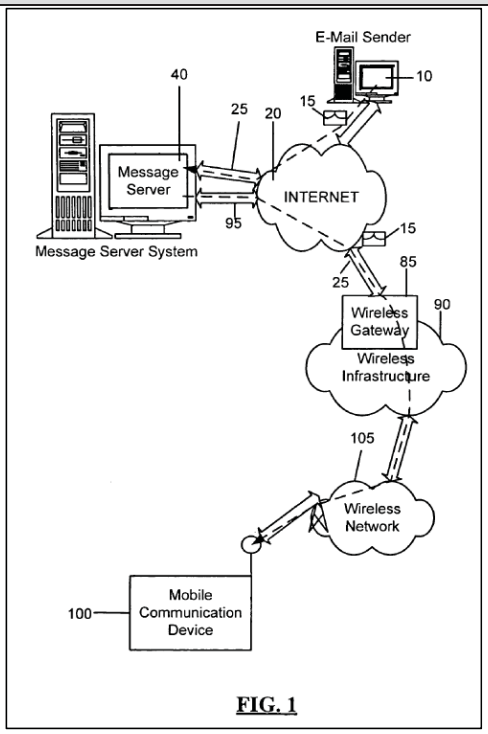
’619 Patent – Claim 24	Brown
	 FIG. 2 Brown, Fig. 2.

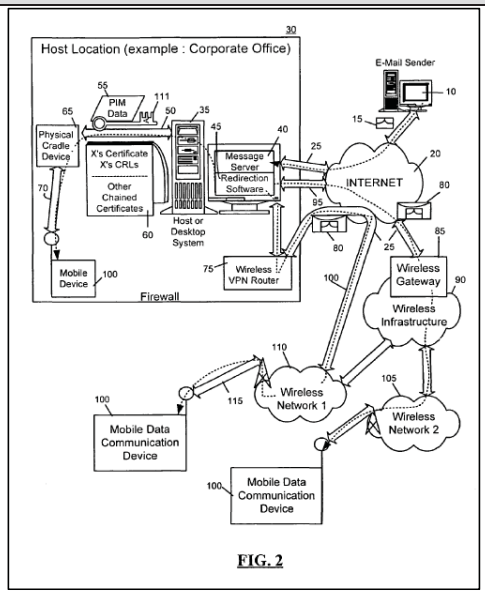
’619 Patent – Claim 24	Brown
	 FIG. 4 Brown, Fig. 4. “When device 10 is connected to the desktop system 35, for instance through a serial link such as a universal serial bus (USB) link, the user of the desktop system 35 is prompted to enter a password in order to authenticate the user to the device 10. The desktop system 35 creates a one-way hash of the password provided by the user, and transmits the hash of the password to the device 10. The device 10 then compares the hash of the password to a stored hash of the device password. If the two values match, then the user is authenticated and the desktop system 35 is allowed to form a connection with the device 10. In this

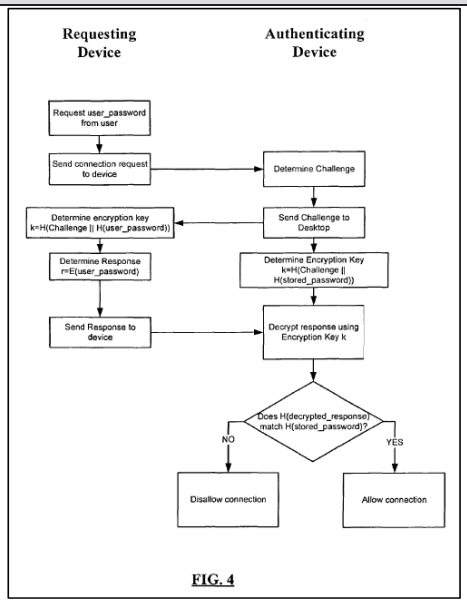
’619 Patent – Claim 24	Brown
	typical challenge response scheme, only the hash of the password is transmitted to the device 10. If the password itself were sent over the communications link, an attacker would be able to intercept the transmission and gain knowledge of the password.” Brown at 7:67-8:15. “The mobile device 100 may be manually synchronized with a host system by placing the device 100 in an interface cradle, which couples the serial port 330 of the mobile device 100 to the serial port of a computer system or device. The serial port 330 may also be used to enable a user to set preferences through an external device or software application, or to download other application modules 324N for installation. This wired download path may be used to load an encryption key onto the device, which is a more secure method than exchanging encryption information via the wireless network 319. Interfaces for other wired download paths may be provided in the mobile device 100, in addition to or instead of the serial port 330. For example, a USB port would provide an interface to a similarly equipped personal computer.” Brown at 12:46-61. “A short-range communications subsystem 340 is also included in the mobile device 100. The subsystem 340 may include an infrared device and associated circuits and components, or a short-range RF communication module such as a BLUETOOTH® module or an 802.11 module, for example, to provide for communication with similarly-enabled systems and devices. Those skilled in the art will appreciate that "BLUETOOTH" and "802.11" refer to sets of specifications, available from the Institute of Electrical and Electronics Engineers, relating to wireless personal area networks and wireless local area networks, respectively.” Brown at 13:43-54. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person

'619 Patent – Claim 24	Brown
	of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

'619 Patent – Claim 25	Brown
[25] The device of claim 24, wherein the off-line communication involves a local connection.	Brown discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22pre]-[22h] and [24], *above*.

’619 Patent – Claim 25	Brown
	 FIG. 1 Brown, Fig. 1.

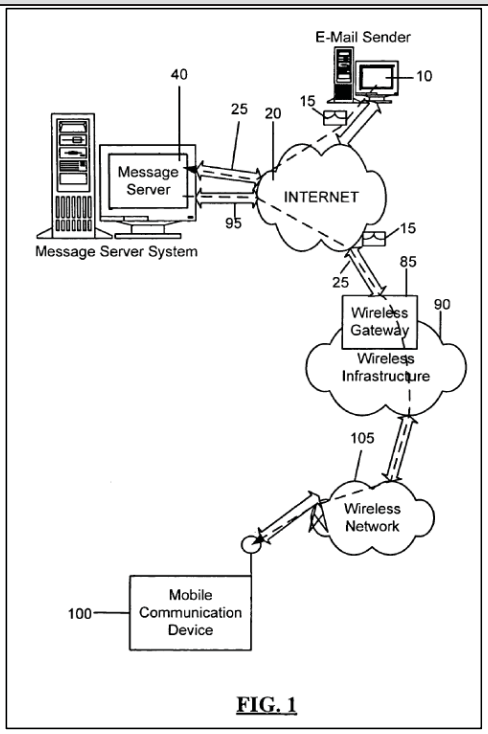
’619 Patent – Claim 25	Brown
	 FIG. 2 Brown, Fig. 2.

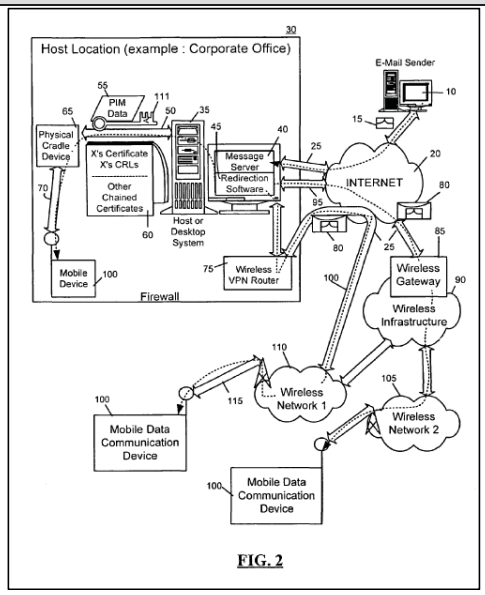
’619 Patent – Claim 25	Brown
	 FIG. 4 Brown, Fig. 4. “When device 10 is connected to the desktop system 35, for instance through a serial link such as a universal serial bus (USB) link, the user of the desktop system 35 is prompted to enter a password in order to authenticate the user to the device 10. The desktop system 35 creates a one-way hash of the password provided by the user, and transmits the hash of the password to the device 10. The device 10 then compares the hash of the password to a stored hash of the device password. If the two values match, then the user is authenticated and the desktop system 35 is allowed to form a connection with the device 10. In this

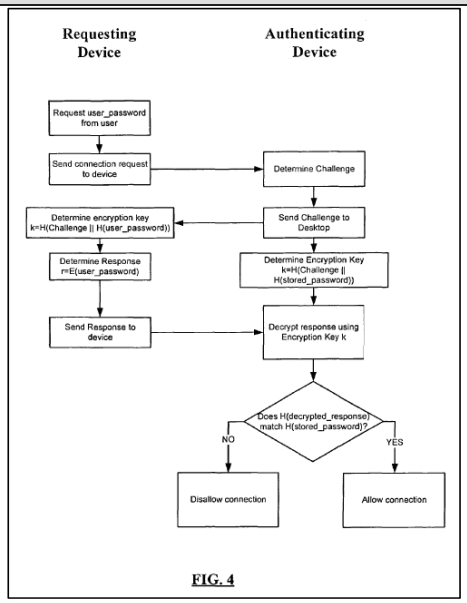
’619 Patent – Claim 25	Brown
	typical challenge response scheme, only the hash of the password is transmitted to the device 10. If the password itself were sent over the communications link, an attacker would be able to intercept the transmission and gain knowledge of the password.” Brown at 7:67-8:15. “The mobile device 100 may be manually synchronized with a host system by placing the device 100 in an interface cradle, which couples the serial port 330 of the mobile device 100 to the serial port of a computer system or device. The serial port 330 may also be used to enable a user to set preferences through an external device or software application, or to download other application modules 324N for installation. This wired download path may be used to load an encryption key onto the device, which is a more secure method than exchanging encryption information via the wireless network 319. Interfaces for other wired download paths may be provided in the mobile device 100, in addition to or instead of the serial port 330. For example, a USB port would provide an interface to a similarly equipped personal computer.” Brown at 12:46-61. “A short-range communications subsystem 340 is also included in the mobile device 100. The subsystem 340 may include an infrared device and associated circuits and components, or a short-range RF communication module such as a BLUETOOTH® module or an 802.11 module, for example, to provide for communication with similarly-enabled systems and devices. Those skilled in the art will appreciate that "BLUETOOTH" and "802.11" refer to sets of specifications, available from the Institute of Electrical and Electronics Engineers, relating to wireless personal area networks and wireless local area networks, respectively.” Brown at 13:43-54. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person

'619 Patent – Claim 25	Brown
	of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

'619 Patent – Claim 26	Brown
[26] The device of claim 24, wherein the off-line communication prevents eavesdropping of the service activation code.	Brown discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22pre]-[22h] and [24], *above*.

’619 Patent – Claim 26	Brown
	 FIG. 1 Brown, Fig. 1.

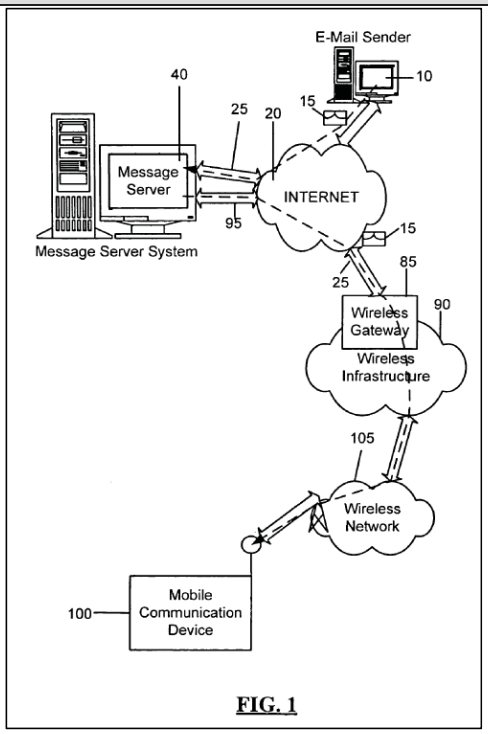
’619 Patent – Claim 26	Brown
	 FIG. 2 Brown, Fig. 2.

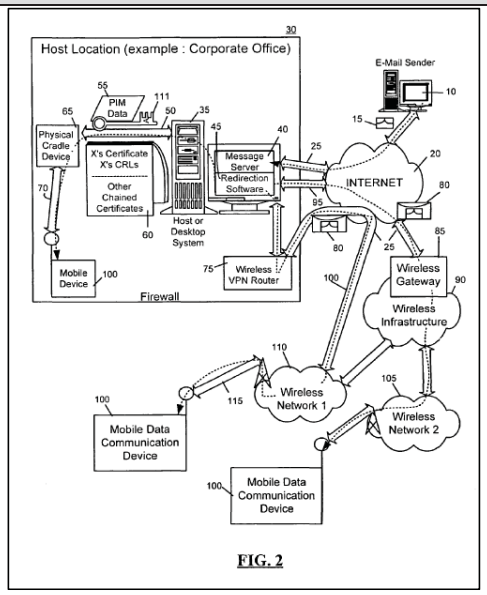
’619 Patent – Claim 26	Brown
	 FIG. 4 Brown, Fig. 4. “When device 10 is connected to the desktop system 35, for instance through a serial link such as a universal serial bus (USB) link, the user of the desktop system 35 is prompted to enter a password in order to authenticate the user to the device 10. The desktop system 35 creates a one-way hash of the password provided by the user, and transmits the hash of the password to the device 10. The device 10 then compares the hash of the password to a stored hash of the device password. If the two values match, then the user is authenticated and the desktop system 35 is allowed to form a connection with the device 10. In this

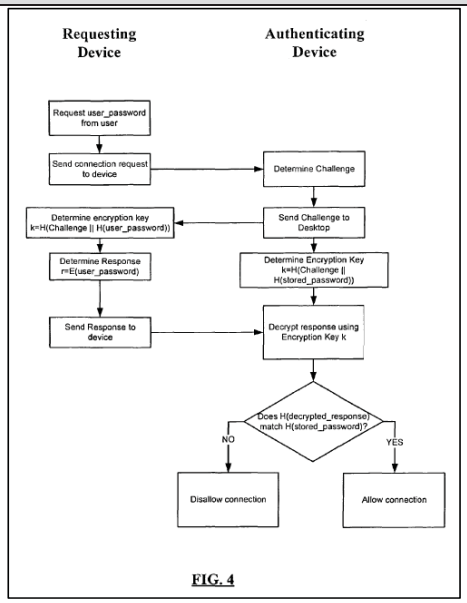
’619 Patent – Claim 26	Brown
	typical challenge response scheme, only the hash of the password is transmitted to the device 10. If the password itself were sent over the communications link, an attacker would be able to intercept the transmission and gain knowledge of the password.” Brown at 7:67-8:15. “The mobile device 100 may be manually synchronized with a host system by placing the device 100 in an interface cradle, which couples the serial port 330 of the mobile device 100 to the serial port of a computer system or device. The serial port 330 may also be used to enable a user to set preferences through an external device or software application, or to download other application modules 324N for installation. This wired download path may be used to load an encryption key onto the device, which is a more secure method than exchanging encryption information via the wireless network 319. Interfaces for other wired download paths may be provided in the mobile device 100, in addition to or instead of the serial port 330. For example, a USB port would provide an interface to a similarly equipped personal computer.” Brown at 12:46-61. “A short-range communications subsystem 340 is also included in the mobile device 100. The subsystem 340 may include an infrared device and associated circuits and components, or a short-range RF communication module such as a BLUETOOTH® module or an 802.11 module, for example, to provide for communication with similarly-enabled systems and devices. Those skilled in the art will appreciate that "BLUETOOTH" and "802.11" refer to sets of specifications, available from the Institute of Electrical and Electronics Engineers, relating to wireless personal area networks and wireless local area networks, respectively.” Brown at 13:43-54. “According to a further aspect of the invention there is provided a method for securely transmitting information to a receiving device, the receiving device being provided with a hash of the information, a random number, and a receiving encryption key including a hash of the random number and the hash

’619 Patent – Claim 26	Brown
	of the information.” Brown at 3:27-32. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

’619 Patent – Claim 27	Brown
[27] The device of claim 22, wherein the authentication of the device relies on the authentication of the messaging account.	Brown discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22pre]-[22h], *above*.

’619 Patent – Claim 27	Brown
	 FIG. 1 Brown, Fig. 1.

’619 Patent – Claim 27	Brown
	 FIG. 2 Brown, Fig. 2.

’619 Patent – Claim 27	Brown
	 FIG. 4 Brown, Fig. 4. “An e-mail sender system 10 may, for example, be connected to an ISP (Internet Service Provider) on which a user of the system 10 has an account, located within a company, possibly connected to a local area network (LAN), and connected to the Internet 20, or connected to the Internet 20 through a large ASP (application service provider) such as AMERICA ONLINE® (AOL).” Brown 4:63-5:2. “FIG. 3 shows a typical challenge response scheme used by an authenticating

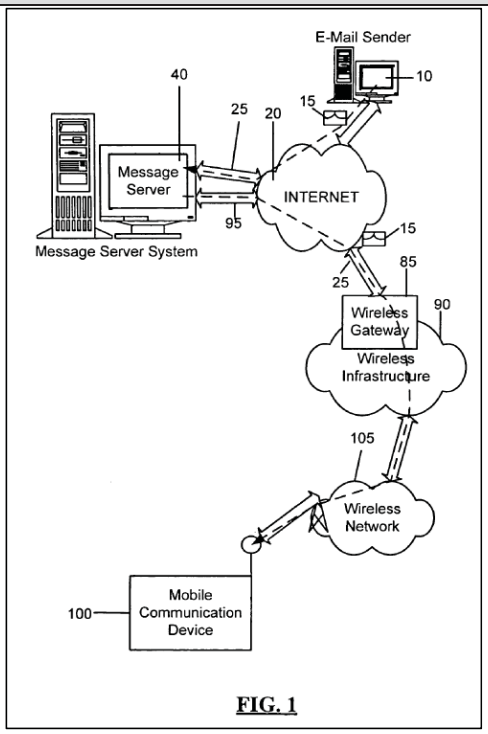
’619 Patent – Claim 27	Brown
	device, such as mobile device 10 to authenticate a requesting device, such as desktop system 35 that may be requesting a connection to the device 10. When device 10 is connected to the desktop system 35, for instance through a serial link such as a universal serial bus (USB) link, the user of the desktop system 35 is prompted to enter a password in order to authenticate the user to the device 10. The desktop system 35 creates a one-way hash of the password provided by the user, and transmits the hash of the password to the device 10. The device 10 then compares the hash of the password to a stored hash of the device password. If the two values match, then the user is authenticated and the desktop system 35 is allowed to form a connection with the device 10. In this typical challenge response scheme, only the hash of the password is transmitted to the device 10. If the password itself were sent over the communications link, an attacker would be able to intercept the transmission and gain knowledge of the password. FIG. 4 illustrates a challenge response scheme in accordance with a preferred embodiment of the present invention. In the preferred embodiment, a requesting device, such as the desktop system 35, is connected to an authenticating device, such as mobile device 10, using a communications link, such as a universal serial bus (USB) link, through which the requesting device may send a connection request. The connection request may be in the form of a software request sent to the authenticating device, or the detection of a change in a hardware state of the communications link. The authenticating device detects that a connection is being requested, and proceeds to authenticate the requesting device in accordance with the challenge response scheme described below. It will be understood that the authenticating device may only initiate the challenge response scheme if the authenticating device has been secured by a device password (stored_password). In order to determine if a requesting device needs to be authenticated, the authenticating device may check for the presence of a hash of the device password H(stored_password) in a memory of the authenticating device. In other implementations, the authentication device

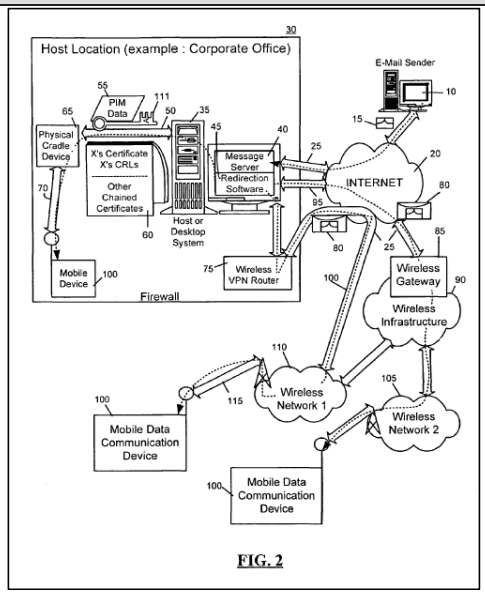
’619 Patent – Claim 27	Brown
	may check for a flag indicating whether the device has been secured. When the authenticating device detects a connection request, it generates a Challenge c to issue to the requesting device. The Challenge c may be a group of bits that have been randomly generated by the authenticating device. Alternatively, the numbers of bits used in the Challenge c may also be randomized. The authenticating device may use a hardware-based random number generator or a software-based random number generator to generate the random Challenge c. The requesting device prompts the user of the requesting device for a password user_password. This password is hashed, using known hashing functions such as SHA-1, to create H(user_password) which is then combined with the Challenge c received from the authenticating device. In the preferred embodiment, the Challenge c and the hash of the password H(user_password) are concatenated together. It is understood that there are different ways in which to combine the two values. This combination of the Challenge c and the hash of the password H(user_password) is further hashed in order to generate a requesting encryption key kr=H(c‖H(user_password)) that is used in creating a response r to the challenge issued by the authenticating device. The response r is generated by encrypting the password user_password using known techniques such as AES or TripleDES. In some implementations, the response r may also be generated by applying the XOR function to the requesting encryption key kr and the password user_password. The response r is then transmitted to the authenticating device. The authenticating device determines an authenticating encryption key ka by following a process similar to that followed by the requesting device. The authenticating device combines the stored hash of the device password H(stored_password) with the randomly generated Challenge c, and then generates a hash of the combination, in order to generate the authenticating encryption key ka=H(c‖H(stored_password)). The authenticating encryption

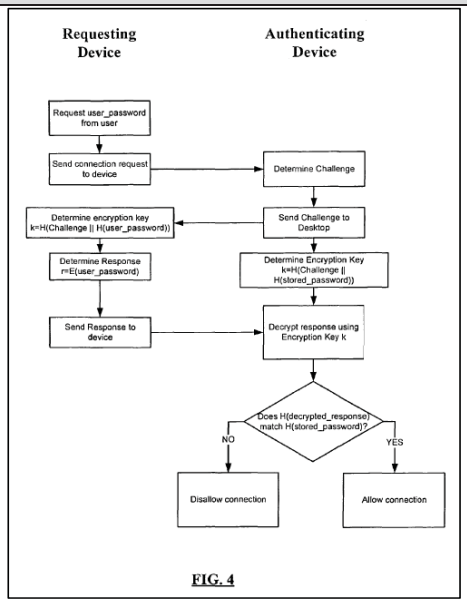
’619 Patent – Claim 27	Brown
	key ka is used to decrypt the response r received from the requesting device. A hash of the decrypted response H(decrypted_response) is then compared to the stored hash of the device password H(stored_password). If the two hashes match, then the decrypted response was the correct device password. Thus the authenticating device has authenticated the requesting device. The authenticating device is also in possession of the device password for use in operations that require the device password. If the two hashes do not match, then the user did not provide the correct password, and the authenticating device rejects the connection request from the requesting device, and thereby disallows the connection.” Brown at 7:64-9:17. “Depending upon the type of network or networks 319, the access requirements for the mobile device 100 may also vary. For example, in the Mobitex and DataTAC data networks, mobile devices are registered on the network using a unique identification number associated with each mobile device. In GPRS data networks, however, network access is associated with a subscriber or user of a mobile device. A GPRS device typically requires a subscriber identity module ("SIM"), which is required in order to operate a mobile device on a GPRS network. Local or non-network communication functions (if any) may be operable, without the SIM device, but a mobile device will be unable to carry out any functions involving communications over the data network 319, other than any legally required operations, such as '911' emergency calling. After any required network registration or activation procedures have been completed, the mobile device 100 may the send and receive communication signals, including both voice and data signals, over the networks 319. Signals received by the antenna 316 from the communication network 319 are routed to the receiver 312, which provides for signal amplification, frequency down conversion, filtering, channel selection, etc., and may also provide analog to digital conversion. Analog to digital conversion of the received signal allows more complex communication functions, such as digital demodulation and decoding to be performed using the DSP 320. In a similar manner, signals to be transmitted to the network 319 are processed, including modulation and

'619 Patent – Claim 27	Brown
	encoding, for example, by the DSP 320 and are then provided to the transmitter 314 for digital to analog conversion, frequency up conversion, filtering, amplification and transmission to the communication network 319 via the antenna 318." Brown 10:40-11:4. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

'619 Patent – Claim 28	Brown
[28] The device of claim 27, wherein the authentication of the messaging account includes a username and password.	Brown discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22pre]-[22h] and [27], *above*.

’619 Patent – Claim 28	Brown
	 FIG. 1 Brown, Fig. 1.

’619 Patent – Claim 28	Brown
	 FIG. 2 Brown, Fig. 2.

’619 Patent – Claim 28	Brown
	 FIG. 4 Brown, Fig. 4. “An e-mail sender system 10 may, for example, be connected to an ISP (Internet Service Provider) on which a user of the system 10 has an account, located within a company, possibly connected to a local area network (LAN), and connected to the Internet 20, or connected to the Internet 20 through a large ASP (application service provider) such as AMERICA ONLINE® (AOL).” Brown 4:63-5:2. “FIG. 3 shows a typical challenge response scheme used by an authenticating

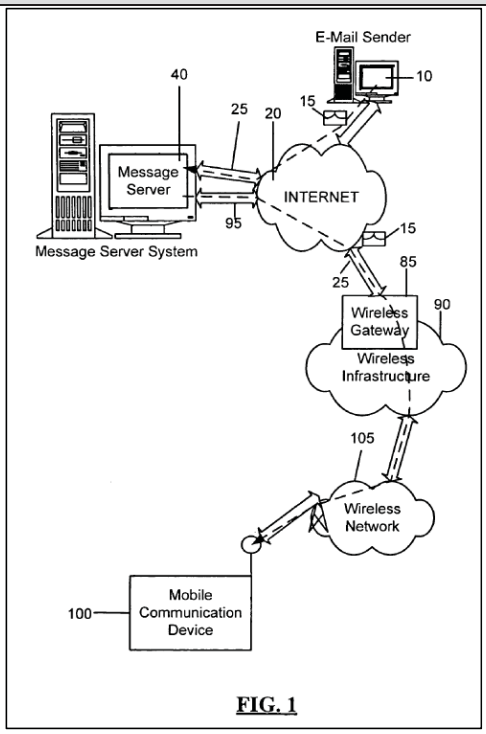
’619 Patent – Claim 28	Brown
	device, such as mobile device 10 to authenticate a requesting device, such as desktop system 35 that may be requesting a connection to the device 10. When device 10 is connected to the desktop system 35, for instance through a serial link such as a universal serial bus (USB) link, the user of the desktop system 35 is prompted to enter a password in order to authenticate the user to the device 10. The desktop system 35 creates a one-way hash of the password provided by the user, and transmits the hash of the password to the device 10. The device 10 then compares the hash of the password to a stored hash of the device password. If the two values match, then the user is authenticated and the desktop system 35 is allowed to form a connection with the device 10. In this typical challenge response scheme, only the hash of the password is transmitted to the device 10. If the password itself were sent over the communications link, an attacker would be able to intercept the transmission and gain knowledge of the password. FIG. 4 illustrates a challenge response scheme in accordance with a preferred embodiment of the present invention. In the preferred embodiment, a requesting device, such as the desktop system 35, is connected to an authenticating device, such as mobile device 10, using a communications link, such as a universal serial bus (USB) link, through which the requesting device may send a connection request. The connection request may be in the form of a software request sent to the authenticating device, or the detection of a change in a hardware state of the communications link. The authenticating device detects that a connection is being requested, and proceeds to authenticate the requesting device in accordance with the challenge response scheme described below. It will be understood that the authenticating device may only initiate the challenge response scheme if the authenticating device has been secured by a device password (stored_password). In order to determine if a requesting device needs to be authenticated, the authenticating device may check for the presence of a hash of the device password H(stored_password) in a memory of the authenticating device. In other implementations, the authentication device

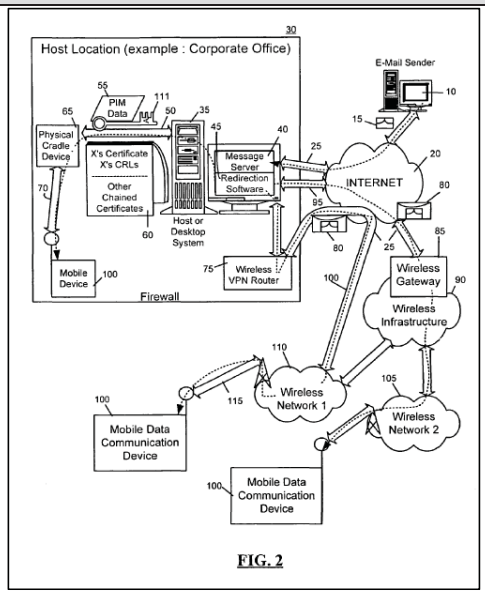
’619 Patent – Claim 28	Brown
	may check for a flag indicating whether the device has been secured. When the authenticating device detects a connection request, it generates a Challenge c to issue to the requesting device. The Challenge c may be a group of bits that have been randomly generated by the authenticating device. Alternatively, the numbers of bits used in the Challenge c may also be randomized. The authenticating device may use a hardware-based random number generator or a software-based random number generator to generate the random Challenge c. The requesting device prompts the user of the requesting device for a password user_password. This password is hashed, using known hashing functions such as SHA-1, to create H(user_password) which is then combined with the Challenge c received from the authenticating device. In the preferred embodiment, the Challenge c and the hash of the password H(user_password) are concatenated together. It is understood that there are different ways in which to combine the two values. This combination of the Challenge c and the hash of the password H(user_password) is further hashed in order to generate a requesting encryption key kr=H(c‖H(user_password)) that is used in creating a response r to the challenge issued by the authenticating device. The response r is generated by encrypting the password user_password using known techniques such as AES or TripleDES. In some implementations, the response r may also be generated by applying the XOR function to the requesting encryption key kr and the password user_password. The response r is then transmitted to the authenticating device. The authenticating device determines an authenticating encryption key ka by following a process similar to that followed by the requesting device. The authenticating device combines the stored hash of the device password H(stored_password) with the randomly generated Challenge c, and then generates a hash of the combination, in order to generate the authenticating encryption key ka=H(c‖H(stored_password)). The authenticating encryption

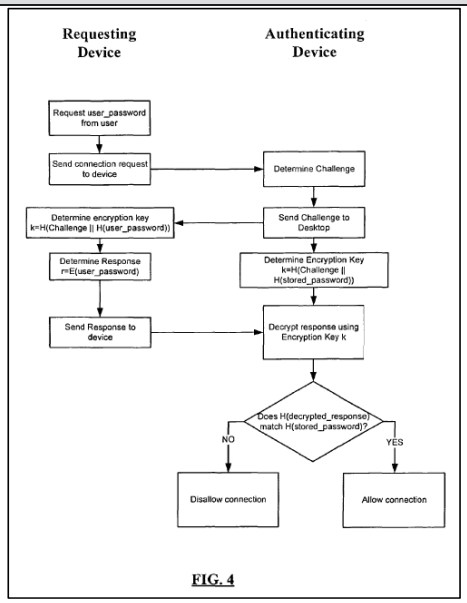
’619 Patent – Claim 28	Brown
	key ka is used to decrypt the response r received from the requesting device. A hash of the decrypted response H(decrypted_response) is then compared to the stored hash of the device password H(stored_password). If the two hashes match, then the decrypted response was the correct device password. Thus the authenticating device has authenticated the requesting device. The authenticating device is also in possession of the device password for use in operations that require the device password. If the two hashes do not match, then the user did not provide the correct password, and the authenticating device rejects the connection request from the requesting device, and thereby disallows the connection.” Brown at 7:64-9:17. “Depending upon the type of network or networks 319, the access requirements for the mobile device 100 may also vary. For example, in the Mobitex and DataTAC data networks, mobile devices are registered on the network using a unique identification number associated with each mobile device. In GPRS data networks, however, network access is associated with a subscriber or user of a mobile device. A GPRS device typically requires a subscriber identity module ("SIM"), which is required in order to operate a mobile device on a GPRS network. Local or non-network communication functions (if any) may be operable, without the SIM device, but a mobile device will be unable to carry out any functions involving communications over the data network 319, other than any legally required operations, such as '911' emergency calling. After any required network registration or activation procedures have been completed, the mobile device 100 may the send and receive communication signals, including both voice and data signals, over the networks 319. Signals received by the antenna 316 from the communication network 319 are routed to the receiver 312, which provides for signal amplification, frequency down conversion, filtering, channel selection, etc., and may also provide analog to digital conversion. Analog to digital conversion of the received signal allows more complex communication functions, such as digital demodulation and decoding to be performed using the DSP 320. In a similar manner, signals to be transmitted to the network 319 are processed, including modulation and

’619 Patent – Claim 28	Brown
	encoding, for example, by the DSP 320 and are then provided to the transmitter 314 for digital to analog conversion, frequency up conversion, filtering, amplification and transmission to the communication network 319 via the antenna 318.” Brown 10:40-11:4. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

’619 Patent – Claim 32	Brown
[32] The device of claim 22, wherein the encryption key is closely related to the service activation code.	Brown discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22pre]-[22h], *above*.

’619 Patent – Claim 32	Brown
	 FIG. 1 Brown, Fig. 1.

’619 Patent – Claim 32	Brown
	 FIG. 2 Brown, Fig. 2.

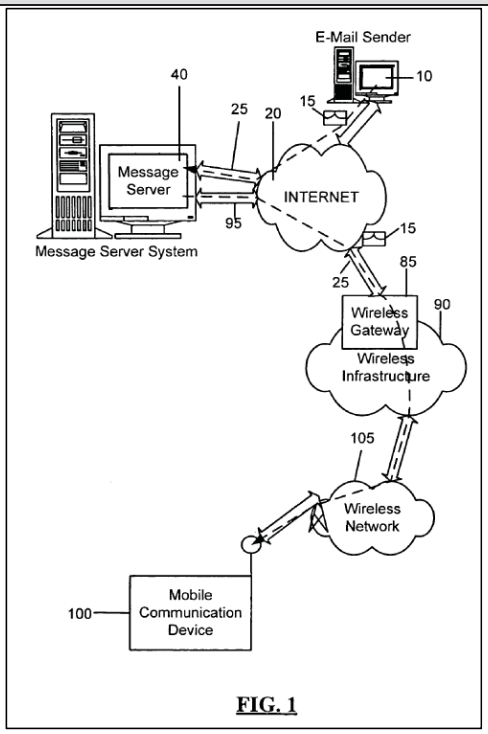
’619 Patent – Claim 32	Brown
	 FIG. 4 Brown, Fig. 4. “FIG. 4 illustrates a challenge response scheme in accordance with a preferred embodiment of the present invention. In the preferred embodiment, a requesting device, such as the desktop system 35, is connected to an authenticating device, such as mobile device 10, using a communications link, such as a universal serial bus (USB) link, through which the requesting device may send a connection request.” Brown at 8:16-23. “The requesting device prompts the user of the requesting device for a

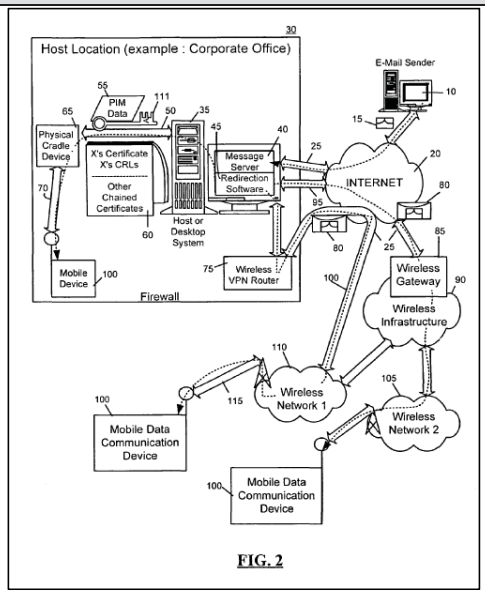
’619 Patent – Claim 32	Brown
	password user_password. This password is hashed, using known hashing functions such as SHA-1, to create H(user_password) which is then combined with the 50 Challenge c received from the authenticating device. In the preferred embodiment, the Challenge c and the hash of the password H(user_password) are concatenated together. It is understood that there are different ways in which to combine the two values. This combination of the Challenge c and the 55 hash of the password H(user_password) is further hashed in order to generate a requesting encryption key kr=H(cllH (user_password)) that is used in creating a response r to the challenge issued by the authenticating device.” Brown at 8:46-58 “The authenticating device determines an authenticating encryption key ka by following a process similar to that followed by the requesting device. The authenticating device combines the stored hash of the device password H(stored_password) with the randomly generated Challenge c, and then generates a hash of the combination, in order to generate the authenticating encryption key ka=H(c‖H(stored_password)). The authenticating encryption key ka is used to decrypt the response r received from the requesting device. A hash of the decrypted response H(decrypted_response) is then compared to the stored hash of the device password H(stored_password). If the two hashes match, then the decrypted response was the correct device password. Thus the authenticating device has authenticated the requesting device. The authenticating device is also in possession of the device password for use in operations that require the device password. If the two hashes do not match, then the user did not provide the correct password, and the authenticating device rejects the connection request from the requesting device, and thereby disallows the connection.” Brown at 8:65-9:17. “A challenge response scheme authenticates a requesting device by an authenticating device. The authenticating device generates and issues a challenge to the requesting device. The requesting device combines the challenge with a hash of a password provided by a user, and the combination is

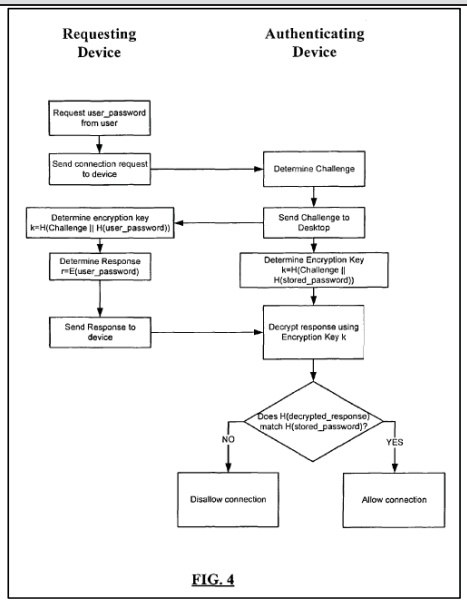
’619 Patent – Claim 32	Brown
	further hashed in order to generate a requesting encryption key used to encrypt the user supplied password. The encrypted user supplied password is sent to the authenticating device as a response to the issued challenge. The authenticating device generates an authenticating encryption key by generating the hash of a combination of the challenge and a stored hash of an authenticating device password. The authenticating encryption key is used to decrypt the response in order to retrieve the user-supplied password. If the user-supplied password hash matches the stored authenticating device password hash, the requesting device is authenticated and the authenticating device is in possession of the password.” Brown at ABSTRACT; Brown at SUMMARY. “The mobile device 100 may be manually synchronized with a host system by placing the device 100 in an interface cradle, which couples the serial port 330 of the mobile device 100 to the serial port of a computer system or device. The serial port 330 may also be used to enable a user to set preferences through an external device or software application, or to download other application modules 324N for installation. This wired download path may be used to load an encryption key onto the device, which is a more secure method than exchanging encryption information via the wireless network 319. Interfaces for other wired download paths may be provided in the mobile device 100, in addition to or instead of the serial port 330. For example, a USB port would provide an interface to a similarly equipped personal computer.” Brown at 12:46-61. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and

’619 Patent – Claim 32	Brown
	Exhibit 619-B.

’619 Patent – Claim 33	Brown
[33a] The device of claim 22, wherein the device is further operable to:	Brown discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22pre]-[22h], *above*. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[33b] store an association between at least two of the encryption key, the messaging account, an identifier of the remote device, and the service activation code.	Brown discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22pre]-[22h], *above*.

’619 Patent – Claim 33	Brown
	 FIG. 1 Brown, Fig. 1.

’619 Patent – Claim 33	Brown
	 FIG. 2 Brown, Fig. 2.

’619 Patent – Claim 33	Brown
	 FIG. 4 Brown, Fig. 4. “A challenge response scheme authenticates a requesting device by an authenticating device. The authenticating device generates and issues a challenge to the requesting device. The requesting device combines the challenge with a hash of a password provided by a user, and the combination is further hashed in order to generate a requesting encryption key used to encrypt the user supplied password. The encrypted user supplied password is sent to the authenticating device as a response to the issued challenge. The authenticating device generates an authenticating encryption key by generating the hash of a

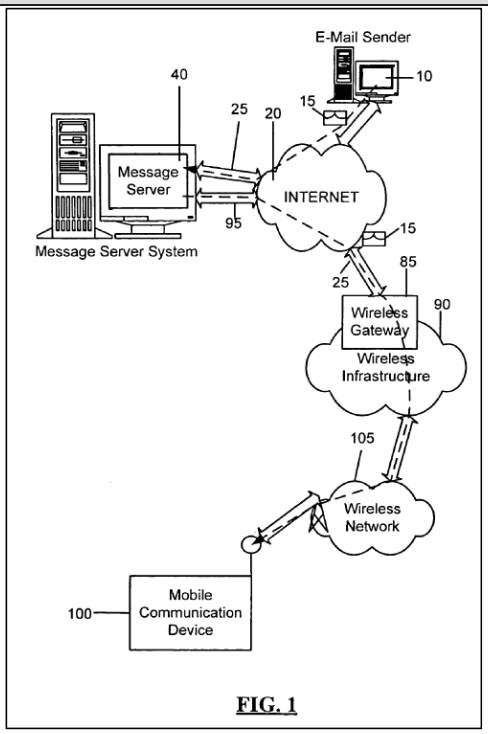
’619 Patent – Claim 33	Brown
	combination of the challenge and a stored hash of an authenticating device password. The authenticating encryption key is used to decrypt the response in order to retrieve the user-supplied password. If the user-supplied password hash matches the stored authenticating device password hash, the requesting device is authenticated and the authenticating device is in possession of the password.” Brown at ABSTRACT; Brown at SUMMARY. “FIG. 4 illustrates a challenge response scheme in accordance with a preferred embodiment of the present invention. In the preferred embodiment, a requesting device, such as the desktop system 35, is connected to an authenticating device, such as mobile device 10, using a communications link, such as a universal serial bus (USB) link, through which the requesting device may send a connection request. The connection request may be in the form of a software request sent to the authenticating device, or the detection of a change in a hardware state of the communications link. The authenticating device detects that a connection is being requested, and proceeds to authenticate the requesting device in accordance with the challenge response scheme described below. It will be understood that the authenticating device may only initiate the challenge response scheme if the authenticating device has been secured by a device password (stored_password). In order to determine if a requesting device needs to be authenticated, the authenticating device may check for the presence of a hash of the device password H(stored_password) in a memory of the authenticating device. In other implementations, the authentication device may check for a flag indicating whether the device has been secured. When the authenticating device detects a connection request, it generates a Challenge c to issue to the requesting device. The Challenge c may be a group of bits that have been randomly generated by the authenticating device. Alternatively, the numbers of bits used in the Challenge c may also be randomized. The authenticating device may use a hardware-based random number generator or a software-based random number generator to generate the

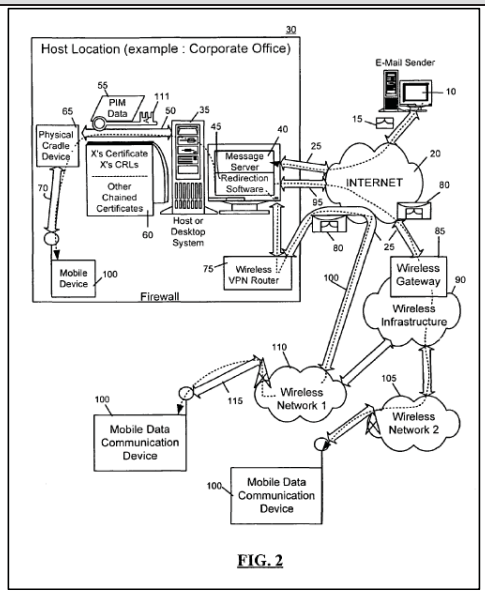
’619 Patent – Claim 33	Brown
	random Challenge c. The requesting device prompts the user of the requesting device for a password user_password. This password is hashed, using known hashing functions such as SHA-1, to create H(user_password) which is then combined with the Challenge c received from the authenticating device. In the preferred embodiment, the Challenge c and the hash of the password H(user_password) are concatenated together. It is understood that there are different ways in which to combine the two values. This combination of the Challenge c and the hash of the password H(user_password) is further hashed in order to generate a requesting encryption key kr=H(c‖H(user_password)) that is used in creating a response r to the challenge issued by the authenticating device. The response r is generated by encrypting the password user_password using known techniques such as AES or TripleDES. In some implementations, the response r may also be generated by applying the XOR function to the requesting encryption key kr and the password user_password. The response r is then transmitted to the authenticating device. The authenticating device determines an authenticating encryption key ka by following a process similar to that followed by the requesting device. The authenticating device combines the stored hash of the device password H(stored_password) with the randomly generated Challenge c, and then generates a hash of the combination, in order to generate the authenticating encryption key ka=H(c‖H(stored_password)). The authenticating encryption key ka is used to decrypt the response r received from the requesting device. A hash of the decrypted response H(decrypted_response) is then compared to the stored hash of the device password H(stored_password). If the two hashes match, then the decrypted response was the correct device password. Thus the authenticating device has authenticated the requesting device. The authenticating device is also in possession of the device password for use in operations that require the device password. If the two hashes do not match, then the user did not provide the correct password, and the authenticating

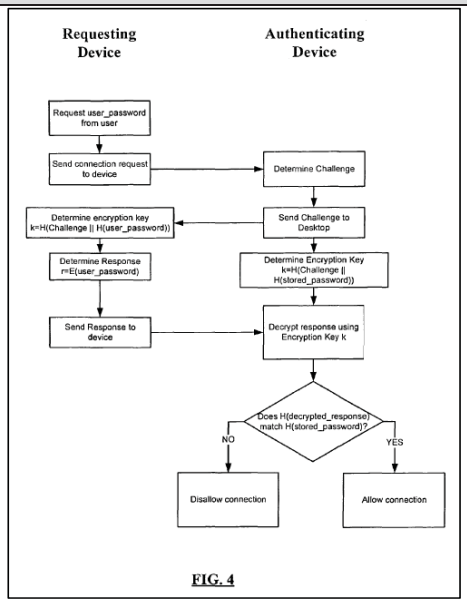
’619 Patent – Claim 33	Brown
	device rejects the connection request from the requesting device, and thereby disallows the connection. In a further embodiment, the device password is concatenated with a random salt s, then hashed and stored in the memory of the authenticating device together with s. Therefore the authenticating device stores (s, H(s‖stored_password)). When the challenge c is transmitted to the requesting device, the salt s is likewise transmitted, and the requesting device then hashes a concatenation of s and user_password to generate an authenticating encrypting key kr=H(c‖H(s‖user_password)) using the process described above. Once the response r is transmitted to the authenticating device, the authenticating device determines an authenticating encryption key ka=H(c‖H(s‖stored_password)) by following a process similar to that described above. The authenticating encryption key ka is used to decrypt the response r received from the requesting device. A hash of the decrypted response H(decrypted_response) is then compared to the stored hash of the salted device password H(s‖stored_password). If the two hashes match, then the decrypted response was the correct device password.” Brown at 8:16-9:18. “The mobile device 100 may be manually synchronized with a host system by placing the device 100 in an interface cradle, which couples the serial port 330 of the mobile device 100 to the serial port of a computer system or device. The serial port 330 may also be used to enable a user to set preferences through an external device or software application, or to download other application modules 324N for installation. This wired download path may be used to load an encryption key onto the device, which is a more secure method than exchanging encryption information via the wireless network 319. Interfaces for other wired download paths may be provided in the mobile device 100, in addition to or instead of the serial port 330. For example, a USB port would provide an interface to a similarly equipped personal computer.” Brown at 12:46-61.

’619 Patent – Claim 33	Brown
	Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

’619 Patent – Claim 36	Brown
[36] The device of claim 22, wherein a control message is received from the remote device upon user interaction with the message.	Brown discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22pre]-[22h], *above*.

’619 Patent – Claim 36	Brown
	 FIG. 1 Brown, Fig. 1.

’619 Patent – Claim 36	Brown
	 FIG. 2 Brown, Fig. 2.

’619 Patent – Claim 36	Brown
	 FIG. 4 Brown, Fig. 4. “A challenge response scheme authenticates a requesting device by an authenticating device. The authenticating device generates and issues a challenge to the requesting device. The requesting device combines the challenge with a hash of a password provided by a user, and the combination is further hashed in order to generate a requesting encryption key used to encrypt the user supplied password. The encrypted user supplied password is sent to the authenticating device as a response to the issued challenge. The authenticating device generates an authenticating encryption key by generating the hash of a

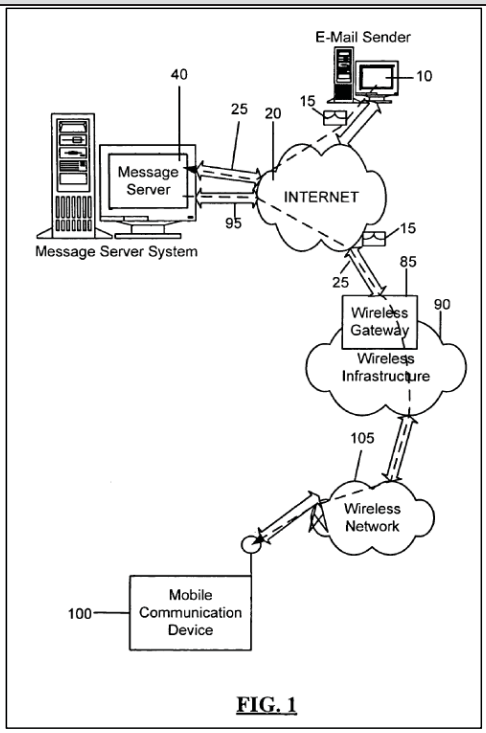
’619 Patent – Claim 36	Brown
	combination of the challenge and a stored hash of an authenticating device password. The authenticating encryption key is used to decrypt the response in order to retrieve the user-supplied password. If the user-supplied password hash matches the stored authenticating device password hash, the requesting device is authenticated and the authenticating device is in possession of the password.” Brown at ABSTRACT; Brown at SUMMARY. “FIG. 4 illustrates a challenge response scheme in accordance with a preferred embodiment of the present invention. In the preferred embodiment, a requesting device, such as the desktop system 35, is connected to an authenticating device, such as mobile device 10, using a communications link, such as a universal serial bus (USB) link, through which the requesting device may send a connection request. The connection request may be in the form of a software request sent to the authenticating device, or the detection of a change in a hardware state of the communications link. The authenticating device detects that a connection is being requested, and proceeds to authenticate the requesting device in accordance with the challenge response scheme described below. It will be understood that the authenticating device may only initiate the challenge response scheme if the authenticating device has been secured by a device password (stored_password). In order to determine if a requesting device needs to be authenticated, the authenticating device may check for the presence of a hash of the device password H(stored_password) in a memory of the authenticating device. In other implementations, the authentication device may check for a flag indicating whether the device has been secured. When the authenticating device detects a connection request, it generates a Challenge c to issue to the requesting device. The Challenge c may be a group of bits that have been randomly generated by the authenticating device. Alternatively, the numbers of bits used in the Challenge c may also be randomized. The authenticating device may use a hardware-based random number generator or a software-based random number generator to generate the

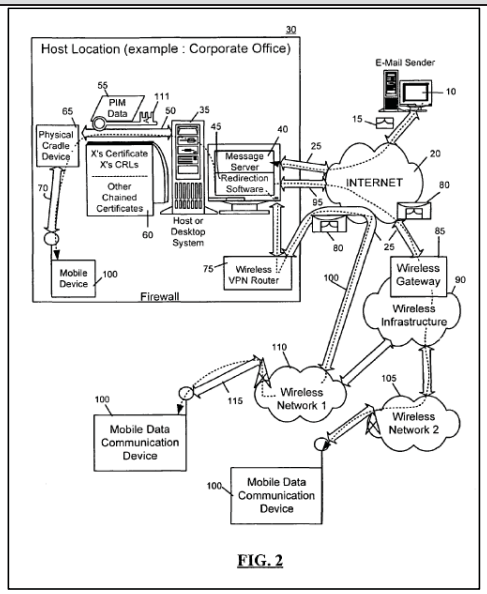
’619 Patent – Claim 36	Brown
	random Challenge c. The requesting device prompts the user of the requesting device for a password user_password. This password is hashed, using known hashing functions such as SHA-1, to create H(user_password) which is then combined with the Challenge c received from the authenticating device. In the preferred embodiment, the Challenge c and the hash of the password H(user_password) are concatenated together. It is understood that there are different ways in which to combine the two values. This combination of the Challenge c and the hash of the password H(user_password) is further hashed in order to generate a requesting encryption key kr=H(c‖H(user_password)) that is used in creating a response r to the challenge issued by the authenticating device. The response r is generated by encrypting the password user_password using known techniques such as AES or TripleDES. In some implementations, the response r may also be generated by applying the XOR function to the requesting encryption key kr and the password user_password. The response r is then transmitted to the authenticating device. The authenticating device determines an authenticating encryption key ka by following a process similar to that followed by the requesting device. The authenticating device combines the stored hash of the device password H(stored_password) with the randomly generated Challenge c, and then generates a hash of the combination, in order to generate the authenticating encryption key ka=H(c‖H(stored_password)). The authenticating encryption key ka is used to decrypt the response r received from the requesting device. A hash of the decrypted response H(decrypted_response) is then compared to the stored hash of the device password H(stored_password). If the two hashes match, then the decrypted response was the correct device password. Thus the authenticating device has authenticated the requesting device. The authenticating device is also in possession of the device password for use in operations that require the device password. If the two hashes do not match, then the user did not provide the correct password, and the authenticating

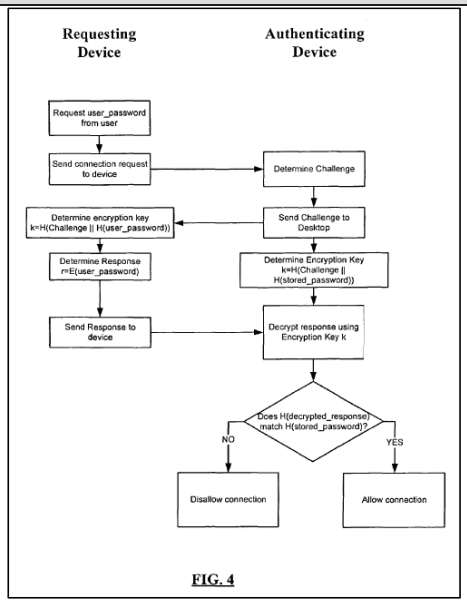
’619 Patent – Claim 36	Brown
	device rejects the connection request from the requesting device, and thereby disallows the connection. In a further embodiment, the device password is concatenated with a random salt s, then hashed and stored in the memory of the authenticating device together with s. Therefore the authenticating device stores (s, H(s‖stored_password)). When the challenge c is transmitted to the requesting device, the salt s is likewise transmitted, and the requesting device then hashes a concatenation of s and user_password to generate an authenticating encrypting key kr=H(c‖H(s‖user_password)) using the process described above. Once the response r is transmitted to the authenticating device, the authenticating device determines an authenticating encryption key ka=H(c‖H(s‖stored_password)) by following a process similar to that described above. The authenticating encryption key ka is used to decrypt the response r received from the requesting device. A hash of the decrypted response H(decrypted_response) is then compared to the stored hash of the salted device password H(s‖stored_password). If the two hashes match, then the decrypted response was the correct device password.” Brown at 8:16-9:18. “The mobile device 100 may be manually synchronized with a host system by placing the device 100 in an interface cradle, which couples the serial port 330 of the mobile device 100 to the serial port of a computer system or device. The serial port 330 may also be used to enable a user to set preferences through an external device or software application, or to download other application modules 324N for installation. This wired download path may be used to load an encryption key onto the device, which is a more secure method than exchanging encryption information via the wireless network 319. Interfaces for other wired download paths may be provided in the mobile device 100, in addition to or instead of the serial port 330. For example, a USB port would provide an interface to a similarly equipped personal computer.” Brown at 12:46-61.

’619 Patent – Claim 36	Brown
	Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

’619 Patent – Claim 37	Brown
[37pre] 37. A method for sharing a messaging account, the method comprising:	To the extent the preamble is limiting, Brown discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:

’619 Patent – Claim 37	Brown
	 FIG. 1 Brown, Fig. 1.

’619 Patent – Claim 37	Brown
	 Brown, Fig. 2.

’619 Patent – Claim 37	Brown
	 FIG. 4 Brown, Fig. 4. “FIG. 1 is an overview of an example communication system in which a wireless communication device may be used. One skilled in the art will appreciate that there may be hundreds of different topologies, but the system shown in FIG. 1 helps demonstrate the operation of the encoded message processing systems and methods described in the present application. There may also be many message senders and recipients. The simple system shown in FIG. 1 is for illustrative purposes only, and shows perhaps the most prevalent Internet e-mail environment where security is not generally used. FIG. 1 shows

’619 Patent – Claim 37	Brown
	an e-mail sender 10, the Internet 20, a message server system 40, a wireless gateway 85, wireless infrastructure 90, a wireless network 105 and a mobile communication device 100.” Brown at 4:49-62. “FIG. 2 is a block diagram of a further example communication system including multiple networks and multiple mobile communication devices. The system of FIG. 2 is substantially similar to the FIG. 1 system, but includes a host system 30 , a redirection program 45, a mobile device cradle 65, a wireless virtual private network (VPN) router 75, an additional wireless network 110 and multiple mobile communication devices 100. As described above in conjunction with FIG. 1, FIG. 2 represents an overview of a sample network topology. Although the encoded message processing systems and methods described herein may be applied to networks having many different topologies, the network of FIG. 2 is useful in understanding an automatic e-mail redirection system mentioned briefly above.” Brown at 6:15-27. “The central host system 30 will typically be a corporate office or other LAN, but may instead be a home office computer or some other private system where mail messages are being exchanged. Within the host system 30 is the message server 40, running on some computer within the firewall of the host system, that acts as the main interface for the host system to exchange e-mail with the Internet 20. In the system of FIG. 2, the redirection program 45 enables redirection of data items from the server 40 to a mobile communication device 100. Although the redirection program 45 is shown to reside on the same machine as the message server 40 for ease of presentation, there is no requirement that it must reside on the message server. The redirection program 45 and the message server 40 are designed to co-operate and interact to allow the pushing of information to mobile devices 100. In this installation, the redirection program 45 takes confidential and non-confidential corporate information for a specific user and redirects it out through the corporate firewall to mobile devices 100.” Brown at 6:29-47.

’619 Patent – Claim 37	Brown
	“As another example, the systems and methods disclosed herein may be used with many different computers and devices, such as a wireless mobile communications device shown in FIG. 5. With reference to FIG. 5, the mobile device 100 is a dual-mode mobile device and includes a transceiver 311, a microprocessor 338, a display 322, non-volatile memory 324, random access memory (RAM) 326, one or more auxiliary input/output (I/O) devices 328, a serial port 330, a keyboard 332, a speaker 334, a microphone 336, a short-range wireless communications sub-system 340, and other device sub-systems 342.” Brown at 9:46-56. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[37a] authenticating a device for access to the messaging account;	Brown discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22h], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

'619 Patent – Claim 37	Brown
[37b] optically receiving information including a displayed service activation code from a remote device;	Brown discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22c], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[37c] registering the remote device for access to the messaging account using the service activation code;	Brown discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22d], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[37d] receiving a message for the messaging account;	Brown discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22e], above. Furthermore, this claim element is obvious in light of this reference itself, when

'619 Patent – Claim 37	Brown
	combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[37e] encrypting the message using an encryption key; and	Brown discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22f], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[37f] sending the message to the remote device.	Brown discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22g], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine

'619 Patent – Claim 37	Brown
	references and additional details may be found in the Cover Pleading and Exhibit 619-B.

'619 Patent – Claim 38	Brown
[38] The method of claim 37, wherein the information including the service activation code is received by the device in response to user input at the remote device.	Brown discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [23], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

'619 Patent – Claim 39	Brown
[39] The method of claim 38, wherein the information including the service activation code is received by the device in an off-line communication.	Brown discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [24], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill

'619 Patent – Claim 39	Brown
	in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

'619 Patent – Claim 40	Brown
[40] The method of claim 39, wherein the off-line communication prevents eavesdropping of the service activation code.	Brown discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [26], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

'619 Patent – Claim 41	Brown
[41] The method of claim 37, wherein the authentication of the device relies on the authentication of the messaging system.	Brown discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [27], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in

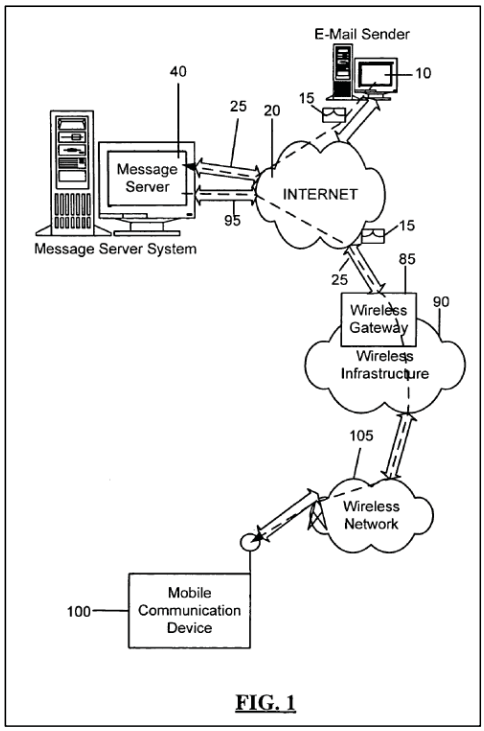
’619 Patent – Claim 41	Brown
	Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

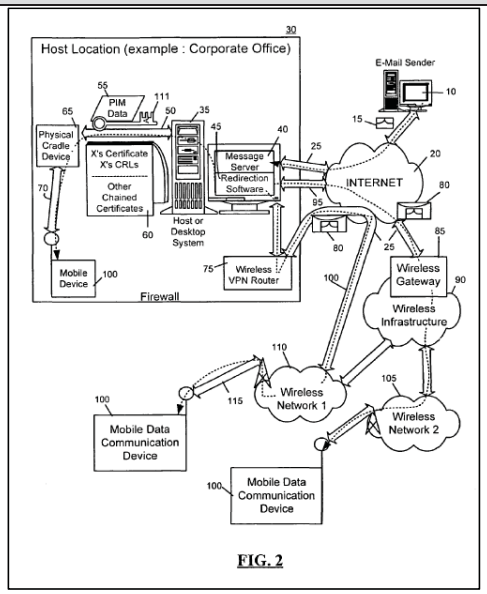
’619 Patent – Claim 42	Brown
[42] The method of claim 41, wherein the authentication of the messaging system includes a username and password.	Brown discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [28], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

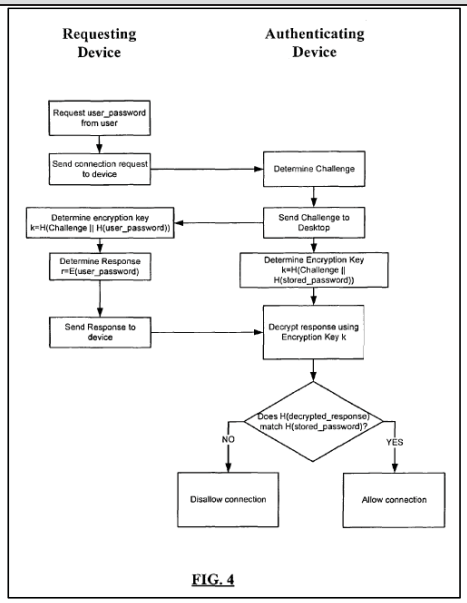
’619 Patent – Claim 46	Brown
[46] The method of claim 37, wherein the encryption key is closely related to the service activation code.	Brown discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:

'619 Patent – Claim 46	Brown
	See [32], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

'619 Patent – Claim 50	Brown
[50] The method of claim 37, wherein a control message is received from the remote device upon user interaction with the message.	Brown discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [36], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

’619 Patent – Claim 51	Brown
[51pre] 51. A non-transient computer-readable medium containing program instructions for causing a device to perform a method, the method comprising:	To the extent the preamble is limiting, Brown discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:  FIG. 1 Brown, Fig. 1.

’619 Patent – Claim 51	Brown
	 FIG. 2 Brown, Fig. 2.

’619 Patent – Claim 51	Brown
	 FIG. 4 Brown, Fig. 4. “FIG. 1 is an overview of an example communication system in which a wireless communication device may be used. One skilled in the art will appreciate that there may be hundreds of different topologies, but the system shown in FIG. 1 helps demonstrate the operation of the encoded message processing systems and methods described in the present application. There may also be many message senders and recipients. The simple system shown in FIG. 1 is for illustrative purposes only, and shows perhaps the most prevalent Internet e-mail environment where security is not generally used. FIG. 1 shows

’619 Patent – Claim 51	Brown
	an e-mail sender 10, the Internet 20, a message server system 40, a wireless gateway 85, wireless infrastructure 90, a wireless network 105 and a mobile communication device 100.” Brown at 4:49-62. “FIG. 2 is a block diagram of a further example communication system including multiple networks and multiple mobile communication devices. The system of FIG. 2 is substantially similar to the FIG. 1 system, but includes a host system 30 , a redirection program 45, a mobile device cradle 65, a wireless virtual private network (VPN) router 75, an additional wireless network 110 and multiple mobile communication devices 100. As described above in conjunction with FIG. 1, FIG. 2 represents an overview of a sample network topology. Although the encoded message processing systems and methods described herein may be applied to networks having many different topologies, the network of FIG. 2 is useful in understanding an automatic e-mail redirection system mentioned briefly above.” Brown at 6:15-27. “The central host system 30 will typically be a corporate office or other LAN, but may instead be a home office computer or some other private system where mail messages are being exchanged. Within the host system 30 is the message server 40, running on some computer within the firewall of the host system, that acts as the main interface for the host system to exchange e-mail with the Internet 20. In the system of FIG. 2, the redirection program 45 enables redirection of data items from the server 40 to a mobile communication device 100. Although the redirection program 45 is shown to reside on the same machine as the message server 40 for ease of presentation, there is no requirement that it must reside on the message server. The redirection program 45 and the message server 40 are designed to co-operate and interact to allow the pushing of information to mobile devices 100. In this installation, the redirection program 45 takes confidential and non-confidential corporate information for a specific user and redirects it out through the corporate firewall to mobile devices 100.” Brown at 6:29-47.

’619 Patent – Claim 51	Brown
	“As another example, the systems and methods disclosed herein may be used with many different computers and devices, such as a wireless mobile communications device shown in FIG. 5. With reference to FIG. 5, the mobile device 100 is a dual-mode mobile device and includes a transceiver 311, a microprocessor 338, a display 322, non-volatile memory 324, random access memory (RAM) 326, one or more auxiliary input/output (I/O) devices 328, a serial port 330, a keyboard 332, a speaker 334, a microphone 336, a short-range wireless communications sub-system 340, and other device sub-systems 342.” Brown at 9:46-56. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[51a] optically receiving information including a displayed service activation code from a remote device;	Brown discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22c], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

'619 Patent – Claim 51	Brown
[51b] registering the remote device for access to a messaging account using the service activation code;	Brown discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22d], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[51c] receiving a message for the messaging account;	Brown discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22e], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[51d] encrypting the message using an encryption key; and	Brown discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22f], above. Furthermore, this claim element is obvious in light of this reference itself, when

'619 Patent – Claim 51	Brown
	combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[51e] sending the message to the remote device,	Brown discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22g], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[51f] wherein the device is authenticated to access the messaging account.	Brown discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22h], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine

'619 Patent – Claim 51	Brown
	references and additional details may be found in the Cover Pleading and Exhibit 619-B.

'619 Patent – Claim 52	Brown
[52] The method of claim 51, wherein a control message is received from the remote device upon user interaction with the message.	Brown discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [36], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

EXHIBIT 619-A04

Invalidity Contentions for U.S. Patent No. 10,027,619 ("the '619 patent")

Based on: U.S. Patent No. 7,849,313 to Klassen et al. ("Klassen")

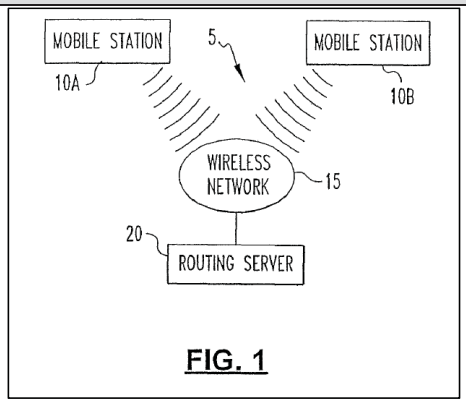
Based on SEVEN's apparent positions as to the scope of the patent's claims, as best they can be deciphered, the reference(s) charted below anticipate(s) or at least render(s) obvious the identified claims. The portions of the prior art reference cited below are not exhaustive but are exemplary in nature. Where Apple identifies a portion of the prior art reference's text, the identification should be understood as referencing any corresponding figure or diagram, and vice versa.

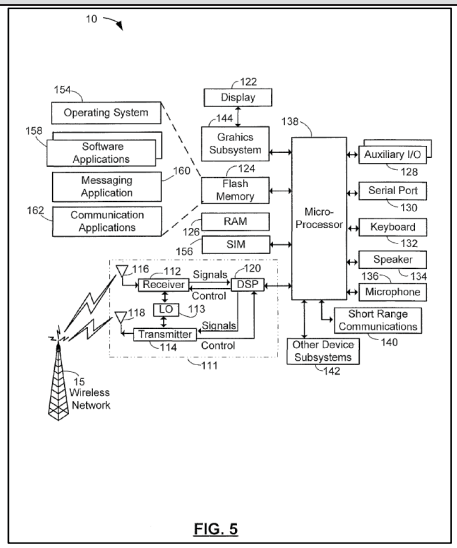
This disclosure is not an admission that Apple concedes any claim construction implied or suggested by SEVEN's apparent positions as to the scope of the patent's claims, nor is it an admission by Apple that any of its products are covered by or infringe the patent's claims, particularly when they are properly construed and applied. Apple is not taking any claim construction positions through this disclosure, including whether the preamble is a limitation.

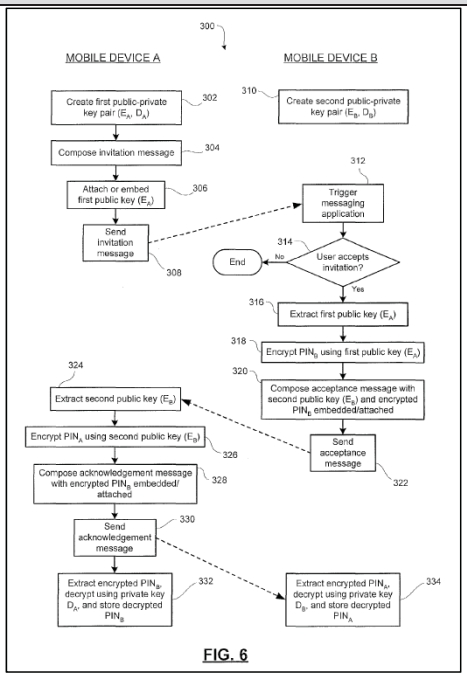
Apple reserves the right to rely on additional citations or sources of evidence that also may be applicable, or that may become applicable in light of claim construction, changes in SEVEN's infringement contentions, and/or information obtained during discovery as the case progresses. Apple further reserves the right to amend or supplement this claim chart at a later date as more fully set forth in the Invalidity Contentions.

Klassen qualifies as prior art under at least pre-AIA 35 U.S.C. § 102(e). Klassen is a U.S. Patent that was filed on December 23, 2008, published on June 25, 2009, and issued on December 7, 2010.

'619 Patent – Claim 22	Klassen
[22pre] A device comprising:	To the extent the preamble is limiting, Klassen discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:

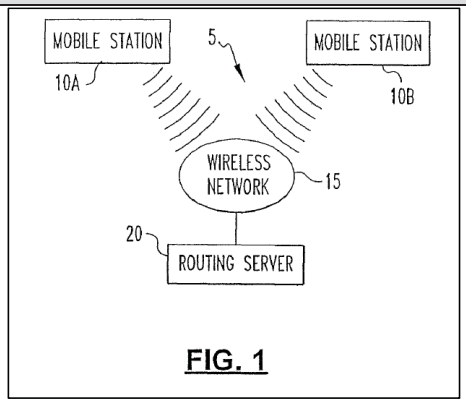
’619 Patent – Claim 22	Klassen
	 FIG. 1 Klassen, Fig. 1.

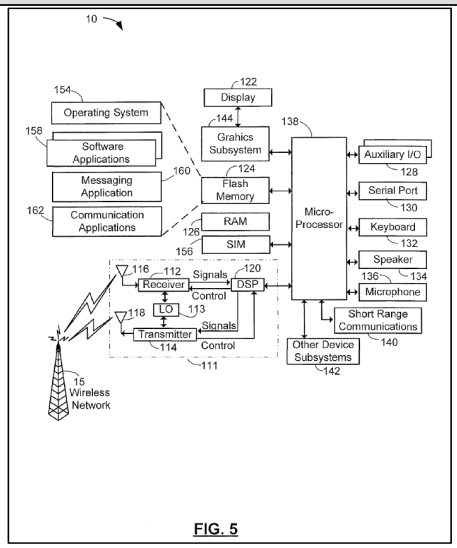
’619 Patent – Claim 22	Klassen
	 FIG. 5 Klassen, Fig. 5.

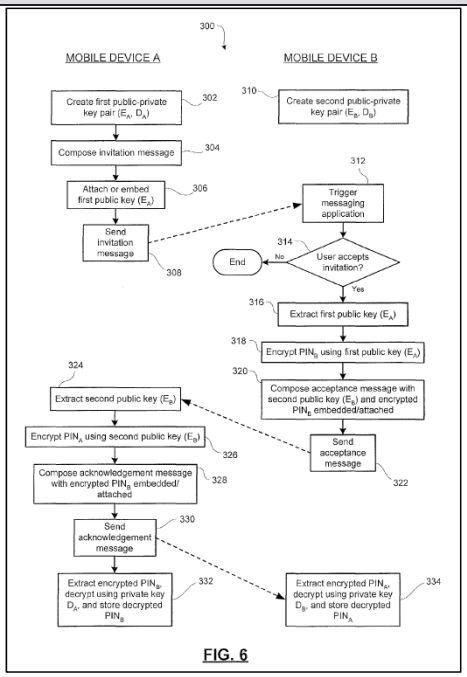
’619 Patent – Claim 22	Klassen
	 FIG. 6 Klassen, Fig. 6. “A system and methods providing immediate peer-to-peer messaging between mobile devices in a wireless system. An invitation architecture is disclosed which enables the exchange of personal identification numbers (PINs) without requiring a user to directly access or provide his or her PIN. A messaging application encrypts its associated PIN before providing it to a messaging application on another mobile device through an existing communication

'619 Patent – Claim 22	Klassen
	application. An invitation process for exchanging encrypted PINs involves receiving an invitation containing a question, obtaining user input of an answer, and transmitting the answer back to the sender with an encrypted PIN. The sender confirms the received answer is correct and replies with its encrypted PIN." Klassen at ABSTRACT. "The present application describes a system and a method that provide for immediate peer-to-peer messaging between mobile devices. The system and method provide increased security by maintaining the secrecy of the underlying address identity of each user of a mobile device in the system. An invitation architecture is disclosed which enables the exchange of personal identification numbers (PINs) without requiring a user to directly access or provide his or her PIN. A messaging application encrypts its associated PIN before providing it to a messaging application on another mobile device through an existing communication application. The invitation architecture automatically manages the encryption, any requisite key exchanges, the composition of invitation and acceptance messages, and the decryption and storage of PINs." Klassen at 2:46-59. "Referring now to the drawings, FIG. 1 is a block diagram of a system 5 for enabling immediate peer-to-peer messaging. System 5 includes a plurality of mobile stations 10, such as mobile devices 10A and 10B shown in FIG. 1, which may be any type of wireless mobile electronic communications device such as a cell phone, a smart phone, a personal data assistant (PDA), a pager, a handheld computer or a phone-enabled laptop computer, to name a few. As is known, each mobile device 10 may be provided with various applications, including, without limitation, one or more currently existing applications that enable communication with other mobile devices 10, such as a wireless telephone application, an email application, a short message service (SMS) application, a multimedia messaging service (MMS) application, an enhanced message service (EMS) application, and other Internet enable messaging applications (each of which may be referred to herein as an "existing

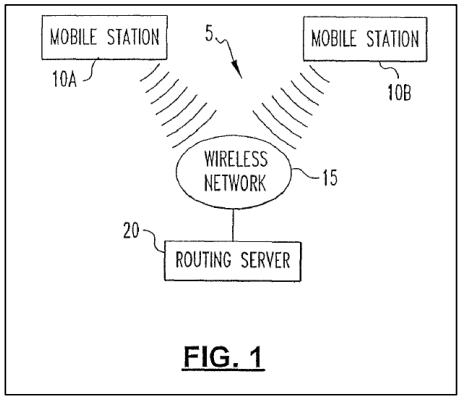
’619 Patent – Claim 22	Klassen
	communications application”). In addition, each mobile device 10 is provided with an application that implements the peer-to-peer messaging solution described herein (referred to herein as the “messaging application”). The term “application” as used herein shall include one or more programs, routines, subroutines, function calls or other type of software or firmware and the like, alone or in combination. System 5 also includes wireless network 15, which may be any wireless communications network or combination of interconnected networks, including, without limitation, Mobiltex™, DataTAC™, AMPS, TDMA, CDMA, GSM/GPRS, PCS, EDGE, UMTS or CDPD. As is known, wireless network 15 includes a plurality of base stations that perform radio frequency (RF) protocols to support data and voice exchanges with mobile devices 10A and 10B. Routing server 20 is coupled to wireless network 15. Routing server 20 may be any type of routing equipment capable of routing data packets, including, without limitation, a TCP/IP router such as those sold by Cisco Systems, Inc. of San Jose, Calif., or a network address translation server (NAT).” Klassen at 5:46-6:15. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[22a] a radio;	Klassen discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:

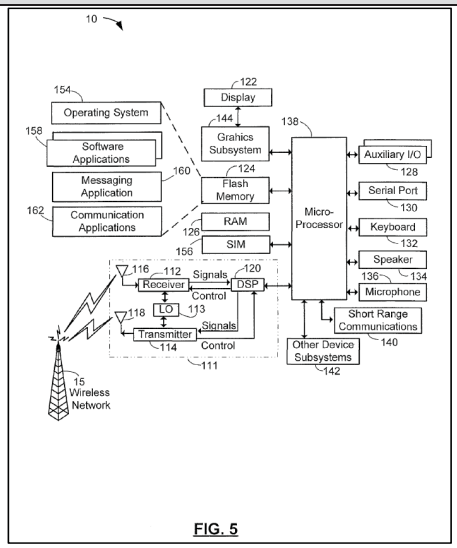
’619 Patent – Claim 22	Klassen
	 FIG. 1 Klassen, Fig. 1.

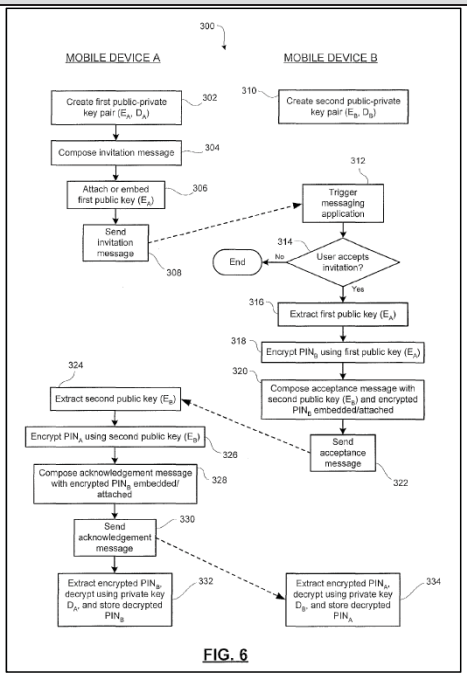
’619 Patent – Claim 22	Klassen
	 FIG. 5 Klassen, Fig. 5.

’619 Patent – Claim 22	Klassen
	 FIG. 6 Klassen, Fig. 6. “Referring now to the drawings, FIG. 1 is a block diagram of a system 5 for enabling immediate peer-to-peer messaging. System 5 includes a plurality of mobile stations 10, such as mobile devices 10A and 10B shown in FIG. 1, which may be any type of wireless mobile electronic communications device such as a cell phone, a smart phone, a personal data assistant (PDA), a pager, a handheld computer or a phone-enabled laptop computer, to name a few. As is

’619 Patent – Claim 22	Klassen
	known, each mobile device 10 may be provided with various applications, including, without limitation, one or more currently existing applications that enable communication with other mobile devices 10, such as a wireless telephone application, an email application, a short message service (SMS) application, a multimedia messaging service (MMS) application, an enhanced message service (EMS) application, and other Internet enable messaging applications (each of which may be referred to herein as an “existing communications application”). In addition, each mobile device 10 is provided with an application that implements the peer-to-peer messaging solution described herein (referred to herein as the “messaging application”). The term “application” as used herein shall include one or more programs, routines, subroutines, function calls or other type of software or firmware and the like, alone or in combination. System 5 also includes wireless network 15, which may be any wireless communications network or combination of interconnected networks, including, without limitation, Mobiltex™, DataTAC™, AMPS, TDMA, CDMA, GSM/GPRS, PCS, EDGE, UMTS or CDPD. As is known, wireless network 15 includes a plurality of base stations that perform radio frequency (RF) protocols to support data and voice exchanges with mobile devices 10A and 10B. Routing server 20 is coupled to wireless network 15. Routing server 20 may be any type of routing equipment capable of routing data packets, including, without limitation, a TCP/IP router such as those sold by Cisco Systems, Inc. of San Jose, Calif., or a network address translation server (NAT).” Klassen at 5:46-6:15. “The device 10 includes a communication subsystem 111, including a receiver 112, a transmitter 114, and associated components such as one or more, preferably embedded or internal, antenna elements 116 and 118, and a processing module such as a digital signal processor (DSP) 120. In some embodiments, the communication subsystem includes local oscillator(s) (LO) 113, and in some embodiments the communication subsystem 111 and a microprocessor 138 share an oscillator. As will be apparent to those skilled in the field of communications, the particular design of the communication

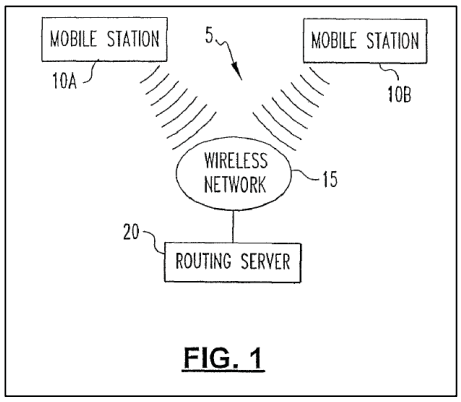
’619 Patent – Claim 22	Klassen
	subsystem 111 will be dependent upon the communication network in which the device 10 is intended to operate.” Klassen at 8:41-53. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[22b] a processor and memory containing instructions executable by the processor whereby the device is operable to:	Klassen discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:  FIG. 1 Klassen, Fig. 1.

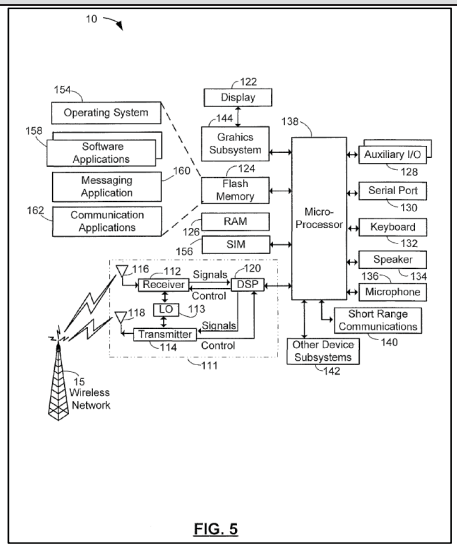
’619 Patent – Claim 22	Klassen
	 FIG. 5 Klassen, Fig. 5.

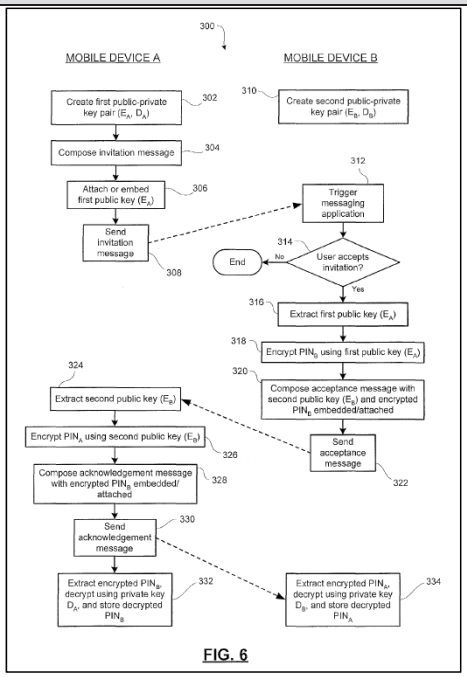
’619 Patent – Claim 22	Klassen
	 FIG. 6 Klassen, Fig. 6. “A system and methods providing immediate peer-to-peer messaging between mobile devices in a wireless system. An invitation architecture is disclosed which enables the exchange of personal identification numbers (PINs) without requiring a user to directly access or provide his or her PIN. A messaging application encrypts its associated PIN before providing it to a messaging application on another mobile device through an existing communication

’619 Patent – Claim 22	Klassen
	application. An invitation process for exchanging encrypted PINs involves receiving an invitation containing a question, obtaining user input of an answer, and transmitting the answer back to the sender with an encrypted PIN. The sender confirms the received answer is correct and replies with its encrypted PIN.” Klassen at ABSTRACT. “Referring now to the drawings, FIG. 1 is a block diagram of a system 5 for enabling immediate peer-to-peer messaging. System 5 includes a plurality of mobile stations 10, such as mobile devices 10A and 10B shown in FIG. 1, which may be any type of wireless mobile electronic communications device such as a cell phone, a smart phone, a personal data assistant (PDA), a pager, a handheld computer or a phone-enabled laptop computer, to name a few. As is known, each mobile device 10 may be provided with various applications, including, without limitation, one or more currently existing applications that enable communication with other mobile devices 10, such as a wireless telephone application, an email application, a short message service (SMS) application, a multimedia messaging service (MMS) application, an enhanced message service (EMS) application, and other Internet enable messaging applications (each of which may be referred to herein as an “existing communications application”). In addition, each mobile device 10 is provided with an application that implements the peer-to-peer messaging solution described herein (referred to herein as the “messaging application”). The term “application” as used herein shall include one or more programs, routines, subroutines, function calls or other type of software or firmware and the like, alone or in combination. System 5 also includes wireless network 15, which may be any wireless communications network or combination of interconnected networks, including, without limitation, Mobiltex™, DataTAC™, AMPS, TDMA, CDMA, GSM/GPRS, PCS, EDGE, UMTS or CDPD. As is known, wireless network 15 includes a plurality of base stations that perform radio frequency (RF) protocols to support data and voice exchanges with mobile devices 10A and 10B. Routing server 20 is coupled to wireless network 15. Routing server 20 may be any type of routing equipment

’619 Patent – Claim 22	Klassen
	capable of routing data packets, including, without limitation, a TCP/IP router such as those sold by Cisco Systems, Inc. of San Jose, Calif., or a network address translation server (NAT).” Klassen at 5:46-6:15. “The device 10 includes the microprocessor 138 that controls the overall operation of the device. The microprocessor 138 interacts with the communications subsystem 111 and also interacts with further device subsystems such as the graphics subsystem 144, flash memory 124, random access memory (RAM) 126, a subscriber identity module (SIM) 156, auxiliary input/output (I/O) subsystems 128, serial port 130, keyboard or keypad 132, speaker 134, microphone 136, a short-range communications subsystem 140, and any other device subsystems generally designated as 142. The graphics subsystem 144 interacts with the display 122 and renders graphics or text upon the display 122. Operating system software 154 and various software applications 158 used by the microprocessor 138 are, in one example embodiment, stored in a persistent store such as flash memory 124 or similar storage element. Those skilled in the art will appreciate that the operating system 154, software applications 158, or parts thereof, may be temporarily loaded into a volatile store such as RAM 126. It is contemplated that received communication signals may also be stored to RAM 126.” Klassen at 8:64-9:17. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[22c] optically receive information including a	Klassen discloses this claim limitation. For example, see the following

’619 Patent – Claim 22	Klassen
displayed service activation code from a remote device;	passages and/or figures, as well as all related disclosures:  FIG. 1 Klassen, Fig. 1.

’619 Patent – Claim 22	Klassen
	 FIG. 5 Klassen, Fig. 5.

’619 Patent – Claim 22	Klassen
	 FIG. 6 Klassen, Fig. 6. “A system and methods providing immediate peer-to-peer messaging between mobile devices in a wireless system. An invitation architecture is disclosed which enables the exchange of personal identification numbers (PINs) without requiring a user to directly access or provide his or her PIN. A messaging application encrypts its associated PIN before providing it to a messaging application on another mobile device through an existing communication

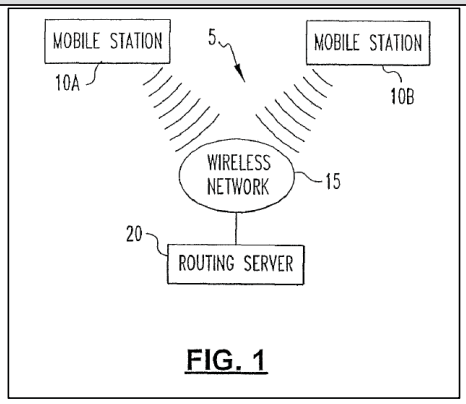
’619 Patent – Claim 22	Klassen
	application. An invitation process for exchanging encrypted PINs involves receiving an invitation containing a question, obtaining user input of an answer, and transmitting the answer back to the sender with an encrypted PIN. The sender confirms the received answer is correct and replies with its encrypted PIN.” Klassen at ABSTRACT. “The present application describes a system and a method that provide for immediate peer-to-peer messaging between mobile devices. The system and method provide increased security by maintaining the secrecy of the underlying address identity of each user of a mobile device in the system. An invitation architecture is disclosed which enables the exchange of personal identification numbers (PINs) without requiring a user to directly access or provide his or her PIN. A messaging application encrypts its associated PIN before providing it to a messaging application on another mobile device through an existing communication application. The invitation architecture automatically manages the encryption, any requisite key exchanges, the composition of invitation and acceptance messages, and the decryption and storage of PINs..” Klassen at 2:46-59. “In one aspect, the present application provides a method of securely exchanging personal identification numbers between a first mobile device and a second mobile device. The mobile devices are used in a system including a wireless network and a routing server coupled to the wireless network. Each mobile device has one or more communications applications and each mobile device further has a messaging application. The first mobile device has a first personal identification number and the second mobile device has a second personal identification number. The method includes the steps of encrypting the first personal identification number, sending the encrypted first personal identification number from the first mobile device to the second mobile device using one of the communication applications, and decrypting the encrypted first personal identification number and storing the first personal identification number in a memory on the second mobile device. The method also includes

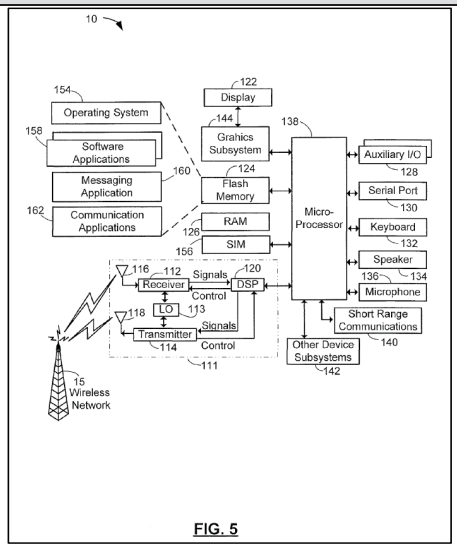
’619 Patent – Claim 22	Klassen
	the steps of encrypting the second personal identification number, sending the encrypted second personal identification number from the second mobile device to the first mobile device using one of the communication applications, and decrypting the encrypted second personal identification number and storing the second personal identification number in a memory on the first mobile device. After this exchange of PINs, peer-to-peer messages are exchanged between the first mobile device and the second mobile device using the messaging applications. Each peer-to-peer message contains one of the personal identification numbers and each peer-to-peer message is routed by the routing server based upon the personal identification numbers..” Klassen at 2:60-3:22. “Each mobile device 10 of system 5 is assigned and stores a unique personal identification number (PIN) . The PIN for each mobile device 10 may be assigned and stored therein when it is manufactured or through its subscriber identity module (SIM). Each PIN is mapped to a network address for the corresponding mobile device 10 on wireless network 15 that enables data to be routed to the mobile device 10. Routing server 20 includes one or more routing tables for routing messages sent by mobile devices 10 based on this mapping. In one exemplary embodiment, the PIN may actually be the network address itself, and in another exemplary embodiment, the PIN may be the phone number of the mobile device 10 or a unique ID such as the mobile subscriber ISDN (MSISDN) for the mobile device 10, and the network address may be an IP address or the like. It will be understood that the term “personal identification number” or “PIN” used herein is not intended to be limited solely to numeric identifiers, but is to be understood broadly and may include alphanumeric identifiers, binary identifiers, or other identifiers that can be used to enable peer-to-peer messaging.” Klassen at 6:16-35. “If the user of mobile device 10B indicates that he or she accepts the invitation and therefore wishes to establish a peer-to-peer messaging session, for example by selecting an “accept” button on the GUI, then the messaging application on

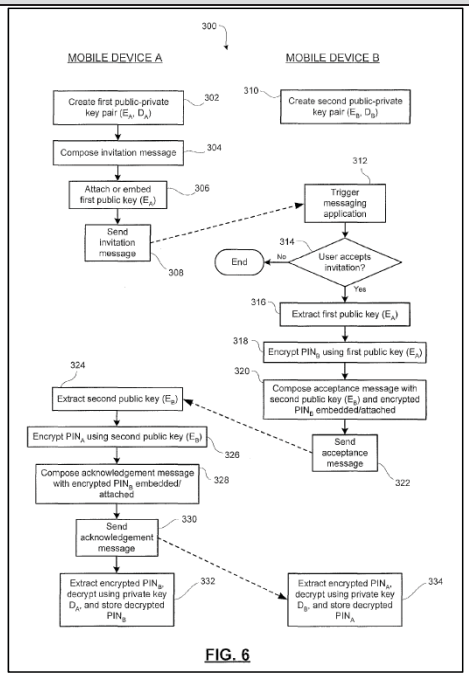
’619 Patent – Claim 22	Klassen
	mobile device 10B causes an acceptance communication to be transmitted to the originating mobile device 10A by way of the appropriate existing communication application. For example, in one embodiment the messaging application causes an acceptance e-mail to be composed and sent using the e-mail application. The messaging application on mobile device 10A is configured to recognize receipt of an acceptance message, like an acceptance e-mail. In addition to, or in conjunction with, exchanging an invitation and acceptance using the existing communication applications, the mobile devices 10A and 10B exchange PINs. In one embodiment, the PIN for mobile device 10B is sent with the acceptance message. In one embodiment, the PIN for mobile device 10A may be sent with either the invitation message or with a subsequent acknowledgement message after receipt of the acceptance message.” Klassen at 7:27-46. “The encrypted PINs may be embedded directly within the messages sent using the existing communication applications or may be attached to the messages. For example, with an e-mail application the encrypted PIN may be attached as a binary file. It will be appreciated that e-mail having a binary file attached may encounter problems in traversing firewalls and spam filters. Accordingly, in another embodiment, the encrypted PIN is embedded directly within the body of the e-mail. In this embodiment, a reader of the e-mail will see the encrypted PIN as a series of incomprehensible text symbols, however the messaging application is configured to extract and decrypt the encrypted PIN. Additional details regarding the exchange of encrypted PINs and related key management and key exchange operations are provided below.” Klassen at 7:60-8:6. “As will be appreciated, once the above steps are complete, mobile device 10A will have the PIN for mobile device 10B, and mobile device 10B will have the PIN for mobile device 10A. Now, if either mobile device 10A or 10B desires to send a peer-to-peer message to the other, it prepares a peer-to-peer message

’619 Patent – Claim 22	Klassen
	using the peer-to-peer messaging application that includes the PIN of the recipient mobile device 10 (10A or 10B, as the case may be), preferably in the message header, along with the message information that is to be sent. The peer-to-peer message is then sent by the mobile device 10 through wireless network 15 to routing server 20. Routing server 20 obtains the PIN from the peer-to-peer message and uses it to determine the network address of the recipient mobile device 10 (10A or 10B, as the case may be) using the routing table(s) stored therein, and sends the message to the recipient mobile device 10 (10A or 10B, as the case may be) through wireless network 15 using the determined network address. Once received, the peer-to-peer message, and in particular the message information contained therein, may be displayed to the user of the recipient mobile device 10 (10A or 10B, as the case may be)..” Klassen at 8:7-27. “The messaging application 160 includes components for performing encryption, decryption, and related key management functions for exchanging PINs. These components may be provided as a part of the invitation and acceptance components or as separate components interacting therewith. These components manage the encryption of a resident PIN, the generation or calculation of any required key values or session keys, the attachment or embedding of encrypted PINs into messages for transmission through one of the existing communication applications 162, and the decryption of encrypted PINs received from other mobile devices 10 through one of the communication applications 162. Further detail regarding encryption, decryption, and key exchange within the context of the invitation architecture is given below..” Klassen at 10:47-62. “Reference is again made to FIGS. 1 and 5. As noted above, in the invitation architecture described in the present application the respective PINs of the mobile devices 10 are covertly exchanged using one of the existing communication applications. A sending mobile device encrypts its PIN prior to transmitting it using the communication application. At the receiving mobile

’619 Patent – Claim 22	Klassen
	device, the received encrypted PIN is decrypted. Through appropriate key management, access to the unencrypted PIN is limited to the messaging applications on the respective two mobile devices. There are a number of encryption and key management techniques that may be employed in various embodiments within the scope of the present application. Moreover, the particular transformation or function that may be used in conjunction with a key value to convert the PIN into an encrypted PIN may include a wide range of cryptographic transformations or functions. Those of ordinary skill in the art will appreciate that a wide range of such functions are known and may be selected, having regard to the processing power and any time constraints associated with a particular application or system.” Klassen at 11:57-12:11 Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[22d] register the remote device for access to a messaging account using the service activation code;	Klassen discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:

’619 Patent – Claim 22	Klassen
	 FIG. 1 Klassen, Fig. 1.

’619 Patent – Claim 22	Klassen
	 FIG. 5 Klassen, Fig. 5.

’619 Patent – Claim 22	Klassen
	 FIG. 6 Klassen, Fig. 6. “A system and methods providing immediate peer-to-peer messaging between mobile devices in a wireless system. An invitation architecture is disclosed which enables the exchange of personal identification numbers (PINs) without requiring a user to directly access or provide his or her PIN. A messaging application encrypts its associated PIN before providing it to a messaging application on another mobile device through an existing communication

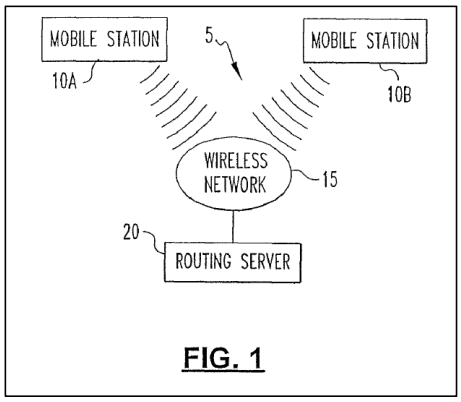
’619 Patent – Claim 22	Klassen
	application. An invitation process for exchanging encrypted PINs involves receiving an invitation containing a question, obtaining user input of an answer, and transmitting the answer back to the sender with an encrypted PIN. The sender confirms the received answer is correct and replies with its encrypted PIN.” Klassen at ABSTRACT. “The present application describes a system and a method that provide for immediate peer-to-peer messaging between mobile devices. The system and method provide increased security by maintaining the secrecy of the underlying address identity of each user of a mobile device in the system. An invitation architecture is disclosed which enables the exchange of personal identification numbers (PINs) without requiring a user to directly access or provide his or her PIN. A messaging application encrypts its associated PIN before providing it to a messaging application on another mobile device through an existing communication application. The invitation architecture automatically manages the encryption, any requisite key exchanges, the composition of invitation and acceptance messages, and the decryption and storage of PINs..” Klassen at 2:46-59. “In one aspect, the present application provides a method of securely exchanging personal identification numbers between a first mobile device and a second mobile device. The mobile devices are used in a system including a wireless network and a routing server coupled to the wireless network. Each mobile device has one or more communications applications and each mobile device further has a messaging application. The first mobile device has a first personal identification number and the second mobile device has a second personal identification number. The method includes the steps of encrypting the first personal identification number, sending the encrypted first personal identification number from the first mobile device to the second mobile device using one of the communication applications, and decrypting the encrypted first personal identification number and storing the first personal identification number in a memory on the second mobile device. The method also includes

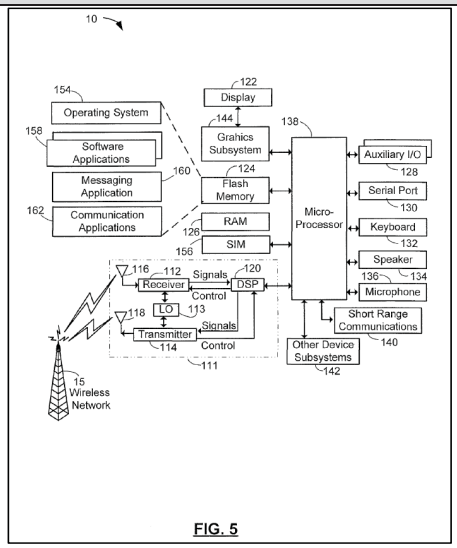
’619 Patent – Claim 22	Klassen
	the steps of encrypting the second personal identification number, sending the encrypted second personal identification number from the second mobile device to the first mobile device using one of the communication applications, and decrypting the encrypted second personal identification number and storing the second personal identification number in a memory on the first mobile device. After this exchange of PINs, peer-to-peer messages are exchanged between the first mobile device and the second mobile device using the messaging applications. Each peer-to-peer message contains one of the personal identification numbers and each peer-to-peer message is routed by the routing server based upon the personal identification numbers..” Klassen at 2:60-3:22. “Each mobile device 10 of system 5 is assigned and stores a unique personal identification number (PIN) . The PIN for each mobile device 10 may be assigned and stored therein when it is manufactured or through its subscriber identity module (SIM). Each PIN is mapped to a network address for the corresponding mobile device 10 on wireless network 15 that enables data to be routed to the mobile device 10. Routing server 20 includes one or more routing tables for routing messages sent by mobile devices 10 based on this mapping. In one exemplary embodiment, the PIN may actually be the network address itself, and in another exemplary embodiment, the PIN may be the phone number of the mobile device 10 or a unique ID such as the mobile subscriber ISDN (MSISDN) for the mobile device 10, and the network address may be an IP address or the like. It will be understood that the term “personal identification number” or “PIN” used herein is not intended to be limited solely to numeric identifiers, but is to be understood broadly and may include alphanumeric identifiers, binary identifiers, or other identifiers that can be used to enable peer-to-peer messaging.” Klassen at 6:16-35. “If the user of mobile device 10B indicates that he or she accepts the invitation and therefore wishes to establish a peer-to-peer messaging session, for example by selecting an “accept” button on the GUI, then the messaging application on

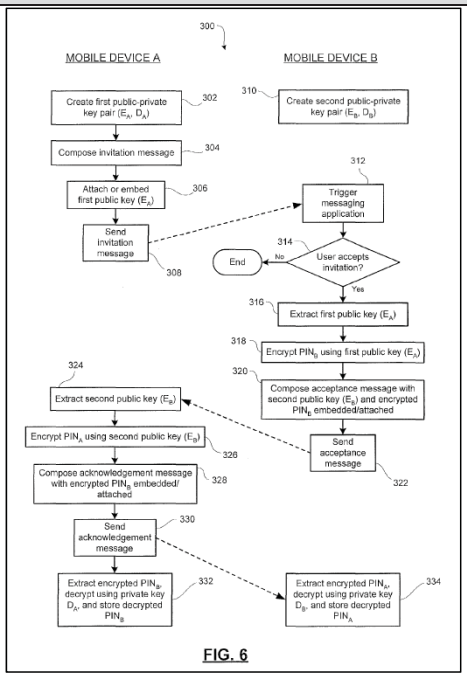
’619 Patent – Claim 22	Klassen
	mobile device 10B causes an acceptance communication to be transmitted to the originating mobile device 10A by way of the appropriate existing communication application. For example, in one embodiment the messaging application causes an acceptance e-mail to be composed and sent using the e-mail application. The messaging application on mobile device 10A is configured to recognize receipt of an acceptance message, like an acceptance e-mail. In addition to, or in conjunction with, exchanging an invitation and acceptance using the existing communication applications, the mobile devices 10A and 10B exchange PINs. In one embodiment, the PIN for mobile device 10B is sent with the acceptance message. In one embodiment, the PIN for mobile device 10A may be sent with either the invitation message or with a subsequent acknowledgement message after receipt of the acceptance message.” Klassen at 7:27-46. “The encrypted PINs may be embedded directly within the messages sent using the existing communication applications or may be attached to the messages. For example, with an e-mail application the encrypted PIN may be attached as a binary file. It will be appreciated that e-mail having a binary file attached may encounter problems in traversing firewalls and spam filters. Accordingly, in another embodiment, the encrypted PIN is embedded directly within the body of the e-mail. In this embodiment, a reader of the e-mail will see the encrypted PIN as a series of incomprehensible text symbols, however the messaging application is configured to extract and decrypt the encrypted PIN. Additional details regarding the exchange of encrypted PINs and related key management and key exchange operations are provided below.” Klassen at 7:60-8:6. “As will be appreciated, once the above steps are complete, mobile device 10A will have the PIN for mobile device 10B, and mobile device 10B will have the PIN for mobile device 10A. Now, if either mobile device 10A or 10B desires to send a peer-to-peer message to the other, it prepares a peer-to-peer message

’619 Patent – Claim 22	Klassen
	using the peer-to-peer messaging application that includes the PIN of the recipient mobile device 10 (10A or 10B, as the case may be), preferably in the message header, along with the message information that is to be sent. The peer-to-peer message is then sent by the mobile device 10 through wireless network 15 to routing server 20. Routing server 20 obtains the PIN from the peer-to-peer message and uses it to determine the network address of the recipient mobile device 10 (10A or 10B, as the case may be) using the routing table(s) stored therein, and sends the message to the recipient mobile device 10 (10A or 10B, as the case may be) through wireless network 15 using the determined network address. Once received, the peer-to-peer message, and in particular the message information contained therein, may be displayed to the user of the recipient mobile device 10 (10A or 10B, as the case may be)..” Klassen at 8:7-27. “The messaging application 160 includes components for performing encryption, decryption, and related key management functions for exchanging PINs. These components may be provided as a part of the invitation and acceptance components or as separate components interacting therewith. These components manage the encryption of a resident PIN, the generation or calculation of any required key values or session keys, the attachment or embedding of encrypted PINs into messages for transmission through one of the existing communication applications 162, and the decryption of encrypted PINs received from other mobile devices 10 through one of the communication applications 162. Further detail regarding encryption, decryption, and key exchange within the context of the invitation architecture is given below..” Klassen at 10:47-62. “Reference is again made to FIGS. 1 and 5. As noted above, in the invitation architecture described in the present application the respective PINs of the mobile devices 10 are covertly exchanged using one of the existing communication applications. A sending mobile device encrypts its PIN prior to transmitting it using the communication application. At the receiving mobile

’619 Patent – Claim 22	Klassen
	device, the received encrypted PIN is decrypted. Through appropriate key management, access to the unencrypted PIN is limited to the messaging applications on the respective two mobile devices. There are a number of encryption and key management techniques that may be employed in various embodiments within the scope of the present application. Moreover, the particular transformation or function that may be used in conjunction with a key value to convert the PIN into an encrypted PIN may include a wide range of cryptographic transformations or functions. Those of ordinary skill in the art will appreciate that a wide range of such functions are known and may be selected, having regard to the processing power and any time constraints associated with a particular application or system.” Klassen at 11:57-12:11 Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[22e] receive a message for the messaging account;	Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[22f] encrypt the message using an encryption	Klassen discloses this claim limitation. For example, see the following

’619 Patent – Claim 22	Klassen
key; and	passages and/or figures, as well as all related disclosures:  FIG. 1 Klassen, Fig. 1.

’619 Patent – Claim 22	Klassen
	 FIG. 5 Klassen, Fig. 5.

’619 Patent – Claim 22	Klassen
	 FIG. 6 Klassen, Fig. 6. “A system and methods providing immediate peer-to-peer messaging between mobile devices in a wireless system. An invitation architecture is disclosed which enables the exchange of personal identification numbers (PINs) without requiring a user to directly access or provide his or her PIN. A messaging application encrypts its associated PIN before providing it to a messaging application on another mobile device through an existing communication

’619 Patent – Claim 22	Klassen
	application. An invitation process for exchanging encrypted PINs involves receiving an invitation containing a question, obtaining user input of an answer, and transmitting the answer back to the sender with an encrypted PIN. The sender confirms the received answer is correct and replies with its encrypted PIN.” Klassen at ABSTRACT. “The present application describes a system and a method that provide for immediate peer-to-peer messaging between mobile devices. The system and method provide increased security by maintaining the secrecy of the underlying address identity of each user of a mobile device in the system. An invitation architecture is disclosed which enables the exchange of personal identification numbers (PINs) without requiring a user to directly access or provide his or her PIN. A messaging application encrypts its associated PIN before providing it to a messaging application on another mobile device through an existing communication application. The invitation architecture automatically manages the encryption, any requisite key exchanges, the composition of invitation and acceptance messages, and the decryption and storage of PINs..” Klassen at 2:46-59. “In one aspect, the present application provides a method of securely exchanging personal identification numbers between a first mobile device and a second mobile device. The mobile devices are used in a system including a wireless network and a routing server coupled to the wireless network. Each mobile device has one or more communications applications and each mobile device further has a messaging application. The first mobile device has a first personal identification number and the second mobile device has a second personal identification number. The method includes the steps of encrypting the first personal identification number, sending the encrypted first personal identification number from the first mobile device to the second mobile device using one of the communication applications, and decrypting the encrypted first personal identification number and storing the first personal identification number in a memory on the second mobile device. The method also includes

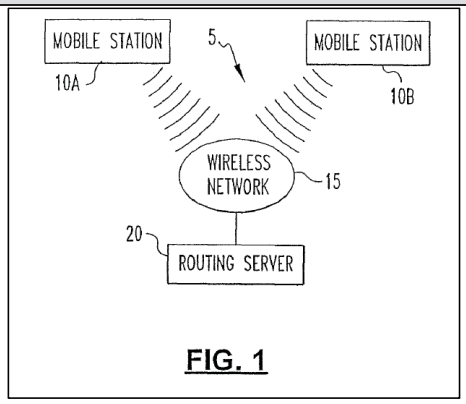
’619 Patent – Claim 22	Klassen
	the steps of encrypting the second personal identification number, sending the encrypted second personal identification number from the second mobile device to the first mobile device using one of the communication applications, and decrypting the encrypted second personal identification number and storing the second personal identification number in a memory on the first mobile device. After this exchange of PINs, peer-to-peer messages are exchanged between the first mobile device and the second mobile device using the messaging applications. Each peer-to-peer message contains one of the personal identification numbers and each peer-to-peer message is routed by the routing server based upon the personal identification numbers..” Klassen at 2:60-3:22. “Each mobile device 10 of system 5 is assigned and stores a unique personal identification number (PIN) . The PIN for each mobile device 10 may be assigned and stored therein when it is manufactured or through its subscriber identity module (SIM). Each PIN is mapped to a network address for the corresponding mobile device 10 on wireless network 15 that enables data to be routed to the mobile device 10. Routing server 20 includes one or more routing tables for routing messages sent by mobile devices 10 based on this mapping. In one exemplary embodiment, the PIN may actually be the network address itself, and in another exemplary embodiment, the PIN may be the phone number of the mobile device 10 or a unique ID such as the mobile subscriber ISDN (MSISDN) for the mobile device 10, and the network address may be an IP address or the like. It will be understood that the term “personal identification number” or “PIN” used herein is not intended to be limited solely to numeric identifiers, but is to be understood broadly and may include alphanumeric identifiers, binary identifiers, or other identifiers that can be used to enable peer-to-peer messaging.” Klassen at 6:16-35. “If the user of mobile device 10B indicates that he or she accepts the invitation and therefore wishes to establish a peer-to-peer messaging session, for example by selecting an “accept” button on the GUI, then the messaging application on

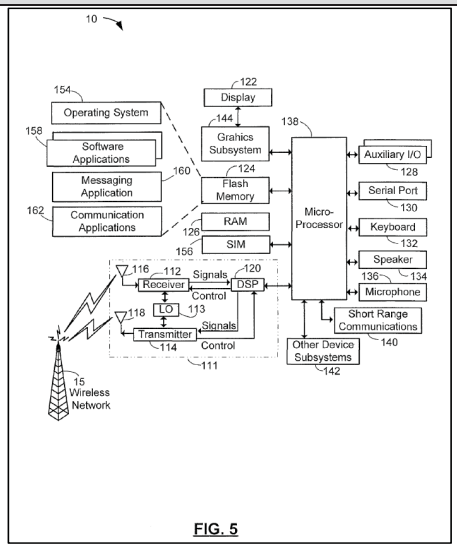
’619 Patent – Claim 22	Klassen
	mobile device 10B causes an acceptance communication to be transmitted to the originating mobile device 10A by way of the appropriate existing communication application. For example, in one embodiment the messaging application causes an acceptance e-mail to be composed and sent using the e-mail application. The messaging application on mobile device 10A is configured to recognize receipt of an acceptance message, like an acceptance e-mail. In addition to, or in conjunction with, exchanging an invitation and acceptance using the existing communication applications, the mobile devices 10A and 10B exchange PINs. In one embodiment, the PIN for mobile device 10B is sent with the acceptance message. In one embodiment, the PIN for mobile device 10A may be sent with either the invitation message or with a subsequent acknowledgement message after receipt of the acceptance message.” Klassen at 7:27-46. “The encrypted PINs may be embedded directly within the messages sent using the existing communication applications or may be attached to the messages. For example, with an e-mail application the encrypted PIN may be attached as a binary file. It will be appreciated that e-mail having a binary file attached may encounter problems in traversing firewalls and spam filters. Accordingly, in another embodiment, the encrypted PIN is embedded directly within the body of the e-mail. In this embodiment, a reader of the e-mail will see the encrypted PIN as a series of incomprehensible text symbols, however the messaging application is configured to extract and decrypt the encrypted PIN. Additional details regarding the exchange of encrypted PINs and related key management and key exchange operations are provided below.” Klassen at 7:60-8:6. “As will be appreciated, once the above steps are complete, mobile device 10A will have the PIN for mobile device 10B, and mobile device 10B will have the PIN for mobile device 10A. Now, if either mobile device 10A or 10B desires to send a peer-to-peer message to the other, it prepares a peer-to-peer message

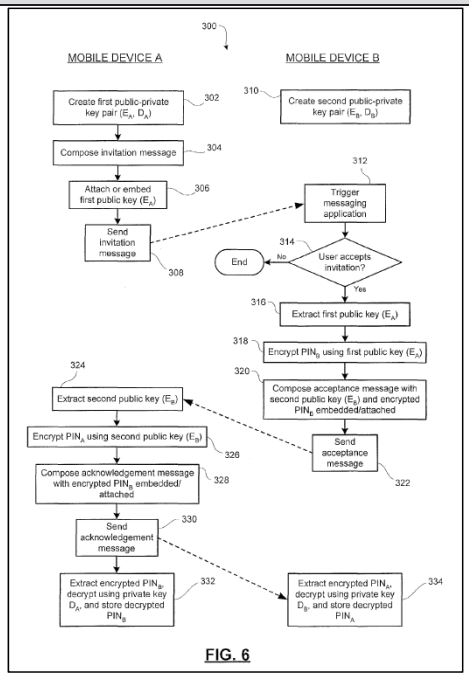
’619 Patent – Claim 22	Klassen
	using the peer-to-peer messaging application that includes the PIN of the recipient mobile device 10 (10A or 10B, as the case may be), preferably in the message header, along with the message information that is to be sent. The peer-to-peer message is then sent by the mobile device 10 through wireless network 15 to routing server 20. Routing server 20 obtains the PIN from the peer-to-peer message and uses it to determine the network address of the recipient mobile device 10 (10A or 10B, as the case may be) using the routing table(s) stored therein, and sends the message to the recipient mobile device 10 (10A or 10B, as the case may be) through wireless network 15 using the determined network address. Once received, the peer-to-peer message, and in particular the message information contained therein, may be displayed to the user of the recipient mobile device 10 (10A or 10B, as the case may be)..” Klassen at 8:7-27. “The messaging application 160 includes components for performing encryption, decryption, and related key management functions for exchanging PINs. These components may be provided as a part of the invitation and acceptance components or as separate components interacting therewith. These components manage the encryption of a resident PIN, the generation or calculation of any required key values or session keys, the attachment or embedding of encrypted PINs into messages for transmission through one of the existing communication applications 162, and the decryption of encrypted PINs received from other mobile devices 10 through one of the communication applications 162. Further detail regarding encryption, decryption, and key exchange within the context of the invitation architecture is given below..” Klassen at 10:47-62. “Reference is again made to FIGS. 1 and 5. As noted above, in the invitation architecture described in the present application the respective PINs of the mobile devices 10 are covertly exchanged using one of the existing communication applications. A sending mobile device encrypts its PIN prior to transmitting it using the communication application. At the receiving mobile

’619 Patent – Claim 22	Klassen
	device, the received encrypted PIN is decrypted. Through appropriate key management, access to the unencrypted PIN is limited to the messaging applications on the respective two mobile devices. There are a number of encryption and key management techniques that may be employed in various embodiments within the scope of the present application. Moreover, the particular transformation or function that may be used in conjunction with a key value to convert the PIN into an encrypted PIN may include a wide range of cryptographic transformations or functions. Those of ordinary skill in the art will appreciate that a wide range of such functions are known and may be selected, having regard to the processing power and any time constraints associated with a particular application or system.” Klassen at 11:57-12:11 “The messaging application 160 includes components for performing encryption, decryption, and related key management functions for exchanging PINs. These components may be provided as a part of the invitation and acceptance components or as separate components interacting therewith. These components manage the encryption of a resident PIN, the generation or calculation of any required key values or session keys, the attachment or embedding of encrypted PINs into messages for transmission through one of the existing communication applications 162, and the decryption of encrypted PINs received from other mobile devices 10 through one of the communication applications 162. Further detail regarding encryption, decryption, and key exchange within the context of the invitation architecture is given below.” Klassen at 10:48-62. “In the context of the messaging system described herein, the messaging applications 160 include a component for managing key pair generation and key exchanges. The key pair may be generated from a random seed value, such as, for example the time and date or other pseudo-random seeds. The public key for each mobile device 10 is communicated to the other mobile device 10

’619 Patent – Claim 22	Klassen
	using one of the communication applications 162. For example, the public key value may be embedded or attached to an e-mail sent from one mobile device 10A to the other mobile device 10B. In some embodiments, the messaging application 160 on the initiating mobile device 10A embeds or attaches its public key Ka to the invitation message sent to the receiving mobile device 10B. The receiving mobile device 10 in turn embeds or attaches its public key Kb to the acceptance message sent to the initiating mobile device 10A. In one embodiment, the communication application 162 employed by the messaging application 160 to implement the invitation and acceptance procedure is an e-mail application. In such an embodiment, the public keys may be attached to the e-mail as binary files. They may alternatively be embedded in the body of the e-mail text. Those of ordinary skill in the art will be familiar with the range of possibilities for attaching or embedding public key data into existing communication application messages.” Klassen at 12:46-13:3. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[22g] send the message to the remote device,	Klassen discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:

’619 Patent – Claim 22	Klassen
	 FIG. 1 Klassen, Fig. 1.

’619 Patent – Claim 22	Klassen
	 FIG. 5 Klassen, Fig. 5.

’619 Patent – Claim 22	Klassen
	 FIG. 6 Klassen, Fig. 6. “A system and methods providing immediate peer-to-peer messaging between mobile devices in a wireless system. An invitation architecture is disclosed which enables the exchange of personal identification numbers (PINs) without requiring a user to directly access or provide his or her PIN. A messaging application encrypts its associated PIN before providing it to a messaging application on another mobile device through an existing communication

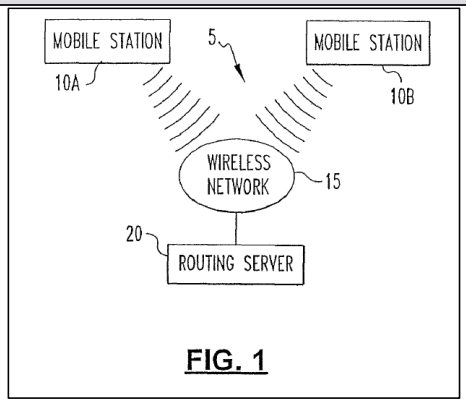
’619 Patent – Claim 22	Klassen
	application. An invitation process for exchanging encrypted PINs involves receiving an invitation containing a question, obtaining user input of an answer, and transmitting the answer back to the sender with an encrypted PIN. The sender confirms the received answer is correct and replies with its encrypted PIN.” Klassen at ABSTRACT. “The present application describes a system and a method that provide for immediate peer-to-peer messaging between mobile devices. The system and method provide increased security by maintaining the secrecy of the underlying address identity of each user of a mobile device in the system. An invitation architecture is disclosed which enables the exchange of personal identification numbers (PINs) without requiring a user to directly access or provide his or her PIN. A messaging application encrypts its associated PIN before providing it to a messaging application on another mobile device through an existing communication application. The invitation architecture automatically manages the encryption, any requisite key exchanges, the composition of invitation and acceptance messages, and the decryption and storage of PINs..” Klassen at 2:46-59. “In one aspect, the present application provides a method of securely exchanging personal identification numbers between a first mobile device and a second mobile device. The mobile devices are used in a system including a wireless network and a routing server coupled to the wireless network. Each mobile device has one or more communications applications and each mobile device further has a messaging application. The first mobile device has a first personal identification number and the second mobile device has a second personal identification number. The method includes the steps of encrypting the first personal identification number, sending the encrypted first personal identification number from the first mobile device to the second mobile device using one of the communication applications, and decrypting the encrypted first personal identification number and storing the first personal identification number in a memory on the second mobile device. The method also includes

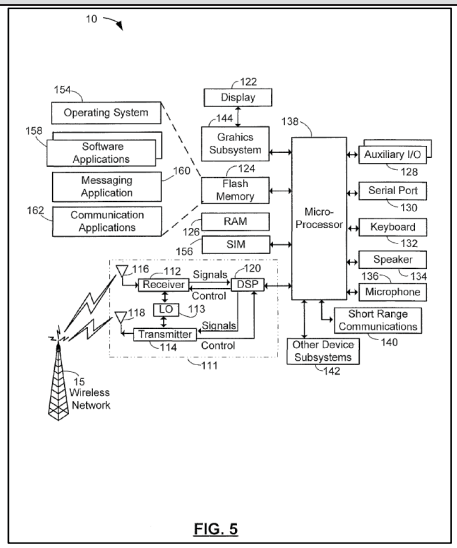
’619 Patent – Claim 22	Klassen
	the steps of encrypting the second personal identification number, sending the encrypted second personal identification number from the second mobile device to the first mobile device using one of the communication applications, and decrypting the encrypted second personal identification number and storing the second personal identification number in a memory on the first mobile device. After this exchange of PINs, peer-to-peer messages are exchanged between the first mobile device and the second mobile device using the messaging applications. Each peer-to-peer message contains one of the personal identification numbers and each peer-to-peer message is routed by the routing server based upon the personal identification numbers..” Klassen at 2:60-3:22. “Each mobile device 10 of system 5 is assigned and stores a unique personal identification number (PIN) . The PIN for each mobile device 10 may be assigned and stored therein when it is manufactured or through its subscriber identity module (SIM). Each PIN is mapped to a network address for the corresponding mobile device 10 on wireless network 15 that enables data to be routed to the mobile device 10. Routing server 20 includes one or more routing tables for routing messages sent by mobile devices 10 based on this mapping. In one exemplary embodiment, the PIN may actually be the network address itself, and in another exemplary embodiment, the PIN may be the phone number of the mobile device 10 or a unique ID such as the mobile subscriber ISDN (MSISDN) for the mobile device 10, and the network address may be an IP address or the like. It will be understood that the term “personal identification number” or “PIN” used herein is not intended to be limited solely to numeric identifiers, but is to be understood broadly and may include alphanumeric identifiers, binary identifiers, or other identifiers that can be used to enable peer-to-peer messaging.” Klassen at 6:16-35. “If the user of mobile device 10B indicates that he or she accepts the invitation and therefore wishes to establish a peer-to-peer messaging session, for example by selecting an “accept” button on the GUI, then the messaging application on

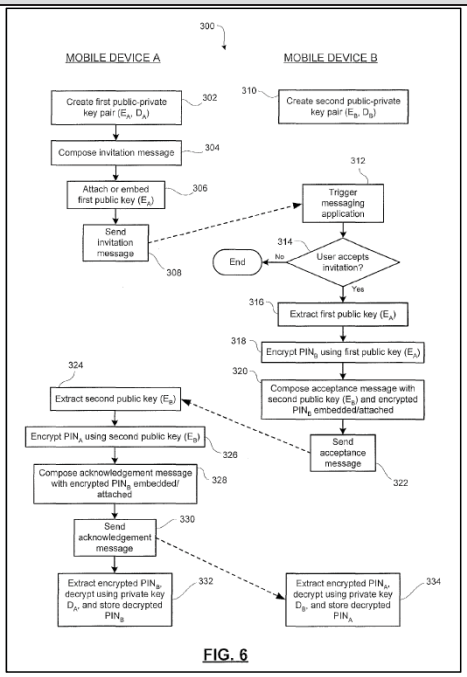
’619 Patent – Claim 22	Klassen
	mobile device 10B causes an acceptance communication to be transmitted to the originating mobile device 10A by way of the appropriate existing communication application. For example, in one embodiment the messaging application causes an acceptance e-mail to be composed and sent using the e-mail application. The messaging application on mobile device 10A is configured to recognize receipt of an acceptance message, like an acceptance e-mail. In addition to, or in conjunction with, exchanging an invitation and acceptance using the existing communication applications, the mobile devices 10A and 10B exchange PINs. In one embodiment, the PIN for mobile device 10B is sent with the acceptance message. In one embodiment, the PIN for mobile device 10A may be sent with either the invitation message or with a subsequent acknowledgement message after receipt of the acceptance message.” Klassen at 7:27-46. “The encrypted PINs may be embedded directly within the messages sent using the existing communication applications or may be attached to the messages. For example, with an e-mail application the encrypted PIN may be attached as a binary file. It will be appreciated that e-mail having a binary file attached may encounter problems in traversing firewalls and spam filters. Accordingly, in another embodiment, the encrypted PIN is embedded directly within the body of the e-mail. In this embodiment, a reader of the e-mail will see the encrypted PIN as a series of incomprehensible text symbols, however the messaging application is configured to extract and decrypt the encrypted PIN. Additional details regarding the exchange of encrypted PINs and related key management and key exchange operations are provided below.” Klassen at 7:60-8:6. “As will be appreciated, once the above steps are complete, mobile device 10A will have the PIN for mobile device 10B, and mobile device 10B will have the PIN for mobile device 10A. Now, if either mobile device 10A or 10B desires to send a peer-to-peer message to the other, it prepares a peer-to-peer message

’619 Patent – Claim 22	Klassen
	using the peer-to-peer messaging application that includes the PIN of the recipient mobile device 10 (10A or 10B, as the case may be), preferably in the message header, along with the message information that is to be sent. The peer-to-peer message is then sent by the mobile device 10 through wireless network 15 to routing server 20. Routing server 20 obtains the PIN from the peer-to-peer message and uses it to determine the network address of the recipient mobile device 10 (10A or 10B, as the case may be) using the routing table(s) stored therein, and sends the message to the recipient mobile device 10 (10A or 10B, as the case may be) through wireless network 15 using the determined network address. Once received, the peer-to-peer message, and in particular the message information contained therein, may be displayed to the user of the recipient mobile device 10 (10A or 10B, as the case may be)..” Klassen at 8:7-27. “The messaging application 160 includes components for performing encryption, decryption, and related key management functions for exchanging PINs. These components may be provided as a part of the invitation and acceptance components or as separate components interacting therewith. These components manage the encryption of a resident PIN, the generation or calculation of any required key values or session keys, the attachment or embedding of encrypted PINs into messages for transmission through one of the existing communication applications 162, and the decryption of encrypted PINs received from other mobile devices 10 through one of the communication applications 162. Further detail regarding encryption, decryption, and key exchange within the context of the invitation architecture is given below..” Klassen at 10:47-62. “Reference is again made to FIGS. 1 and 5. As noted above, in the invitation architecture described in the present application the respective PINs of the mobile devices 10 are covertly exchanged using one of the existing communication applications. A sending mobile device encrypts its PIN prior to transmitting it using the communication application. At the receiving mobile

’619 Patent – Claim 22	Klassen
	device, the received encrypted PIN is decrypted. Through appropriate key management, access to the unencrypted PIN is limited to the messaging applications on the respective two mobile devices. There are a number of encryption and key management techniques that may be employed in various embodiments within the scope of the present application. Moreover, the particular transformation or function that may be used in conjunction with a key value to convert the PIN into an encrypted PIN may include a wide range of cryptographic transformations or functions. Those of ordinary skill in the art will appreciate that a wide range of such functions are known and may be selected, having regard to the processing power and any time constraints associated with a particular application or system.” Klassen at 11:57-12:11 Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[22h] wherein the device is authenticated to access the messaging account.	Klassen discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:

’619 Patent – Claim 22	Klassen
	 FIG. 1 Klassen, Fig. 1.

’619 Patent – Claim 22	Klassen
	 FIG. 5 Klassen, Fig. 5.

’619 Patent – Claim 22	Klassen
	 FIG. 6 Klassen, Fig. 6. “A system and methods providing immediate peer-to-peer messaging between mobile devices in a wireless system. An invitation architecture is disclosed which enables the exchange of personal identification numbers (PINs) without requiring a user to directly access or provide his or her PIN. A messaging application encrypts its associated PIN before providing it to a messaging application on another mobile device through an existing communication

’619 Patent – Claim 22	Klassen
	application. An invitation process for exchanging encrypted PINs involves receiving an invitation containing a question, obtaining user input of an answer, and transmitting the answer back to the sender with an encrypted PIN. The sender confirms the received answer is correct and replies with its encrypted PIN.” Klassen at ABSTRACT. “The present application describes a system and a method that provide for immediate peer-to-peer messaging between mobile devices. The system and method provide increased security by maintaining the secrecy of the underlying address identity of each user of a mobile device in the system. An invitation architecture is disclosed which enables the exchange of personal identification numbers (PINs) without requiring a user to directly access or provide his or her PIN. A messaging application encrypts its associated PIN before providing it to a messaging application on another mobile device through an existing communication application. The invitation architecture automatically manages the encryption, any requisite key exchanges, the composition of invitation and acceptance messages, and the decryption and storage of PINs..” Klassen at 2:46-59. “In one aspect, the present application provides a method of securely exchanging personal identification numbers between a first mobile device and a second mobile device. The mobile devices are used in a system including a wireless network and a routing server coupled to the wireless network. Each mobile device has one or more communications applications and each mobile device further has a messaging application. The first mobile device has a first personal identification number and the second mobile device has a second personal identification number. The method includes the steps of encrypting the first personal identification number, sending the encrypted first personal identification number from the first mobile device to the second mobile device using one of the communication applications, and decrypting the encrypted first personal identification number and storing the first personal identification number in a memory on the second mobile device. The method also includes

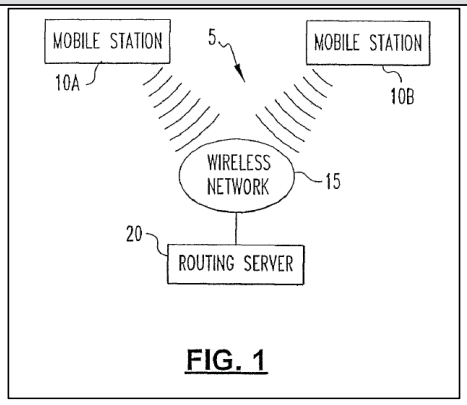
’619 Patent – Claim 22	Klassen
	the steps of encrypting the second personal identification number, sending the encrypted second personal identification number from the second mobile device to the first mobile device using one of the communication applications, and decrypting the encrypted second personal identification number and storing the second personal identification number in a memory on the first mobile device. After this exchange of PINs, peer-to-peer messages are exchanged between the first mobile device and the second mobile device using the messaging applications. Each peer-to-peer message contains one of the personal identification numbers and each peer-to-peer message is routed by the routing server based upon the personal identification numbers..” Klassen at 2:60-3:22. “Each mobile device 10 of system 5 is assigned and stores a unique personal identification number (PIN) . The PIN for each mobile device 10 may be assigned and stored therein when it is manufactured or through its subscriber identity module (SIM). Each PIN is mapped to a network address for the corresponding mobile device 10 on wireless network 15 that enables data to be routed to the mobile device 10. Routing server 20 includes one or more routing tables for routing messages sent by mobile devices 10 based on this mapping. In one exemplary embodiment, the PIN may actually be the network address itself, and in another exemplary embodiment, the PIN may be the phone number of the mobile device 10 or a unique ID such as the mobile subscriber ISDN (MSISDN) for the mobile device 10, and the network address may be an IP address or the like. It will be understood that the term “personal identification number” or “PIN” used herein is not intended to be limited solely to numeric identifiers, but is to be understood broadly and may include alphanumeric identifiers, binary identifiers, or other identifiers that can be used to enable peer-to-peer messaging.” Klassen at 6:16-35. “If the user of mobile device 10B indicates that he or she accepts the invitation and therefore wishes to establish a peer-to-peer messaging session, for example by selecting an “accept” button on the GUI, then the messaging application on

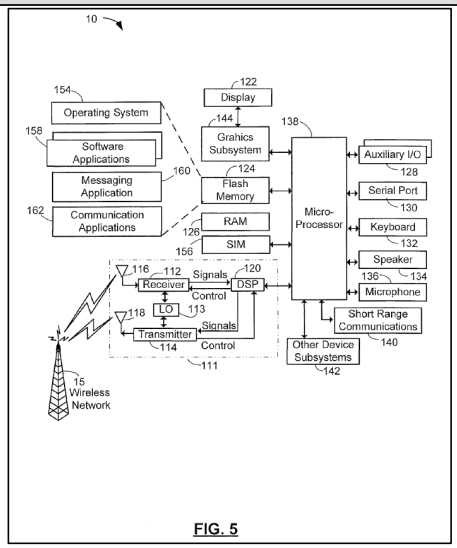
’619 Patent – Claim 22	Klassen
	mobile device 10B causes an acceptance communication to be transmitted to the originating mobile device 10A by way of the appropriate existing communication application. For example, in one embodiment the messaging application causes an acceptance e-mail to be composed and sent using the e-mail application. The messaging application on mobile device 10A is configured to recognize receipt of an acceptance message, like an acceptance e-mail. In addition to, or in conjunction with, exchanging an invitation and acceptance using the existing communication applications, the mobile devices 10A and 10B exchange PINs. In one embodiment, the PIN for mobile device 10B is sent with the acceptance message. In one embodiment, the PIN for mobile device 10A may be sent with either the invitation message or with a subsequent acknowledgement message after receipt of the acceptance message.” Klassen at 7:27-46. “The encrypted PINs may be embedded directly within the messages sent using the existing communication applications or may be attached to the messages. For example, with an e-mail application the encrypted PIN may be attached as a binary file. It will be appreciated that e-mail having a binary file attached may encounter problems in traversing firewalls and spam filters. Accordingly, in another embodiment, the encrypted PIN is embedded directly within the body of the e-mail. In this embodiment, a reader of the e-mail will see the encrypted PIN as a series of incomprehensible text symbols, however the messaging application is configured to extract and decrypt the encrypted PIN. Additional details regarding the exchange of encrypted PINs and related key management and key exchange operations are provided below.” Klassen at 7:60-8:6. “As will be appreciated, once the above steps are complete, mobile device 10A will have the PIN for mobile device 10B, and mobile device 10B will have the PIN for mobile device 10A. Now, if either mobile device 10A or 10B desires to send a peer-to-peer message to the other, it prepares a peer-to-peer message

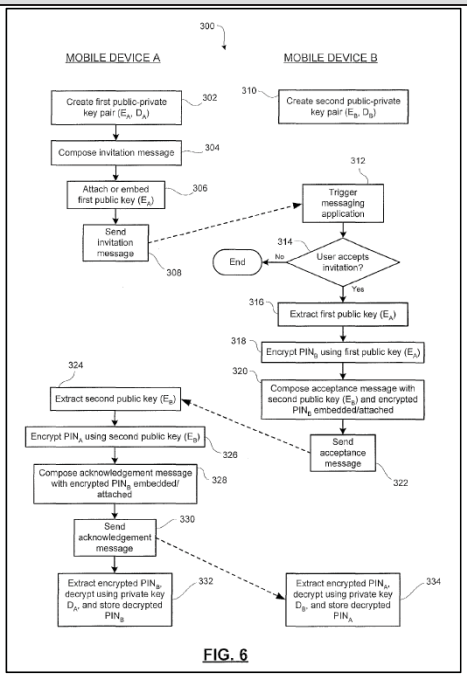
’619 Patent – Claim 22	Klassen
	using the peer-to-peer messaging application that includes the PIN of the recipient mobile device 10 (10A or 10B, as the case may be), preferably in the message header, along with the message information that is to be sent. The peer-to-peer message is then sent by the mobile device 10 through wireless network 15 to routing server 20. Routing server 20 obtains the PIN from the peer-to-peer message and uses it to determine the network address of the recipient mobile device 10 (10A or 10B, as the case may be) using the routing table(s) stored therein, and sends the message to the recipient mobile device 10 (10A or 10B, as the case may be) through wireless network 15 using the determined network address. Once received, the peer-to-peer message, and in particular the message information contained therein, may be displayed to the user of the recipient mobile device 10 (10A or 10B, as the case may be)..” Klassen at 8:7-27. “The messaging application 160 includes components for performing encryption, decryption, and related key management functions for exchanging PINs. These components may be provided as a part of the invitation and acceptance components or as separate components interacting therewith. These components manage the encryption of a resident PIN, the generation or calculation of any required key values or session keys, the attachment or embedding of encrypted PINs into messages for transmission through one of the existing communication applications 162, and the decryption of encrypted PINs received from other mobile devices 10 through one of the communication applications 162. Further detail regarding encryption, decryption, and key exchange within the context of the invitation architecture is given below..” Klassen at 10:47-62. “Reference is again made to FIGS. 1 and 5. As noted above, in the invitation architecture described in the present application the respective PINs of the mobile devices 10 are covertly exchanged using one of the existing communication applications. A sending mobile device encrypts its PIN prior to transmitting it using the communication application. At the receiving mobile

’619 Patent – Claim 22	Klassen
	device, the received encrypted PIN is decrypted. Through appropriate key management, access to the unencrypted PIN is limited to the messaging applications on the respective two mobile devices. There are a number of encryption and key management techniques that may be employed in various embodiments within the scope of the present application. Moreover, the particular transformation or function that may be used in conjunction with a key value to convert the PIN into an encrypted PIN may include a wide range of cryptographic transformations or functions. Those of ordinary skill in the art will appreciate that a wide range of such functions are known and may be selected, having regard to the processing power and any time constraints associated with a particular application or system.” Klassen at 11:57-12:11 Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

’619 Patent – Claim 23	Klassen
[23] The device of claim 22, wherein the information including the service activation code is received by the device in response to user input at the remote device.	Klassen discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22pre]-[22h], *above*.

’619 Patent – Claim 23	Klassen
	 FIG. 1 Klassen, Fig. 1.

’619 Patent – Claim 23	Klassen
	 FIG. 5 Klassen, Fig. 5.

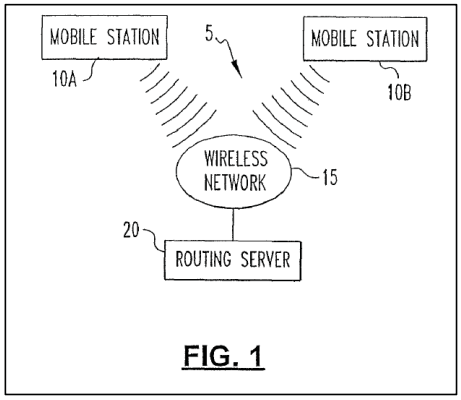
’619 Patent – Claim 23	Klassen
	 FIG. 6 Klassen, Fig. 6. “The method includes receiving an invitation via one of the communications applications, the invitation including a question; displaying the question; receiving through the user interface an answer in response to the question; encrypting the first personal identification number; transmitting the answer and the encrypted first personal identification number in response to the received

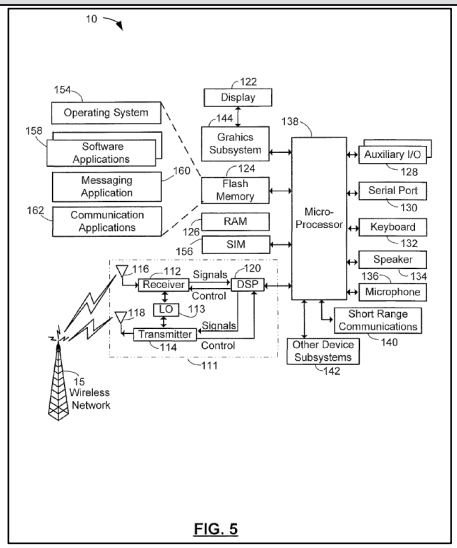
’619 Patent – Claim 23	Klassen
	invitation;” Klassen at 4:25-31. “The method includes sending an invitation via one of the communications applications, the invitation including a question, the question having a stored answer; encrypting the first personal identification number; receiving a user-submitted answer and an encrypted second personal identification number in response to the invitation; confirming that the user-submitted answer matches the stored answer; decrypting the second encrypted personal identification number; and transmitting the encrypted first personal identification number in response to receipt of the encrypted second personal identification number.” Klassen at 4:48-58. “a first contact management component configured to receive an invitation via one of said one or more communication applications, the invitation including a question, display the invitation including the question, receive an answer via a user interface in response to the question, transmit the answer and the encrypted first personal identification number in response to the invitation, and receive the encrypted second personal identification number in response to transmission of the encrypted first personal identification number;” Klassen at 5:8-16. “The another mobile device includes a second memory storing the second personal identification number, one or more communication applications, a second encryption component configured to encrypt said second personal identification number and decrypt the encrypted first personal identification number using the encryption key, a second contact management component configured to send the invitation to the mobile device using said one of said communication applications, receive an acceptance from said mobile device containing said answer, receive the encrypted first personal identification number from the mobile device, confirm that the received answer matches a stored answer, and transmit the encrypted second personal identification number to the mobile device, and a second messaging application for sending

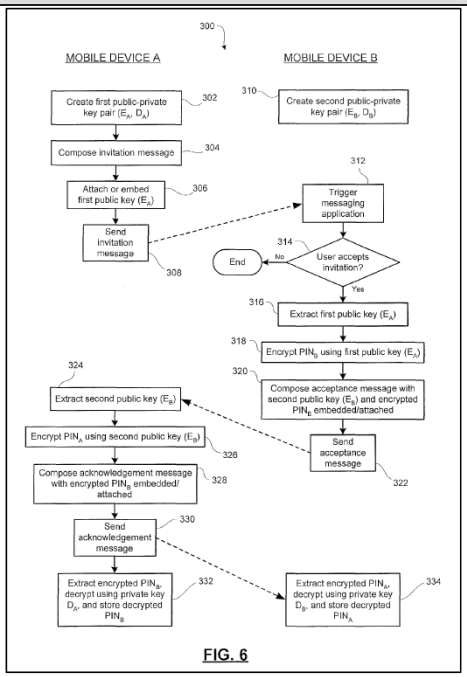
’619 Patent – Claim 23	Klassen
	and receiving peer-to-peer messages” Klassen at 5:27-41. “In addition to, or in conjunction with, exchanging an invitation and acceptance using the existing communication applications, the mobile devices 10A and 10B exchange PINs. In one embodiment, the PIN for mobile device 10B is sent with the acceptance message. In one embodiment, the PIN for mobile device 10A may be sent with either the invitation message or with a subsequent acknowledgement message after receipt of the acceptance message.” Klassen at 7:39-46. “The encrypted PINs may be embedded directly within the messages sent using the existing communication applications or may be attached to the messages. For example, with an e-mail application the encrypted PIN may be attached as a binary file. It will be appreciated that e-mail having a binary file attached may encounter problems in traversing firewalls and spam filters. Accordingly, in another embodiment, the encrypted PIN is embedded directly within the body of the e-mail. In this embodiment, a reader of the e-mail will see the encrypted PIN as a series of incomprehensible text symbols, however the messaging application is configured to extract and decrypt the encrypted PIN. Additional details regarding the exchange of encrypted PINs and related key management and key exchange operations are provided below.” Klassen 7:60-8:6. “The invitation component of the messaging application 160 composes and sends invitations to prospective contacts. A user of the device 10 instructs the messaging application 160 to send an invitation to another device. The user may provide an address for reaching the other device, such as an e-mail address. The invitation component generates and sends an invitation message through one of the communication applications 162, such as the e-mail application.” Klassen at 10:22-29. “The user of device 10A triggers an invitation process by providing an invitation command to the messaging application 160. The invitation command

’619 Patent – Claim 23	Klassen
	may be selected by the user from a menu. The user may be required to provide address or other contact information for the intended recipient of the invitation. The invitation command invokes the invitation component of the messaging application 160, which composes an invitation message in step 304. The message is composed using one of the communication applications 162, such as an e-mail application. The messaging application 160 ensures that the composed message includes an indicator to alert the messaging application 160 on the receiving mobile device 10B to the fact that the message is an invitation. In step 306, the messaging application 160 attaches or embeds the first public key EA into the composed invitation message. In one embodiment, the message is an e-mail message and the first public key EA is inserted in the text body of the e-mail message so as to enable the message to traverse firewalls and spam filters. In step 308, the communication application sends the invitation message to the receiving mobile device 10B. This message appears in the "inbox" for the communication application at the receiving mobile device 10B.” Klassen at 13:25-46. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

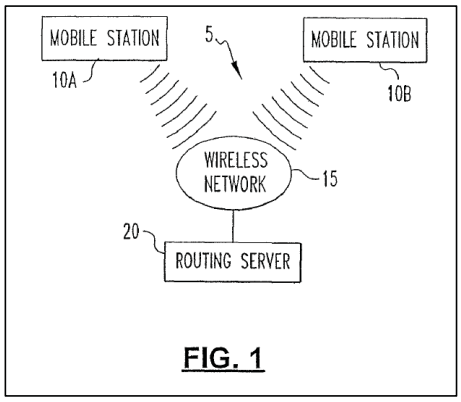
’619 Patent – Claim 24	Klassen
[24] The device of claim 22, wherein the information including the service activation code	Klassen discloses this claim limitation. For example, see the following

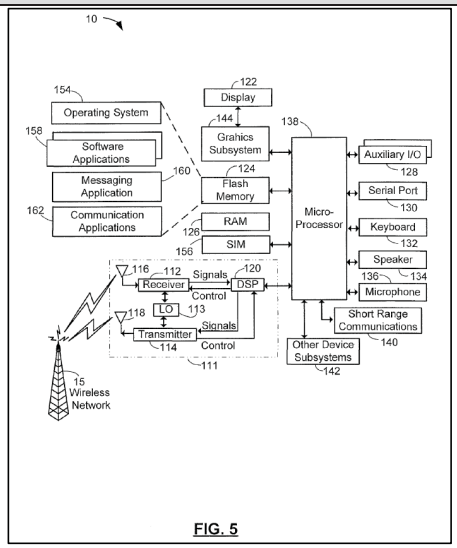
’619 Patent – Claim 24	Klassen
is received by the device in an off-line communication.	passages and/or figures, as well as all related disclosures: *See* [22pre]-[22h], *above*.  FIG. 1 Klassen, Fig. 1.

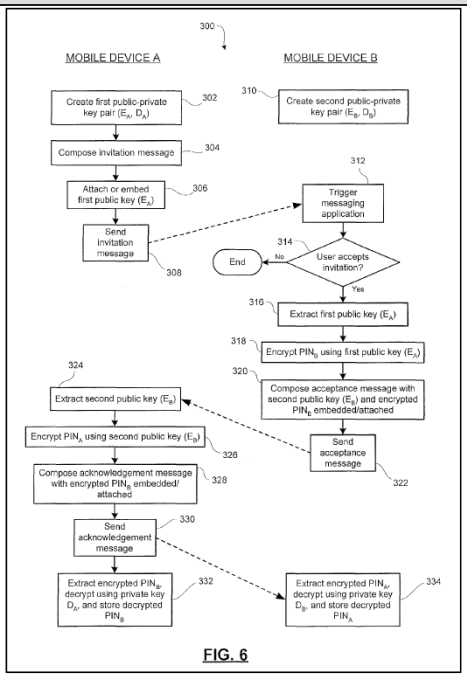
’619 Patent – Claim 24	Klassen
	 FIG. 5 Klassen, Fig. 5.

’619 Patent – Claim 24	Klassen
	 FIG. 6 Klassen, Fig. 6. “As will be appreciated, once the above steps are complete, mobile device 10A will have the PIN for mobile device 10B, and mobile device 10B will have the PIN for mobile device 10A. Now, if either mobile device 10A or 10B desires to send a peer-to-peer message to the other, it prepares a peer-to-peer message using the peer-to-peer messaging application that includes the PIN of the

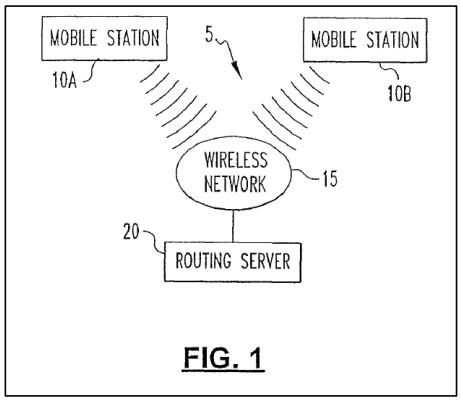
’619 Patent – Claim 24	Klassen
	recipient mobile device 10 (10A or 10B, as the case may be), preferably in the message header, along with the message information that is to be sent. The peer-to-peer message is then sent by the mobile device 10 through wireless network 15 to routing server 20. Routing server 20 obtains the PIN from the peer-to-peer message and uses it to determine the network address of the recipient mobile device 10 (10A or 10B, as the case may be) using the routing table(s) stored therein, and sends the message to the recipient mobile device 10 (10A or 10B, as the case may be) through wireless network 15 using the determined network address. Once received, the peer-to-peer message, and in particular the message information contained therein, may be displayed to the user of the recipient mobile device 10 (10A or 10B, as the case may be).” Klassen at 8:7-27. “The short-range communications subsystem 140 is a further component which may provide for communication between the device 10 and different systems or devices , which need not necessarily be similar devices. For example, the subsystem 140 may include an infrared device and associated circuits and components or a Bluetooth™ communication module to provide for communication with similarly enabled systems and devices. The device 10 may be a handheld device.” Klassen at 9:63-10:4. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

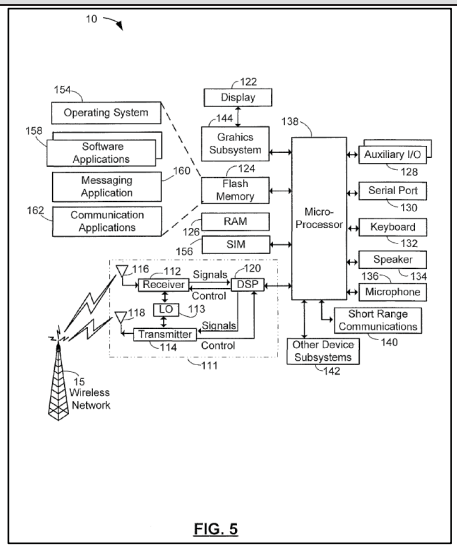
’619 Patent – Claim 25	Klassen
[25] The device of claim 24, wherein the off-line communication involves a local connection.	Klassen discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22pre]-[22h] and [24], *above*.  FIG. 1 Klassen, Fig. 1.

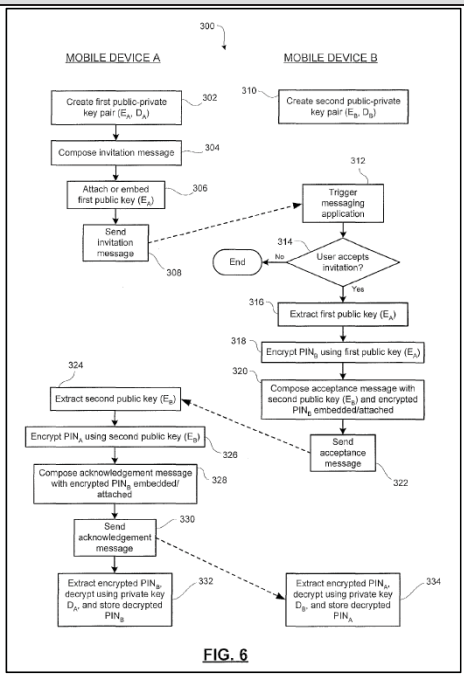
’619 Patent – Claim 25	Klassen
	 FIG. 5 Klassen, Fig. 5.

’619 Patent – Claim 25	Klassen
	 FIG. 6 Klassen, Fig. 6. “As will be appreciated, once the above steps are complete, mobile device 10A will have the PIN for mobile device 10B, and mobile device 10B will have the PIN for mobile device 10A. Now, if either mobile device 10A or 10B desires to send a peer-to-peer message to the other, it prepares a peer-to-peer message using the peer-to-peer messaging application that includes the PIN of the

’619 Patent – Claim 25	Klassen
	recipient mobile device 10 (10A or 10B, as the case may be), preferably in the message header, along with the message information that is to be sent. The peer-to-peer message is then sent by the mobile device 10 through wireless network 15 to routing server 20. Routing server 20 obtains the PIN from the peer-to-peer message and uses it to determine the network address of the recipient mobile device 10 (10A or 10B, as the case may be) using the routing table(s) stored therein, and sends the message to the recipient mobile device 10 (10A or 10B, as the case may be) through wireless network 15 using the determined network address. Once received, the peer-to-peer message, and in particular the message information contained therein, may be displayed to the user of the recipient mobile device 10 (10A or 10B, as the case may be).” Klassen at 8:7-27. “The short-range communications subsystem 140 is a further component which may provide for communication between the device 10 and different systems or devices , which need not necessarily be similar devices. For example, the subsystem 140 may include an infrared device and associated circuits and components or a Bluetooth™ communication module to provide for communication with similarly enabled systems and devices. The device 10 may be a handheld device.” Klassen at 9:63-10:4. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

’619 Patent – Claim 26	Klassen
[26] The device of claim 24, wherein the off-line communication prevents eavesdropping of the service activation code.	Klassen discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22pre]-[22h] and [24], *above*.  FIG. 1 Klassen, Fig. 1.

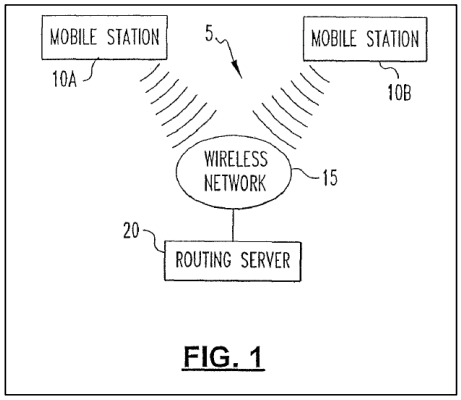
’619 Patent – Claim 26	Klassen
	 FIG. 5 Klassen, Fig. 5.

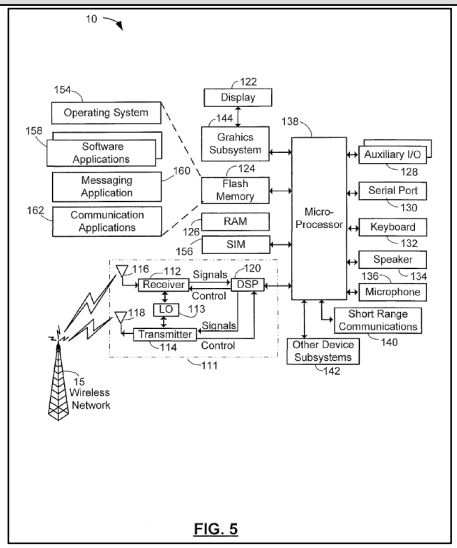
’619 Patent – Claim 26	Klassen
	 FIG. 6 Klassen, Fig. 6. “In addition to, or in conjunction with, exchanging an invitation and acceptance using the existing communication applications, the mobile devices 10A and 10B exchange PINs. In one embodiment, the PIN for mobile device 10B is sent with the acceptance message. In one embodiment, the PIN for mobile device 10A may be sent with either the invitation message or with a subsequent

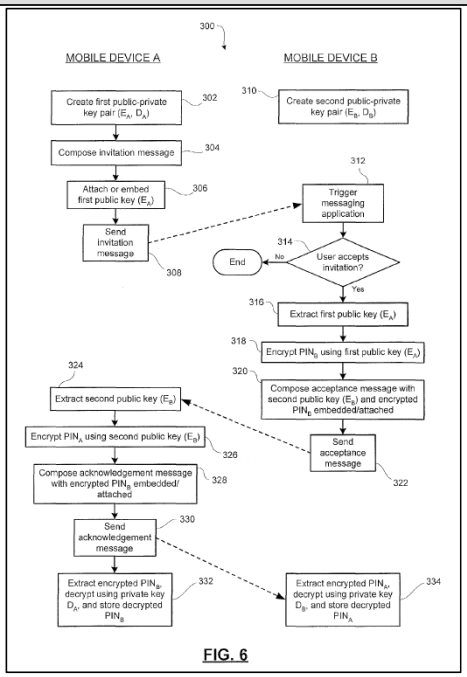
’619 Patent – Claim 26	Klassen
	acknowledgement message after receipt of the acceptance message. In accordance with the present application, the secrecy and confidentiality of the PINs is maintained despite the need to exchange them between mobile devices. If a user's PIN is made generally available to another user by sending it over an unsecured channel, then it is easy for the other user to share the PIN with a wide range of users or it is easy for an unauthorized recipient to intercept a message and obtain the PIN. Most of the existing communication applications, like e-mail, utilize unsecured channels. As a result a mobile device may receive messages from unwanted sources that have obtained the PIN for the mobile device. Accordingly, the PINs are exchanged in an encrypted form in embodiments disclosed in the present application.” Klassen at 7:39-59. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

’619 Patent – Claim 27	Klassen
[27] The device of claim 22, wherein the authentication of the device relies on the authentication of the messaging account.	Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and

’619 Patent – Claim 27	Klassen
	Exhibit 619-B.

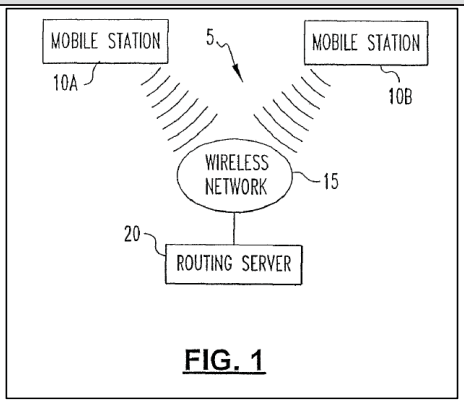
’619 Patent – Claim 28	Klassen
[28] The device of claim 27, wherein the authentication of the messaging account includes a username and password.	Klassen discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22pre]-[22h] and [27], *above*.  FIG. 1 Klassen, Fig. 1.

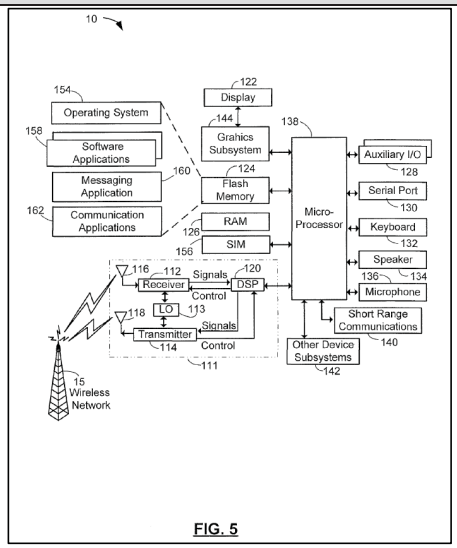
’619 Patent – Claim 28	Klassen
	 FIG. 5 Klassen, Fig. 5.

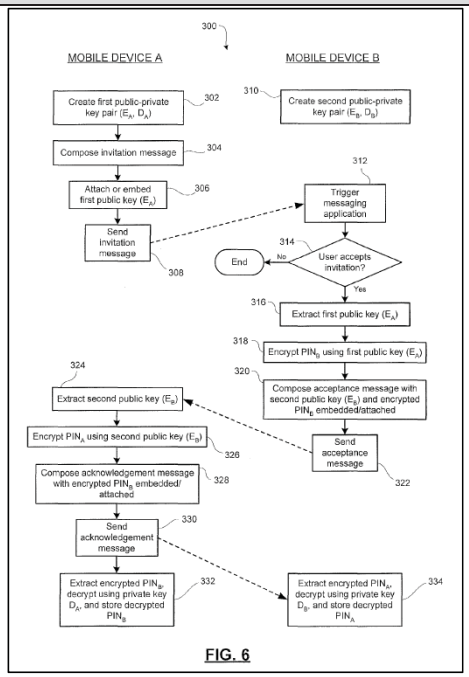
’619 Patent – Claim 28	Klassen
	 FIG. 6 Klassen, Fig. 6. “In one embodiment, the user of mobile device l0A uses a relatively secure chamiel, such as a voice channel, to provide the user of mobile device 10B with a key value or a seed value from which the key may be derived. For example, the first user may provide the second user with a codeword or password which the second user enters into the mobile device 10B when prompted. The

’619 Patent – Claim 28	Klassen
	codeword or password may be used as a seed value in conjunction with an algorithm to compute the secret key for use in encrypting and decrypting communications.” Klassen at 12:19-28. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

’619 Patent – Claim 32	Klassen
[32] The device of claim 22, wherein the encryption key is closely related to the service activation code.	Klassen discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22pre]-[22h], *above*.

’619 Patent – Claim 32	Klassen
	 FIG. 1 Klassen, Fig. 1.

’619 Patent – Claim 32	Klassen
	 FIG. 5 Klassen, Fig. 5.

’619 Patent – Claim 32	Klassen
	 FIG. 6 Klassen, Fig. 6. “A system and methods providing immediate peer-to-peer messaging between mobile devices in a wireless system. An invitation architecture is disclosed which enables the exchange of personal identification numbers (PINs) without requiring a user to directly access or provide his or her PIN. A messaging application encrypts its associated PIN before providing it to a messaging

’619 Patent – Claim 32	Klassen
	application on another mobile device through an existing communication application. An invitation process for exchanging encrypted PINs involves receiving an invitation containing a question, obtaining user input of an answer, and transmitting the answer back to the sender with an encrypted PIN. The sender confirms the received answer is correct and replies with its encrypted PIN.” Klassen at ABSTRACT. “The present application describes a system and a method that provide for immediate peer-to-peer messaging between mobile devices. The system and method provide increased security by maintaining the secrecy of the underlying address identity of each user of a mobile device in the system. An invitation architecture is disclosed which enables the exchange of personal identification numbers (PINs) without requiring a user to directly access or provide his or her PIN. A messaging application encrypts its associated PIN before providing it to a messaging application on another mobile device through an existing communication application. The invitation architecture automatically manages the encryption, any requisite key exchanges, the composition of invitation and acceptance messages, and the decryption and storage of PINs..” Klassen at 2:46-59. “In one aspect, the present application provides a method of securely exchanging personal identification numbers between a first mobile device and a second mobile device. The mobile devices are used in a system including a wireless network and a routing server coupled to the wireless network. Each mobile device has one or more communications applications and each mobile device further has a messaging application. The first mobile device has a first personal identification number and the second mobile device has a second personal identification number. The method includes the steps of encrypting the first personal identification number, sending the encrypted first personal identification number from the first mobile device to the second mobile device using one of the communication applications, and decrypting the encrypted first personal identification number and storing the first personal identification

’619 Patent – Claim 32	Klassen
	number in a memory on the second mobile device. The method also includes the steps of encrypting the second personal identification number, sending the encrypted second personal identification number from the second mobile device to the first mobile device using one of the communication applications, and decrypting the encrypted second personal identification number and storing the second personal identification number in a memory on the first mobile device. After this exchange of PINs, peer-to-peer messages are exchanged between the first mobile device and the second mobile device using the messaging applications. Each peer-to-peer message contains one of the personal identification numbers and each peer-to-peer message is routed by the routing server based upon the personal identification numbers..” Klassen at 2:60-3:22. “Each mobile device 10 of system 5 is assigned and stores a unique personal identification number (PIN) . The PIN for each mobile device 10 may be assigned and stored therein when it is manufactured or through its subscriber identity module (SIM). Each PIN is mapped to a network address for the corresponding mobile device 10 on wireless network 15 that enables data to be routed to the mobile device 10. Routing server 20 includes one or more routing tables for routing messages sent by mobile devices 10 based on this mapping. In one exemplary embodiment, the PIN may actually be the network address itself, and in another exemplary embodiment, the PIN may be the phone number of the mobile device 10 or a unique ID such as the mobile subscriber ISDN (MSISDN) for the mobile device 10, and the network address may be an IP address or the like. It will be understood that the term “personal identification number” or “PIN” used herein is not intended to be limited solely to numeric identifiers, but is to be understood broadly and may include alphanumeric identifiers, binary identifiers, or other identifiers that can be used to enable peer-to-peer messaging.” Klassen at 6:16-35. “If the user of mobile device 10B indicates that he or she accepts the invitation and therefore wishes to establish a peer-to-peer messaging session, for example

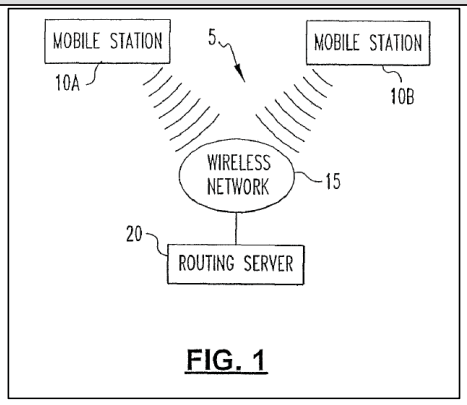
’619 Patent – Claim 32	Klassen
	by selecting an “accept” button on the GUI, then the messaging application on mobile device 10B causes an acceptance communication to be transmitted to the originating mobile device 10A by way of the appropriate existing communication application. For example, in one embodiment the messaging application causes an acceptance e-mail to be composed and sent using the e-mail application. The messaging application on mobile device 10A is configured to recognize receipt of an acceptance message, like an acceptance e-mail. In addition to, or in conjunction with, exchanging an invitation and acceptance using the existing communication applications, the mobile devices 10A and 10B exchange PINs. In one embodiment, the PIN for mobile device 10B is sent with the acceptance message. In one embodiment, the PIN for mobile device 10A may be sent with either the invitation message or with a subsequent acknowledgement message after receipt of the acceptance message.” Klassen at 7:27-46. “The encrypted PINs may be embedded directly within the messages sent using the existing communication applications or may be attached to the messages. For example, with an e-mail application the encrypted PIN may be attached as a binary file. It will be appreciated that e-mail having a binary file attached may encounter problems in traversing firewalls and spam filters. Accordingly, in another embodiment, the encrypted PIN is embedded directly within the body of the e-mail. In this embodiment, a reader of the e-mail will see the encrypted PIN as a series of incomprehensible text symbols, however the messaging application is configured to extract and decrypt the encrypted PIN. Additional details regarding the exchange of encrypted PINs and related key management and key exchange operations are provided below.” Klassen at 7:60-8:6. “As will be appreciated, once the above steps are complete, mobile device 10A will have the PIN for mobile device 10B, and mobile device 10B will have the PIN for mobile device 10A. Now, if either mobile device 10A or 10B desires to

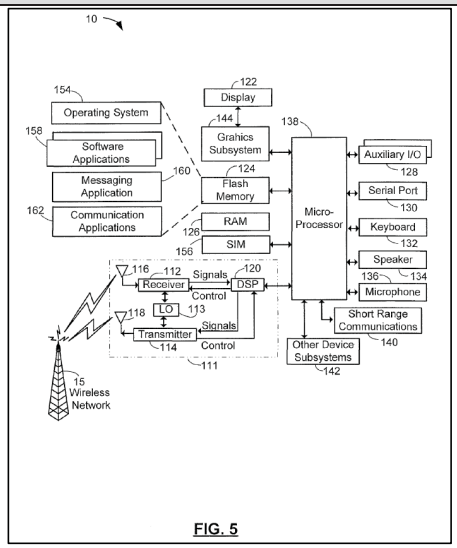
’619 Patent – Claim 32	Klassen
	send a peer-to-peer message to the other, it prepares a peer-to-peer message using the peer-to-peer messaging application that includes the PIN of the recipient mobile device 10 (10A or 10B, as the case may be), preferably in the message header, along with the message information that is to be sent. The peer-to-peer message is then sent by the mobile device 10 through wireless network 15 to routing server 20. Routing server 20 obtains the PIN from the peer-to-peer message and uses it to determine the network address of the recipient mobile device 10 (10A or 10B, as the case may be) using the routing table(s) stored therein, and sends the message to the recipient mobile device 10 (10A or 10B, as the case may be) through wireless network 15 using the determined network address. Once received, the peer-to-peer message, and in particular the message information contained therein, may be displayed to the user of the recipient mobile device 10 (10A or 10B, as the case may be)..” Klassen at 8:7-27. “The messaging application 160 includes components for performing encryption, decryption, and related key management functions for exchanging PINs. These components may be provided as a part of the invitation and acceptance components or as separate components interacting therewith. These components manage the encryption of a resident PIN, the generation or calculation of any required key values or session keys, the attachment or embedding of encrypted PINs into messages for transmission through one of the existing communication applications 162, and the decryption of encrypted PINs received from other mobile devices 10 through one of the communication applications 162. Further detail regarding encryption, decryption, and key exchange within the context of the invitation architecture is given below..” Klassen at 10:47-62. “Reference is again made to FIGS. 1 and 5. As noted above, in the invitation architecture described in the present application the respective PINs of the mobile devices 10 are covertly exchanged using one of the existing communication applications. A sending mobile device encrypts its PIN prior to

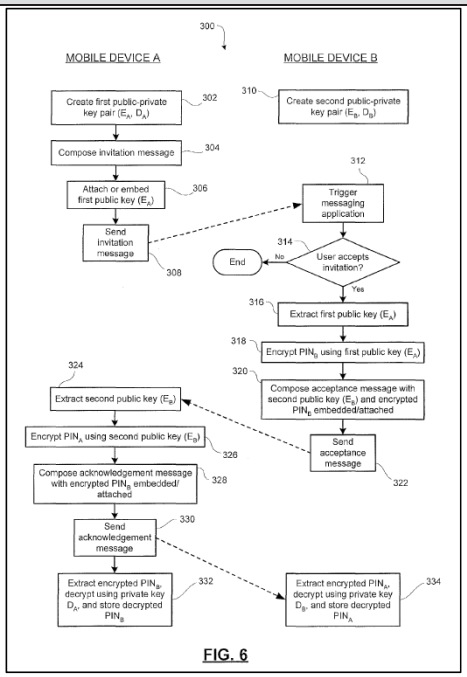
’619 Patent – Claim 32	Klassen
	transmitting it using the communication application. At the receiving mobile device, the received encrypted PIN is decrypted. Through appropriate key management, access to the unencrypted PIN is limited to the messaging applications on the respective two mobile devices. There are a number of encryption and key management techniques that may be employed in various embodiments within the scope of the present application. Moreover, the particular transformation or function that may be used in conjunction with a key value to convert the PIN into an encrypted PIN may include a wide range of cryptographic transformations or functions. Those of ordinary skill in the art will appreciate that a wide range of such functions are known and may be selected, having regard to the processing power and any time constraints associated with a particular application or system.” Klassen at 11:57-12:11 “The acceptance component automatically generates and sends an acceptance message through one of the communication applications 162, such as the e-mail application. The messaging application 160 includes components for performing encryption, decryption, and related key management functions for exchanging PINs. These components may be provided as a part of the invitation and acceptance components or as separate components interacting therewith. These components manage the encryption of a resident PIN, the generation or calculation of any required key values or the generation or calculation of any required key values or session keys, the attachment or embedding of encrypted PINs into messages for transmission through one of the existing communication applications 162, and the decryption of encrypted PINs received from other mobile devices 10 through one of the communication applications 162.” Klassen at 10:45-54. “There are a number of encryption and key management techniques that may be employed in various embodiments within the scope of the present application. Moreover, the particular transformation or function that may be

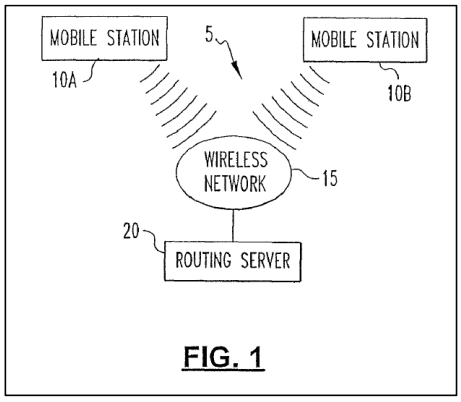
'619 Patent – Claim 32	Klassen
	used in 5 conjunction with a key value to convert the PIN into an encrypted PIN may include a wide range of cryptographic transformations or functions. Those of ordinary skill in the art will appreciate that a wide range of such functions are known and may be selected, having regard to the processing power and any time constraints associated with a particular application or system." Klassen at 12:1-9. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

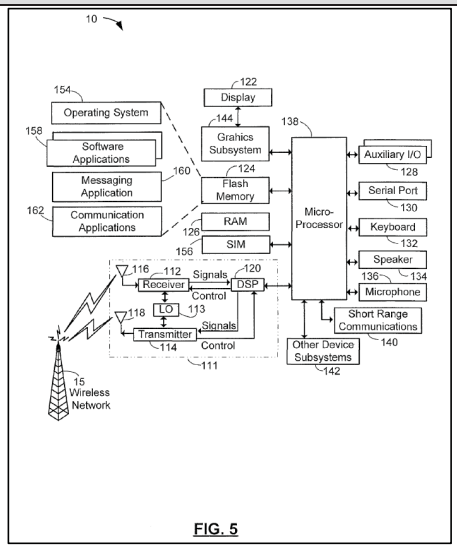
'619 Patent – Claim 33	Klassen
[33a] The device of claim 22, wherein the device is further operable to:	Klassen discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22pre]-[22h], *above*.

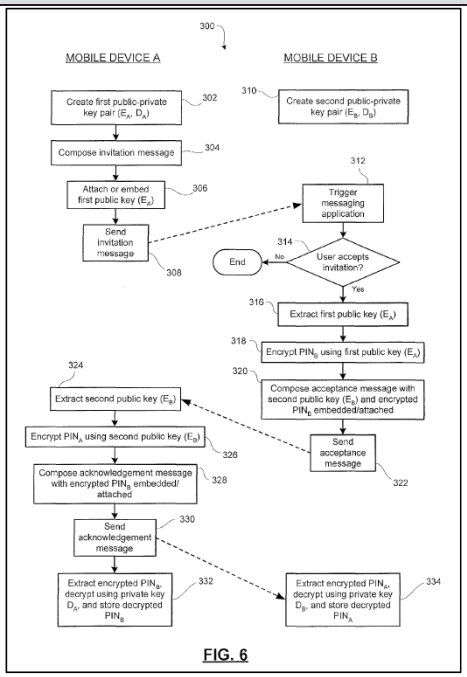
’619 Patent – Claim 33	Klassen
	 FIG. 1 Klassen, Fig. 1.

’619 Patent – Claim 33	Klassen
	 FIG. 5 Klassen, Fig. 5.

’619 Patent – Claim 33	Klassen
	 FIG. 6 Klassen, Fig. 6. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable

’619 Patent – Claim 33	Klassen
	solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[33b] store an association between at least two of the encryption key, the messaging account, an identifier of the remote device, and the service activation code.	Klassen discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22pre]-[22h], *above*.  FIG. 1 Klassen, Fig. 1.

’619 Patent – Claim 33	Klassen
	 FIG. 5 Klassen, Fig. 5.

’619 Patent – Claim 33	Klassen
	 FIG. 6 Klassen, Fig. 6. “A system and methods providing immediate peer-to-peer messaging between mobile devices in a wireless system. An invitation architecture is disclosed which enables the exchange of personal identification numbers (PINs) without requiring a user to directly access or provide his or her PIN. A messaging application encrypts its associated PIN before providing it to a messaging

’619 Patent – Claim 33	Klassen
	application on another mobile device through an existing communication application. An invitation process for exchanging encrypted PINs involves receiving an invitation containing a question, obtaining user input of an answer, and transmitting the answer back to the sender with an encrypted PIN. The sender confirms the received answer is correct and replies with its encrypted PIN.” Klassen at ABSTRACT. “The present application describes a system and a method that provide for immediate peer-to-peer messaging between mobile devices. The system and method provide increased security by maintaining the secrecy of the underlying address identity of each user of a mobile device in the system. An invitation architecture is disclosed which enables the exchange of personal identification numbers (PINs) without requiring a user to directly access or provide his or her PIN. A messaging application encrypts its associated PIN before providing it to a messaging application on another mobile device through an existing communication application. The invitation architecture automatically manages the encryption, any requisite key exchanges, the composition of invitation and acceptance messages, and the decryption and storage of PINs..” Klassen at 2:46-59. “In one aspect, the present application provides a method of securely exchanging personal identification numbers between a first mobile device and a second mobile device. The mobile devices are used in a system including a wireless network and a routing server coupled to the wireless network. Each mobile device has one or more communications applications and each mobile device further has a messaging application. The first mobile device has a first personal identification number and the second mobile device has a second personal identification number. The method includes the steps of encrypting the first personal identification number, sending the encrypted first personal identification number from the first mobile device to the second mobile device using one of the communication applications, and decrypting the encrypted first personal identification number and storing the first personal identification

’619 Patent – Claim 33	Klassen
	number in a memory on the second mobile device. The method also includes the steps of encrypting the second personal identification number, sending the encrypted second personal identification number from the second mobile device to the first mobile device using one of the communication applications, and decrypting the encrypted second personal identification number and storing the second personal identification number in a memory on the first mobile device. After this exchange of PINs, peer-to-peer messages are exchanged between the first mobile device and the second mobile device using the messaging applications. Each peer-to-peer message contains one of the personal identification numbers and each peer-to-peer message is routed by the routing server based upon the personal identification numbers..” Klassen at 2:60-3:22. “Each mobile device 10 of system 5 is assigned and stores a unique personal identification number (PIN) . The PIN for each mobile device 10 may be assigned and stored therein when it is manufactured or through its subscriber identity module (SIM). Each PIN is mapped to a network address for the corresponding mobile device 10 on wireless network 15 that enables data to be routed to the mobile device 10. Routing server 20 includes one or more routing tables for routing messages sent by mobile devices 10 based on this mapping. In one exemplary embodiment, the PIN may actually be the network address itself, and in another exemplary embodiment, the PIN may be the phone number of the mobile device 10 or a unique ID such as the mobile subscriber ISDN (MSISDN) for the mobile device 10, and the network address may be an IP address or the like. It will be understood that the term “personal identification number” or “PIN” used herein is not intended to be limited solely to numeric identifiers, but is to be understood broadly and may include alphanumeric identifiers, binary identifiers, or other identifiers that can be used to enable peer-to-peer messaging.” Klassen at 6:16-35. “If the user of mobile device 10B indicates that he or she accepts the invitation and therefore wishes to establish a peer-to-peer messaging session, for example

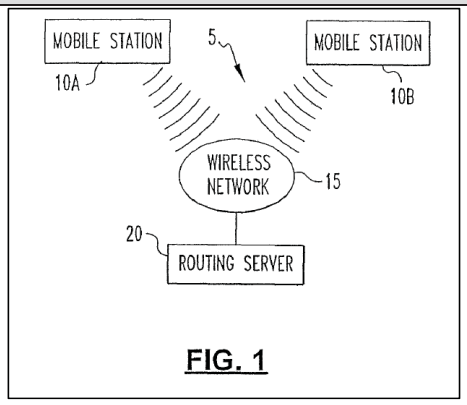
’619 Patent – Claim 33	Klassen
	by selecting an “accept” button on the GUI, then the messaging application on mobile device 10B causes an acceptance communication to be transmitted to the originating mobile device 10A by way of the appropriate existing communication application. For example, in one embodiment the messaging application causes an acceptance e-mail to be composed and sent using the e-mail application. The messaging application on mobile device 10A is configured to recognize receipt of an acceptance message, like an acceptance e-mail. In addition to, or in conjunction with, exchanging an invitation and acceptance using the existing communication applications, the mobile devices 10A and 10B exchange PINs. In one embodiment, the PIN for mobile device 10B is sent with the acceptance message. In one embodiment, the PIN for mobile device 10A may be sent with either the invitation message or with a subsequent acknowledgement message after receipt of the acceptance message.” Klassen at 7:27-46. “The encrypted PINs may be embedded directly within the messages sent using the existing communication applications or may be attached to the messages. For example, with an e-mail application the encrypted PIN may be attached as a binary file. It will be appreciated that e-mail having a binary file attached may encounter problems in traversing firewalls and spam filters. Accordingly, in another embodiment, the encrypted PIN is embedded directly within the body of the e-mail. In this embodiment, a reader of the e-mail will see the encrypted PIN as a series of incomprehensible text symbols, however the messaging application is configured to extract and decrypt the encrypted PIN. Additional details regarding the exchange of encrypted PINs and related key management and key exchange operations are provided below.” Klassen at 7:60-8:6. “As will be appreciated, once the above steps are complete, mobile device 10A will have the PIN for mobile device 10B, and mobile device 10B will have the PIN for mobile device 10A. Now, if either mobile device 10A or 10B desires to

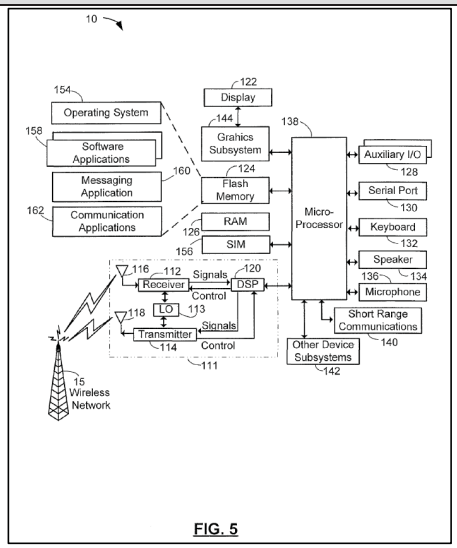
’619 Patent – Claim 33	Klassen
	send a peer-to-peer message to the other, it prepares a peer-to-peer message using the peer-to-peer messaging application that includes the PIN of the recipient mobile device 10 (10A or 10B, as the case may be), preferably in the message header, along with the message information that is to be sent. The peer-to-peer message is then sent by the mobile device 10 through wireless network 15 to routing server 20. Routing server 20 obtains the PIN from the peer-to-peer message and uses it to determine the network address of the recipient mobile device 10 (10A or 10B, as the case may be) using the routing table(s) stored therein, and sends the message to the recipient mobile device 10 (10A or 10B, as the case may be) through wireless network 15 using the determined network address. Once received, the peer-to-peer message, and in particular the message information contained therein, may be displayed to the user of the recipient mobile device 10 (10A or 10B, as the case may be)..” Klassen at 8:7-27. “The messaging application 160 includes components for performing encryption, decryption, and related key management functions for exchanging PINs. These components may be provided as a part of the invitation and acceptance components or as separate components interacting therewith. These components manage the encryption of a resident PIN, the generation or calculation of any required key values or session keys, the attachment or embedding of encrypted PINs into messages for transmission through one of the existing communication applications 162, and the decryption of encrypted PINs received from other mobile devices 10 through one of the communication applications 162. Further detail regarding encryption, decryption, and key exchange within the context of the invitation architecture is given below..” Klassen at 10:47-62. “Reference is again made to FIGS. 1 and 5. As noted above, in the invitation architecture described in the present application the respective PINs of the mobile devices 10 are covertly exchanged using one of the existing communication applications. A sending mobile device encrypts its PIN prior to

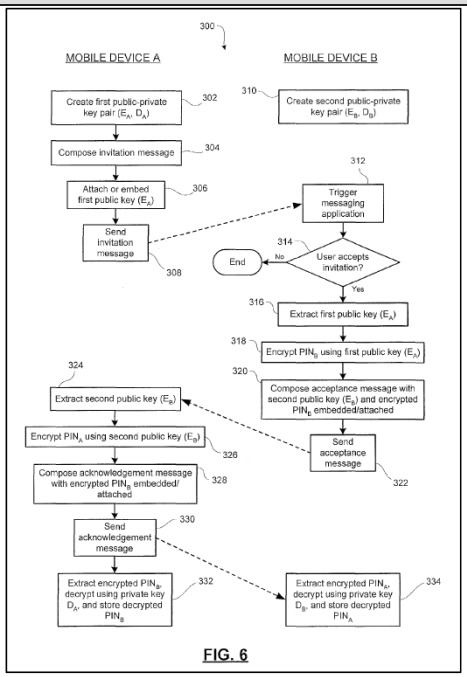
’619 Patent – Claim 33	Klassen
	transmitting it using the communication application. At the receiving mobile device, the received encrypted PIN is decrypted. Through appropriate key management, access to the unencrypted PIN is limited to the messaging applications on the respective two mobile devices. There are a number of encryption and key management techniques that may be employed in various embodiments within the scope of the present application. Moreover, the particular transformation or function that may be used in conjunction with a key value to convert the PIN into an encrypted PIN may include a wide range of cryptographic transformations or functions. Those of ordinary skill in the art will appreciate that a wide range of such functions are known and may be selected, having regard to the processing power and any time constraints associated with a particular application or system.” Klassen at 11:57-12:11. “The messaging application 160 includes components for performing encryption, decryption, and related key management functions for exchanging PINs. These components may be provided as a part of the invitation and acceptance components or as separate components interacting therewith. These components manage the encryption of a resident PIN, the generation or calculation of any required key values or session keys, the attachment or embedding of encrypted PINs into messages for transmission through one of the existing communication applications 162, and the decryption of encrypted PINs received from other mobile devices 10 through one of the communication applications 162. Further detail regarding encryption, decryption, and key exchange within the context of the invitation architecture is given below. Klassen at 10:48-62. “Each mobile device 10 decrypts the encrypted PIN it has received using its private key DA' DB, respectively, as shown in steps 332 and 334. The devices 10 then store the decrypted PINs in association with contact information for the user of the other device 10. Accordingly, the user of the other device 10 is now

'619 Patent – Claim 33	Klassen
	part of a "buddy list" or contact list for use by the messaging application 160." Klassen at 14:15-19. "According to another aspect of the present application, the peer-to-peer messaging application of each mobile device 10 includes a contact database that stores the name and/or other identifying information and corresponding PIN for each user of another mobile device 10 with whom the user of the mobile device 10 has communicated or may wish to communicate using the peer-to-peer messaging application." Klassen at 14:60-67. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

'619 Patent – Claim 36	Klassen
[36] The device of claim 22, wherein a control message is received from the remote device upon user interaction with the message.	Klassen discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22pre]-[22h], *above*.

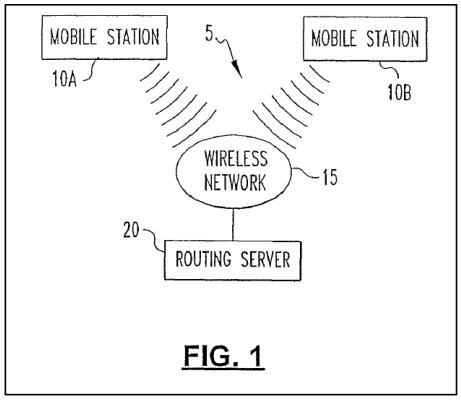
’619 Patent – Claim 36	Klassen
	 FIG. 1 Klassen, Fig. 1.

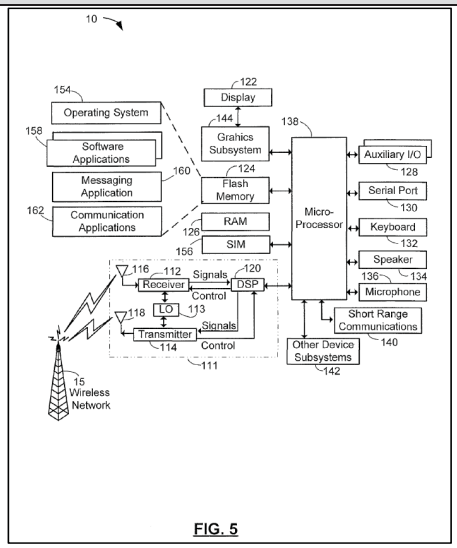
’619 Patent – Claim 36	Klassen
	 FIG. 5 Klassen, Fig. 5.

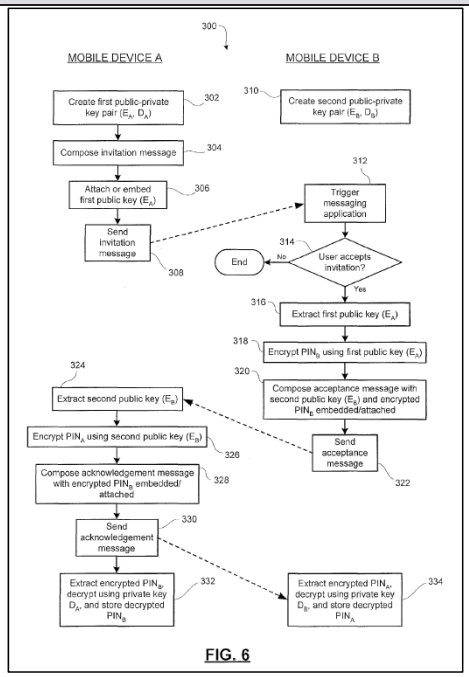
’619 Patent – Claim 36	Klassen
	 FIG. 6 Klassen, Fig. 6. “For example, if the email invitation message is opened first, the peer-to-peer application will scan the "inbox" or the like for the SMS invitation message. As described above, the invitation messages may be identified by the special indicators provided therewith. The peer-to-peer messaging application in this embodiment will not provide the user of mobile device 10B with the ability to

’619 Patent – Claim 36	Klassen
	accept the invitation until the other invitation message(s) is found. Once the other invitation message(s) is found, the user of mobile device 10 may accept the invitation as described above, reject the invitation, or postpone the decision to accept or reject.” Klassen at 11:33-44. “Either on receipt of the invitation message or once the user opens the invitation message, the monitoring component of the messaging application 160 recognizes it to be an invitation. Accordingly, in step 312, the messaging application 160 is triggered. The messaging application 160 queries the user in step 314 to determine whether the user wishes to accept or reject the invitation.” Klassen at 13:46-53. “The messaging application 160 on the first mobile device 10A recognizes the acceptance message, either on receipt or once the user opens the message, and it extracts the second public key EB from the acceptance message in step 324 . In step 326, the messaging application 160 encrypts the PIN for the initiating mobile device 10A (i.e. PINA) in accordance with the predefined encryption transformation or function. The messaging application 160 then composes an acknowledgement message in step 328 for transmission through one of the communication applications 162, such as an e-mail application. The acknowledgement message includes the encrypted PINA, which may be embedded or attached to the acknowledgement message. The acknowledgement message is then sent to the second mobile device 10B in step 330.” Klassen at 14:1-14. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and

’619 Patent – Claim 36	Klassen
	Exhibit 619-B.

’619 Patent – Claim 37	Klassen
[37pre] 37. A method for sharing a messaging account, the method comprising:	To the extent the preamble is limiting, Klassen discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:  FIG. 1 Klassen, Fig. 1.

’619 Patent – Claim 37	Klassen
	 FIG. 5 Klassen, Fig. 5.

’619 Patent – Claim 37	Klassen
	 FIG. 6 Klassen, Fig. 6. “The present application describes a system and a method that provide for immediate peer-to-peer messaging between mobile devices. The system and method provide increased security by maintaining the secrecy of the underlying address identity of each user of a mobile device in the system. An invitation architecture is disclosed which enables the exchange of personal identification numbers (PINs) without requiring a user to directly access or provide his or her

’619 Patent – Claim 37	Klassen
	PIN. A messaging application encrypts its associated PIN before providing it to a messaging application on another mobile device through an existing communication application. The invitation architecture automatically manages the encryption, any requisite key exchanges, the composition of invitation and acceptance messages, and the decryption and storage of PINs.” Klassen at 2:46-59. “Referring now to the drawings, FIG. 1 is a block diagram of a system 5 for enabling immediate peer-to-peer messaging. System 5 includes a plurality of mobile stations 10, such as mobile devices 10A and 10B shown in FIG. 1, which may be any type of wireless mobile electronic communications device such as a cell phone, a smart phone, a personal data assistant (PDA), a pager, a handheld computer or a phone-enabled laptop computer, to name a few. As is known, each mobile device 10 may be provided with various applications, including, without limitation, one or more currently existing applications that enable communication with other mobile devices 10, such as a wireless telephone application, an email application, a short message service (SMS) application, a multimedia messaging service (MMS) application, an enhanced message service (EMS) application, and other Internet enable messaging applications (each of which may be referred to herein as an “existing communications application”). In addition, each mobile device 10 is provided with an application that implements the peer-to-peer messaging solution described herein (referred to herein as the “messaging application”). The term “application” as used herein shall include one or more programs, routines, subroutines, function calls or other type of software or firmware and the like, alone or in combination. System 5 also includes wireless network 15, which may be any wireless communications network or combination of interconnected networks, including, without limitation, Mobiltex™, DataTAC™, AMPS, TDMA, CDMA, GSM/GPRS, PCS, EDGE, UMTS or CDPD. As is known, wireless network 15 includes a plurality of base stations that perform radio frequency (RF) protocols to support data and voice exchanges with mobile devices 10A and 10B. Routing server 20 is coupled to

'619 Patent – Claim 37	Klassen
	wireless network 15. Routing server 20 may be any type of routing equipment capable of routing data packets, including, without limitation, a TCP/IP router such as those sold by Cisco Systems, Inc. of San Jose, Calif., or a network address translation server (NAT)." Klassen at 5:46-6:15. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[37a] authenticating a device for access to the messaging account;	Klassen discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22h], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[37b] optically receiving information including a displayed service activation code from a remote device;	Klassen discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22c], above.

'619 Patent – Claim 37	Klassen
	Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[37c] registering the remote device for access to the messaging account using the service activation code;	Klassen discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22d], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[37d] receiving a message for the messaging account;	Klassen discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22e], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable

’619 Patent – Claim 37	Klassen
	solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[37e] encrypting the message using an encryption key; and	Klassen discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22f], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[37f] sending the message to the remote device.	Klassen discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22g], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

'619 Patent – Claim 38	Klassen
[38] The method of claim 37, wherein the information including the service activation code is received by the device in response to user input at the remote device.	Klassen discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [23], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

'619 Patent – Claim 39	Klassen
[39] The method of claim 38, wherein the information including the service activation code is received by the device in an off-line communication.	Klassen discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [24], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

’619 Patent – Claim 40	Klassen
[40] The method of claim 39, wherein the off-line communication prevents eavesdropping of the service activation code.	Klassen discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [26], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

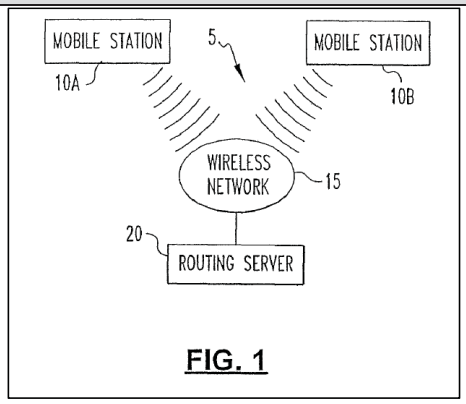
’619 Patent – Claim 41	Klassen
[41] The method of claim 37, wherein the authentication of the device relies on the authentication of the messaging system.	Klassen discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [27], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

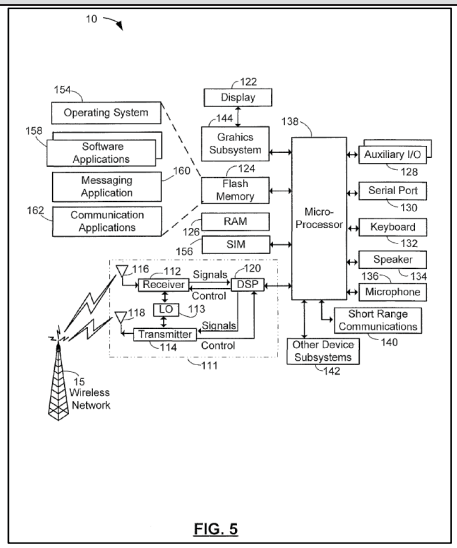
’619 Patent – Claim 42	Klassen
[42] The method of claim 41, wherein the authentication of the messaging system includes a username and password.	Klassen discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [28], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

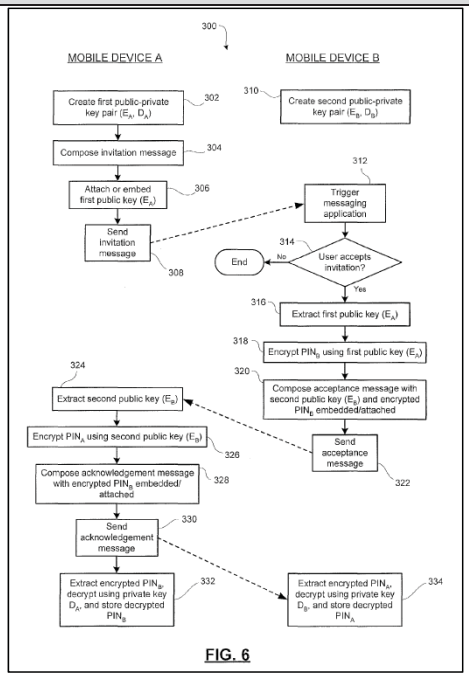
’619 Patent – Claim 46	Klassen
[46] The method of claim 37, wherein the encryption key is closely related to the service activation code.	Klassen discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [32], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

’619 Patent – Claim 50	Klassen
[50] The method of claim 37, wherein a control message is received from the remote device upon user interaction with the message.	Klassen discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [36], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

’619 Patent – Claim 51	Klassen
[51pre] 51. A non-transient computer-readable medium containing program instructions for causing a device to perform a method, the method comprising:	To the extent the preamble is limiting, Klassen discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:

’619 Patent – Claim 51	Klassen
	 FIG. 1 Klassen, Fig. 1.

’619 Patent – Claim 51	Klassen
	 FIG. 5 Klassen, Fig. 5.

’619 Patent – Claim 51	Klassen
	 FIG. 6 Klassen, Fig. 6. “The present application describes a system and a method that provide for immediate peer-to-peer messaging between mobile devices. The system and method provide increased security by maintaining the secrecy of the underlying address identity of each user of a mobile device in the system. An invitation architecture is disclosed which enables the exchange of personal identification numbers (PINs) without requiring a user to directly access or provide his or her

’619 Patent – Claim 51	Klassen
	PIN. A messaging application encrypts its associated PIN before providing it to a messaging application on another mobile device through an existing communication application. The invitation architecture automatically manages the encryption, any requisite key exchanges, the composition of invitation and acceptance messages, and the decryption and storage of PINs.” Klassen at 2:46-59. “Referring now to the drawings, FIG. 1 is a block diagram of a system 5 for enabling immediate peer-to-peer messaging. System 5 includes a plurality of mobile stations 10, such as mobile devices 10A and 10B shown in FIG. 1, which may be any type of wireless mobile electronic communications device such as a cell phone, a smart phone, a personal data assistant (PDA), a pager, a handheld computer or a phone-enabled laptop computer, to name a few. As is known, each mobile device 10 may be provided with various applications, including, without limitation, one or more currently existing applications that enable communication with other mobile devices 10, such as a wireless telephone application, an email application, a short message service (SMS) application, a multimedia messaging service (MMS) application, an enhanced message service (EMS) application, and other Internet enable messaging applications (each of which may be referred to herein as an “existing communications application”). In addition, each mobile device 10 is provided with an application that implements the peer-to-peer messaging solution described herein (referred to herein as the “messaging application”). The term “application” as used herein shall include one or more programs, routines, subroutines, function calls or other type of software or firmware and the like, alone or in combination. System 5 also includes wireless network 15, which may be any wireless communications network or combination of interconnected networks, including, without limitation, Mobiltex™, DataTAC™, AMPS, TDMA, CDMA, GSM/GPRS, PCS, EDGE, UMTS or CDPD. As is known, wireless network 15 includes a plurality of base stations that perform radio frequency (RF) protocols to support data and voice exchanges with mobile devices 10A and 10B. Routing server 20 is coupled to

’619 Patent – Claim 51	Klassen
	wireless network 15. Routing server 20 may be any type of routing equipment capable of routing data packets, including, without limitation, a TCP/IP router such as those sold by Cisco Systems, Inc. of San Jose, Calif., or a network address translation server (NAT).” Klassen at 5:46-6:15. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[51a] optically receiving information including a displayed service activation code from a remote device;	Klassen discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22c], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[51b] registering the remote device for access to a messaging account using the service activation code;	Klassen discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22d], above.

'619 Patent – Claim 51	Klassen
	Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[51c] receiving a message for the messaging account;	Klassen discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22e], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[51d] encrypting the message using an encryption key; and	Klassen discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22f], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable

’619 Patent – Claim 51	Klassen
	solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[51e] sending the message to the remote device,	Klassen discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22g], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[51f] wherein the device is authenticated to access the messaging account.	Klassen discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22h], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

’619 Patent – Claim 52	Klassen
[52] The method of claim 51, wherein a control message is received from the remote device upon user interaction with the message.	Klassen discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [36], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

EXHIBIT 619-A05

Invalidity Contentions for U.S. Patent No. 10,027,619 ("the '619 patent")

Based on: U.S. Patent No. 8,831,576 to Munje et al. ("Munje")

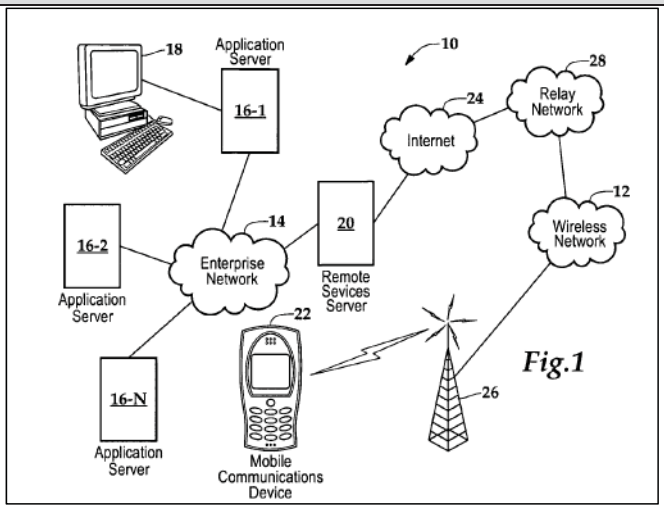
Based on SEVEN's apparent positions as to the scope of the patent's claims, as best they can be deciphered, the reference(s) charted below anticipate(s) or at least render(s) obvious the identified claims. The portions of the prior art reference cited below are not exhaustive but are exemplary in nature. Where Apple identifies a portion of the prior art reference's text, the identification should be understood as referencing any corresponding figure or diagram, and vice versa.

This disclosure is not an admission that Apple concedes any claim construction implied or suggested by SEVEN's apparent positions as to the scope of the patent's claims, nor is it an admission by Apple that any of its products are covered by or infringe the patent's claims, particularly when they are properly construed and applied. Apple is not taking any claim construction positions through this disclosure, including whether the preamble is a limitation.

Apple reserves the right to rely on additional citations or sources of evidence that also may be applicable, or that may become applicable in light of claim construction, changes in SEVEN's infringement contentions, and/or information obtained during discovery as the case progresses. Apple further reserves the right to amend or supplement this claim chart at a later date as more fully set forth in the Invalidity Contentions.

Munje qualifies as prior art under at least pre-AIA 35 U.S.C. § 102(e). Munje is a U.S. Patent that was filed on November 17, 2008, published on March 12, 2009, and issued on September 9, 2014.

'619 Patent – Claim 22	Munje
[22pre] A device comprising:	To the extent the preamble is limiting, Munje discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:

’619 Patent – Claim 22	Munje
	 Munje, Fig. 1.

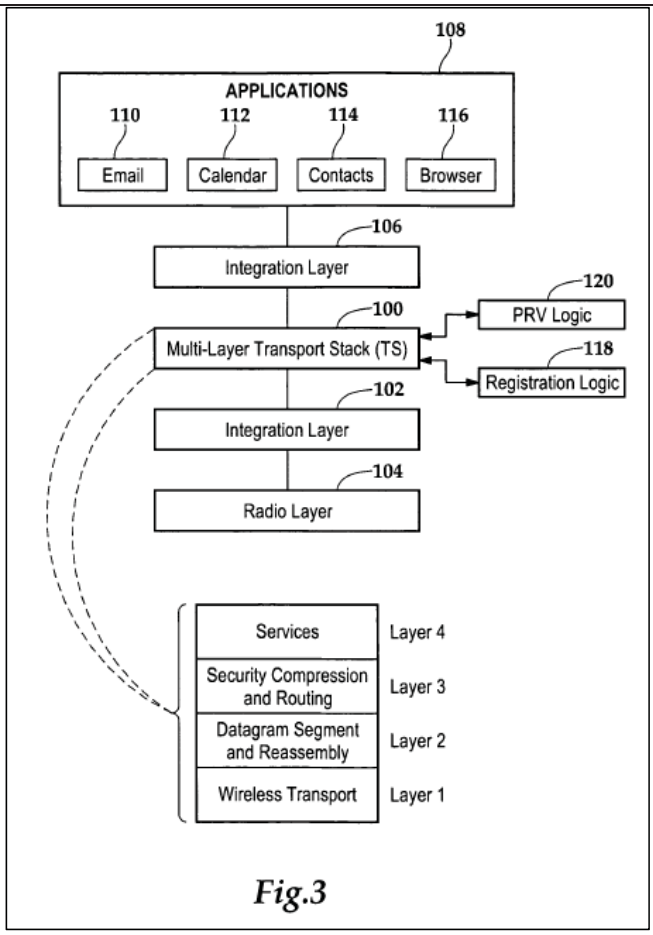
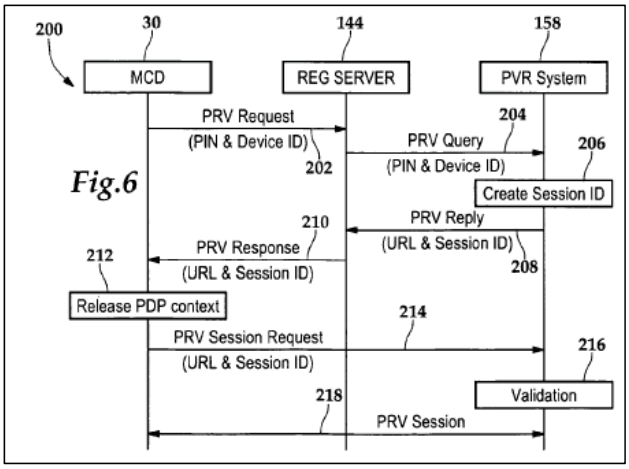
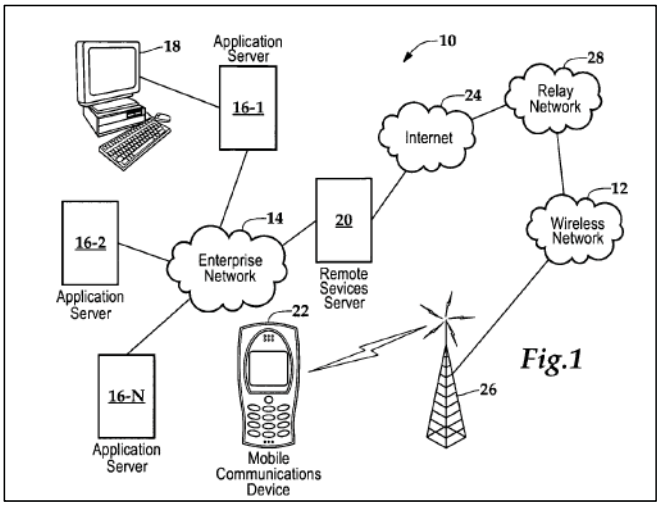

108
APPLICATIONS
110
112
114
116
Email
Calendar
Contacts
Browser
106
Integration Layer
120
PRV Logic
100
Multi-Layer Transport Stack (TS)
118
Registration Logic
102
Integration Layer
104
Radio Layer
Services
Layer 4
Security Compression and Routing
Layer 3
Datagram Segment and Reassembly
Layer 2
Wireless Transport
Layer 1

Fig.3

’619 Patent – Claim 22	Munje
	Munje, Fig. 3.  *Fig.6* Munje, Fig. 6. “Referring now to the drawings, and more particularly to FIG. 1, depicted therein is an exemplary network environment 10 including a wireless packet data service network 12 wherein an embodiment of the present method may be practiced. An enterprise network 14 for serving a plurality of corporate users, which may be a packet-switched network, can include one or more geographic sites and be organized as a local area network (LAN), a wide area network (WAN), a metropolitan area network (MAN) or the like. A number of application servers 16-1 through 16-N disposed as part of the enterprise network 14 are operable to provide or effectuate a host of internal and external services such as email, video mail, Internet access, corporate data access, messaging, calendaring and scheduling, information management and the like.

’619 Patent – Claim 22	Munje
	Accordingly, a diverse array of personal information appliances 18 such as desktop computers, laptop computers, palmtop computers or the like may be operably networked to one or more of the application servers 16-i, i=1, 2, . . . , N, with respect to the services supported in the enterprise network 14.” Munje at 2:49-67. “Additionally, a remote services server 20 may be interfaced with the enterprise network 14 for enabling a corporate user to access or effectuate any of the services from a remote location using a suitable single PDP context mobile communications device (MCD) 22. A secure communication link with end-to-end encryption may be established that is mediated through an external IP network, i.e., a public packet-switched network such as the Internet 24, as well as the wireless packet data service network 12 operable with MCD 22 via suitable wireless network infrastructure that includes a base station 26. In one embodiment, a trusted relay network 28 may be disposed between the Internet 24 and the infrastructure of wireless packet data service network 12. By way of example, MCD 22 may be a data-enabled handheld device capable of receiving and sending messages, web browsing, interfacing with corporate application servers and the like.” Munje at 3:1-17. “Communication between the relay services node 132 and various application gateways and servers is effectuated using any suitable protocol, e.g., Server Relay Protocol (SRP), preferably over IP links. By way of illustration, remote services server 20 associated with the enterprise network 14 (shown in FIG. 1) communicates with the relay using SRP for effectuating internal data services with respect to the enterprise's mobile subscribers. Likewise, reference numerals 136 and 138 refer to external application gateways, such as Internet Service Provider (ISP) or Internet Access Provider (IAP) servers, and other gateways, respectively, which are also interfaced with the relay node 132 using SRP. A peer-to-peer server 140 may also be provided in operable connection with the relay node 132 for handling peer-level messaging between two

’619 Patent – Claim 22	Munje
	MCDs.” Munje at 5:50-64. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[22a] a radio;	Munje discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: 

’619 Patent – Claim 22	Munje
	Munje, Fig. 1.

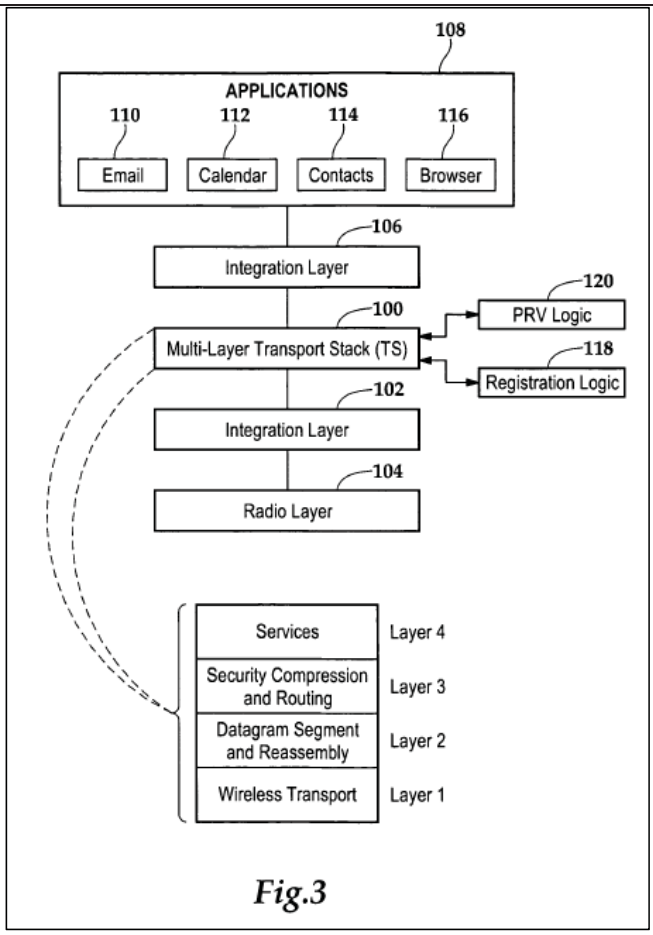
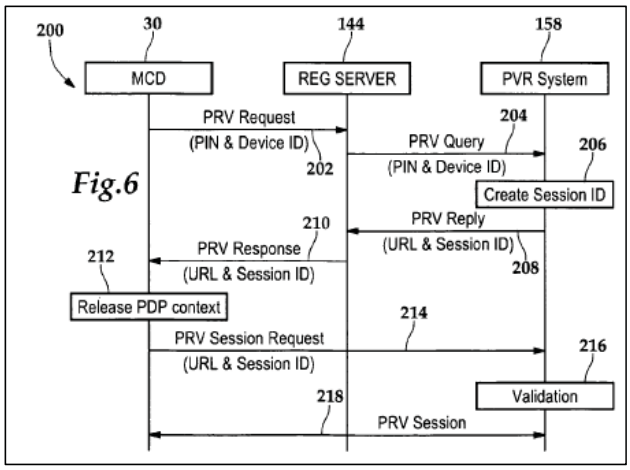
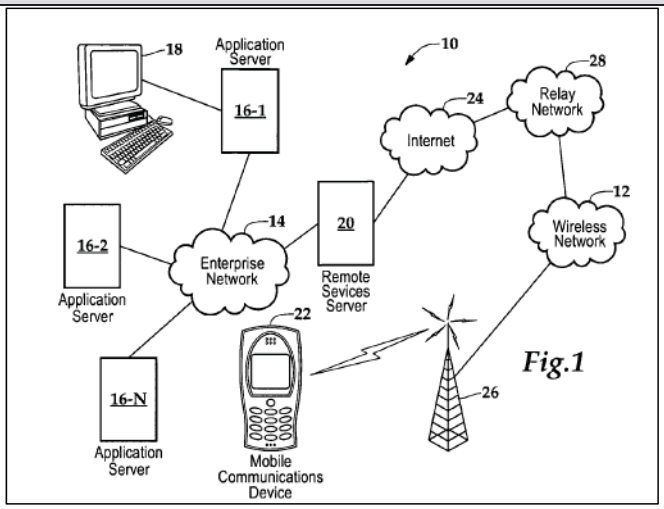

108
APPLICATIONS
110
112
114
116
Email
Calendar
Contacts
Browser
106
Integration Layer
120
PRV Logic
100
Multi-Layer Transport Stack (TS)
118
Registration Logic
102
Integration Layer
104
Radio Layer
Services
Layer 4
Security Compression and Routing
Layer 3
Datagram Segment and Reassembly
Layer 2
Wireless Transport
Layer 1

Fig.3

’619 Patent – Claim 22	Munje
	Munje, Fig. 3.  *Fig.6* Munje, Fig. 6. “For purposes of the present disclosure, the wireless packet data service network 12 may be implemented in any known or heretofore unknown mobile communications technologies and network protocols, as long as a packet-switched data service is available therein for transmitting packetized information. For instance, the wireless packet data service network 12 may be comprised of a General Packet Radio Service (GPRS) network that provides a packet radio access for mobile devices using the cellular infrastructure of a Global System for Mobile Communications (GSM)-based carrier network. In other implementations, the wireless packet data service network 12 may comprise an Enhanced Data Rates for GSM Evolution (EDGE) network, an Integrated Digital Enhanced Network (IDEN), a Code Division Multiple

’619 Patent – Claim 22	Munje
	Access (CDMA) network, a Universal Mobile Telecommunications System (UMTS) network, or any 3rd Generation (3G) network. As will be seen hereinbelow, the embodiments of the present disclosure for provisioning MCD 22 supporting a single PDP context will be described regardless of any particular wireless network implementation.” Munje at 3:17-37. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[22b] a processor and memory containing instructions executable by the processor whereby the device is operable to:	Munje discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:

’619 Patent – Claim 22	Munje
	 Munje, Fig. 1.

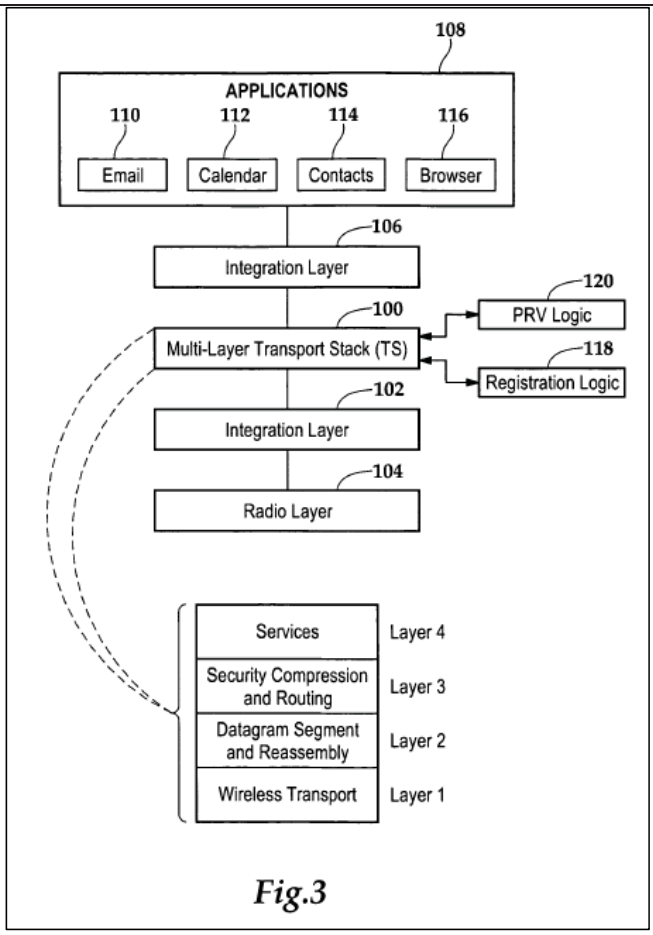
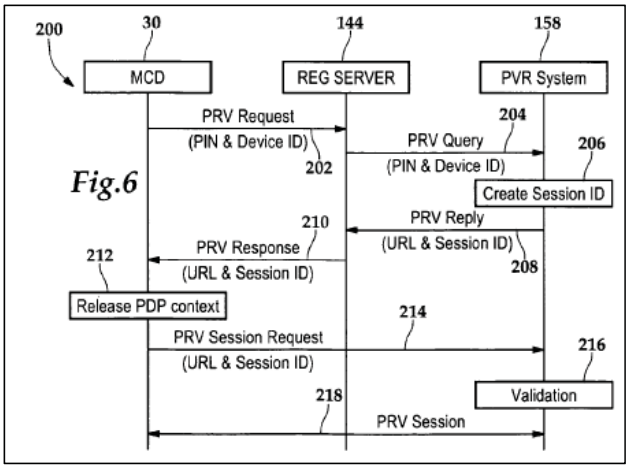
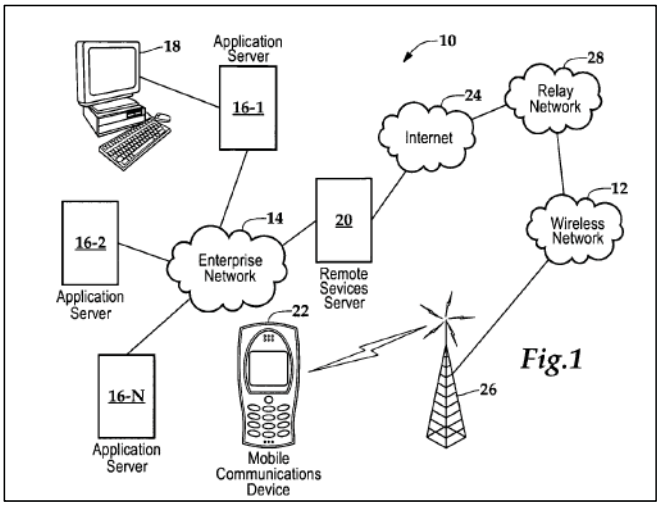

108
APPLICATIONS
110
112
114
116
Email
Calendar
Contacts
Browser
106
Integration Layer
120
PRV Logic
100
Multi-Layer Transport Stack (TS)
118
Registration Logic
102
Integration Layer
104
Radio Layer
Services
Layer 4
Security Compression and Routing
Layer 3
Datagram Segment and Reassembly
Layer 2
Wireless Transport
Layer 1

Fig.3

’619 Patent – Claim 22	Munje
	Munje, Fig. 3.  *Fig.6* Munje, Fig. 6. “Referring now to the drawings, and more particularly to FIG. 1, depicted therein is an exemplary network environment 10 including a wireless packet data service network 12 wherein an embodiment of the present method may be practiced. An enterprise network 14 for serving a plurality of corporate users, which may be a packet-switched network, can include one or more geographic sites and be organized as a local area network (LAN), a wide area network (WAN), a metropolitan area network (MAN) or the like. A number of application servers 16-1 through 16-N disposed as part of the enterprise network 14 are operable to provide or effectuate a host of internal and external services such as email, video mail, Internet access, corporate data access, messaging, calendaring and scheduling, information management and the like.

’619 Patent – Claim 22	Munje
	Accordingly, a diverse array of personal information appliances 18 such as desktop computers, laptop computers, palmtop computers or the like may be operably networked to one or more of the application servers 16-i, i=1, 2, . . . , N, with respect to the services supported in the enterprise network 14.” Munje at 2:49-67. “Additionally, a remote services server 20 may be interfaced with the enterprise network 14 for enabling a corporate user to access or effectuate any of the services from a remote location using a suitable single PDP context mobile communications device (MCD) 22. A secure communication link with end-to-end encryption may be established that is mediated through an external IP network, i.e., a public packet-switched network such as the Internet 24, as well as the wireless packet data service network 12 operable with MCD 22 via suitable wireless network infrastructure that includes a base station 26. In one embodiment, a trusted relay network 28 may be disposed between the Internet 24 and the infrastructure of wireless packet data service network 12. By way of example, MCD 22 may be a data-enabled handheld device capable of receiving and sending messages, web browsing, interfacing with corporate application servers and the like.” Munje at 3:1-17. “Communication between the relay services node 132 and various application gateways and servers is effectuated using any suitable protocol, e.g., Server Relay Protocol (SRP), preferably over IP links. By way of illustration, remote services server 20 associated with the enterprise network 14 (shown in FIG. 1) communicates with the relay using SRP for effectuating internal data services with respect to the enterprise's mobile subscribers. Likewise, reference numerals 136 and 138 refer to external application gateways, such as Internet Service Provider (ISP) or Internet Access Provider (IAP) servers, and other gateways, respectively, which are also interfaced with the relay node 132 using SRP. A peer-to-peer server 140 may also be provided in operable connection with the relay node 132 for handling peer-level messaging between two

’619 Patent – Claim 22	Munje
	MCDs.” Munje at 5:50-64. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[22c] optically receive information including a displayed service activation code from a remote device;	Munje discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: 

’619 Patent – Claim 22	Munje
	Munje, Fig. 1.

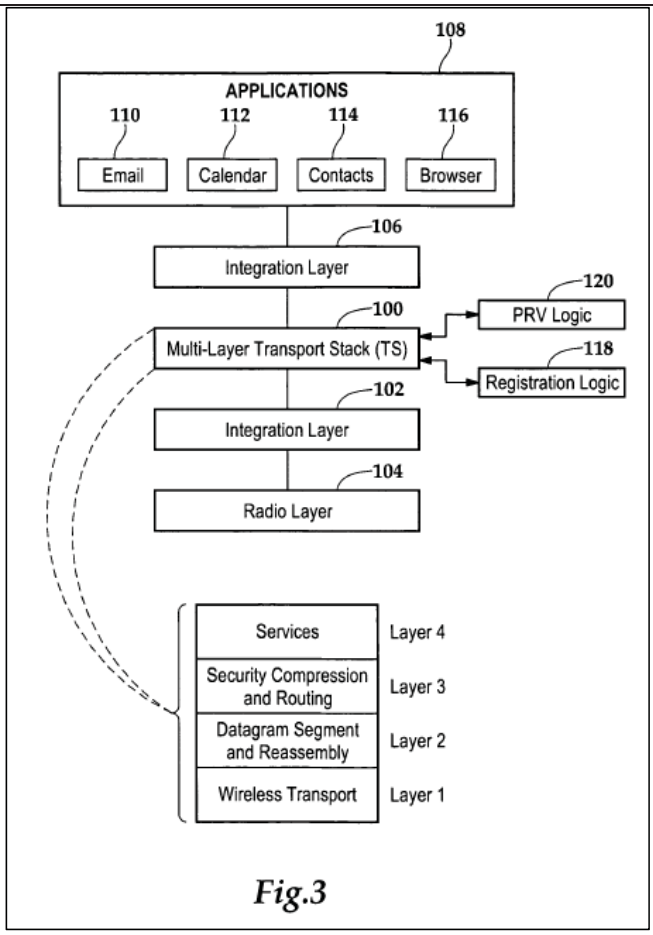
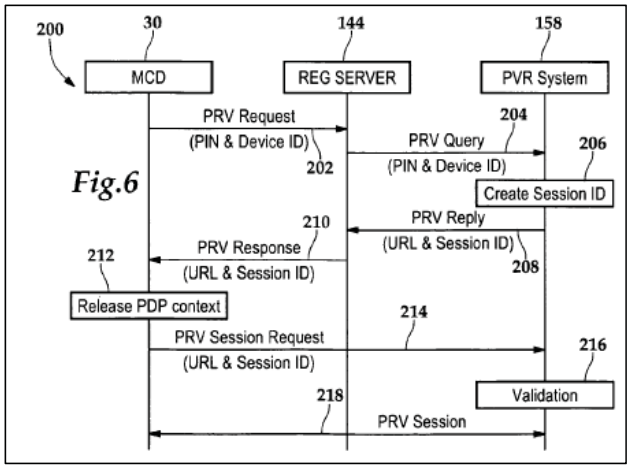

108
APPLICATIONS
110
112
114
116
Email
Calendar
Contacts
Browser
106
Integration Layer
120
PRV Logic
100
Multi-Layer Transport Stack (TS)
118
Registration Logic
102
Integration Layer
104
Radio Layer
Services
Layer 4
Security Compression and Routing
Layer 3
Datagram Segment and Reassembly
Layer 2
Wireless Transport
Layer 1

Fig.3

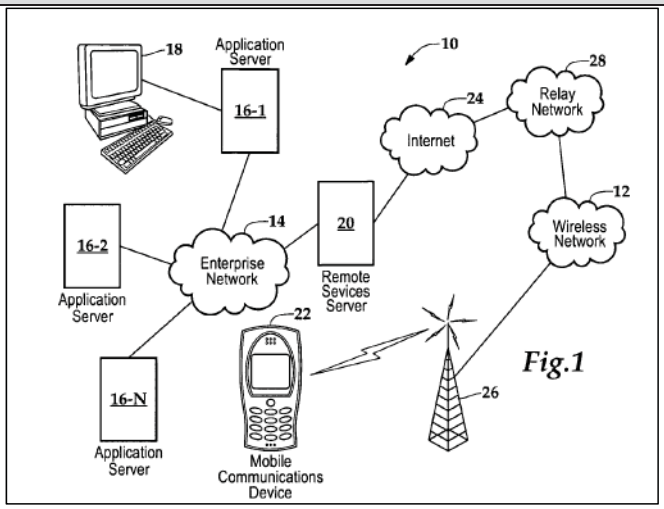
’619 Patent – Claim 22	Munje
	Munje, Fig. 3.  *Fig.6* Munje, Fig. 6. “Additionally, a remote services server 20 may be interfaced with the enterprise network 14 for enabling a corporate user to access or effectuate any of the services from a remote location using a suitable single PDP context mobile communications device (MCD) 22. A secure communication link with end-to-end encryption may be established that is mediated through an external IP network, i.e., a public packet-switched network such as the Internet 24, as well as the wireless packet data service network 12 operable with MCD 22 via suitable wireless network infrastructure that includes a base station 26. In one embodiment, a trusted relay network 28 may be disposed between the Internet 24 and the infrastructure of wireless packet data service network 12. By way of example, MCD 22 may be a data-enabled handheld device capable of receiving

’619 Patent – Claim 22	Munje
	and sending messages, web browsing, interfacing with corporate application servers and the like.” Munje at 3:1-17. “FIG. 3 also depicts a registration logic module 118 provided as part of the MCD's software environment that is disposed in operable communication with the transport stack 100 as well as the OS environment for effectuating registration procedures, as and when needed, with the serving relay network. In one implementation, where a PIN is not otherwise provided or associated with the MCD, the registration logic module 118 includes logic means operable to execute a registration procedure with the serving relay node to request and receive a PIN, which will allow identification of the MCD by this network node during future communication sessions therebetween. A PRV logic module 120 provided as part of the MCD's software environment is disposed in operable communication with the transport stack 100 as well as the OS environment. In one embodiment, the PRV logic module 120 comprises logic operable to generate a request including the PIN and at least one hardware device identifier associated with the MCD for transmission in a message to a network node such as the above mentioned serving relay node with an associated registration server, provisioning server and the like. As stated above, the PIN may be a required parameter in communications between an MCD and the serving relay node for identification and verification purposes.” Munje at 4:60-5:16. “Additionally, a database 142 may be provided in operable connection with the relay node 132 for handling and managing MCD location information. Preferably, this location information is stored by PIN of the MCDs, wherein the records maintain a particular device's last known location. A registration server 144 is operable for providing registration services for MCDs when they are initially activated or when the user re-registers due to moving to a different wireless network coverage area. In one implementation, the location information of registration server 144 may be programmed into an MCD.

’619 Patent – Claim 22	Munje
	When the MCD registers successfully, registration server 144 is operable to provide the serving relay node's location, whereupon data sessions may be engaged by the MCD.” Munje at 5:65-6:11. “FIG. 5 depicts a flowchart of an embodiment for establishing sequential PDP contexts with a MCD that supports a single PDP context such that the MCD can be provisioned over the air via a remote provisioning system. In the present embodiment, the communication sessions may be both web based and non web based communication sessions preferably using Wireless Application Protocol (WAP) or other suitable communication protocol. Prior to full utilization of the MCD, certain aspect of the device's overall functionality may need to be provisioned such as particular parameters to enable information to be pushed to the MCD. The provisioning of these aspects of the MCD may require authentication of the device, via a PIN, a device identifier or both, prior to provisioning. When the MCD is manufactured, one or more device identifiers such as IMEI, IMSI, ESN, MIN or the like are typically associated with the device. A PIN for these desires services, on the other hand, may not be assigned to the device upon manufacturing requiring the user to acquire such a PIN directly from the service provider via an over the air request and response sequence, which may take place with little or no user intervention. Additionally, once the MCD is deployed, it may be provided with an IP address since it is an IP appliance operable with a wireless packet data service network. Once the device has acquired the PIN relating to the aspects of the device the user desires to provision, it is now desirable to make the provisioning process as seamless as possible such as through the use of a web browser. It has been found, however, that many web browsers used in MCDs are not capable of retrieving and using PIN and device identifier information. In addition, it has been found that many MCDs are capable of only a single PDP context. The present disclosure, however, provides for sequential PDP contexts on the MCD and for communicating the PIN information to the web browser to allow the web browser to establish a communication session with the

’619 Patent – Claim 22	Munje
	appropriate provisioning system. As such, those of ordinary skill in the art should recognized that the present disclosure is not only applicable to single PDP context MCDs but also to any MCD/network system wherein the two required PDP contexts cannot simultaneously be active including, but not limited to, a MCD currently conducting its maximum number of PDP contexts, a network capable of supporting only one PDP context with a given MCD or the like. Specifically, as detailed in method 170 of FIG. 5, once the MCD has the appropriate PIN, the transport stack of the MCD establishes a first data context, which is preferably a non web based PDP context with the registration server (block 172). The transport stack accesses the PIN and device identifier information and transmits a request for parameters to the registration server (block 174). In one embodiment, this request for parameter includes the PIN and a device identifier. This information is then communicated from the registration server to the provisioning system which may be colocated, integrate or otherwise communicably associated with the registration server. The provisioning system can then generate the requested parameters which, in the present example, are a URL associated with the provisioning system and a session ID appended thereto which is preferably based upon the PIN and the device identifier such as by using a hashing technique. Preferably, the provisioning system starts a clock to establish a time frame within which the session ID will be valid. The provisioning system than communicates the requested parameters to the registration server which is still in communication with the MCD via the first data context. The registration server then provides a response including the requested parameters (the URL with session ID parameters) to the MCD which receives this information via the transport stack (block 176). Once the MCD has obtained the requested parameters, the first data context between the MCD and the registration server is automatically released (block 178). The requested parameters are then passed to the web browser which automatically launches the web page associated with the URL, which includes the session ID such that the device information of the MCD is

'619 Patent – Claim 22	Munje
	known to the provisioning system. This establishes a second data context, which is preferably a web based PDP context with the provisioning system (block 180). In this communication session, the aspects of the MCD that are associated with this service provider can now be provisioned over the air using well known data entry techniques via the web browser (block 182). As such, the MCD can be seamlessly provisioned by establishing one data context with a registration server to transmit a request for parameters and receive a response including the parameters then automatically releasing that data context and establishing a second data context by transmitting the parameters to a provisioning system." Munje at 6:44-7:61. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[22d] register the remote device for access to a messaging account using the service activation code;	Munje discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:

’619 Patent – Claim 22	Munje
	 Munje, Fig. 1.

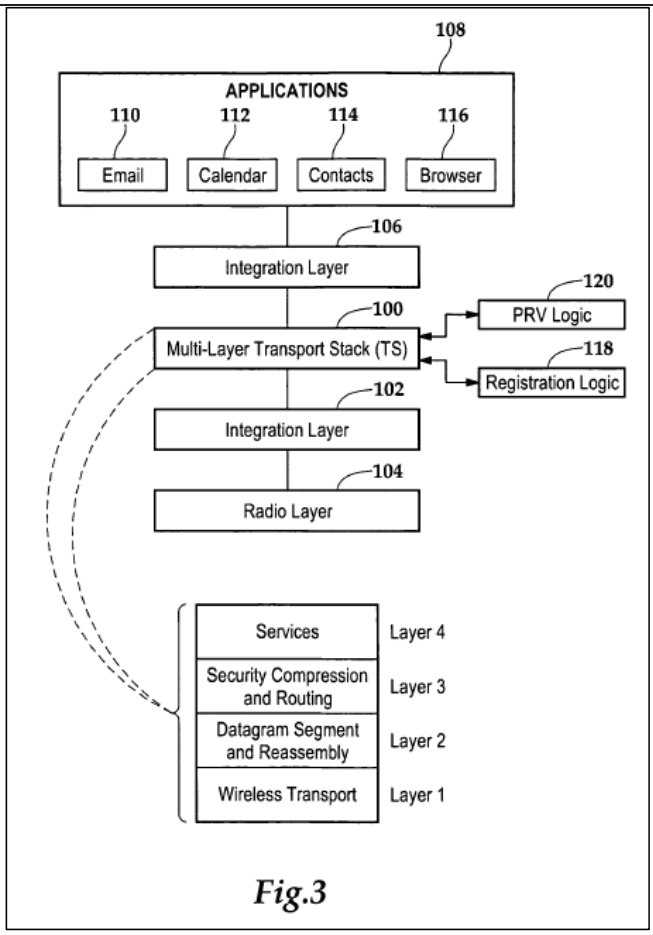
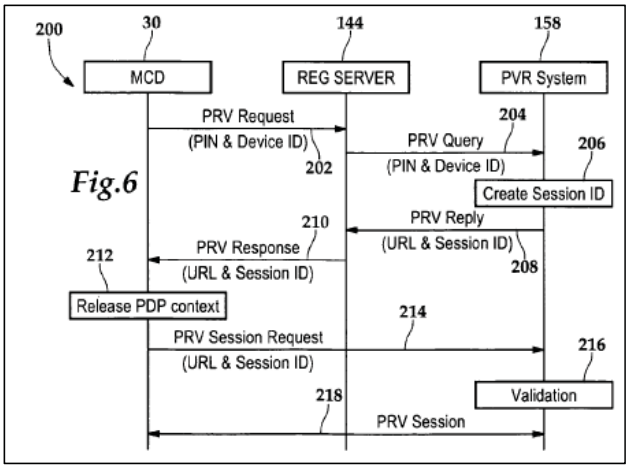
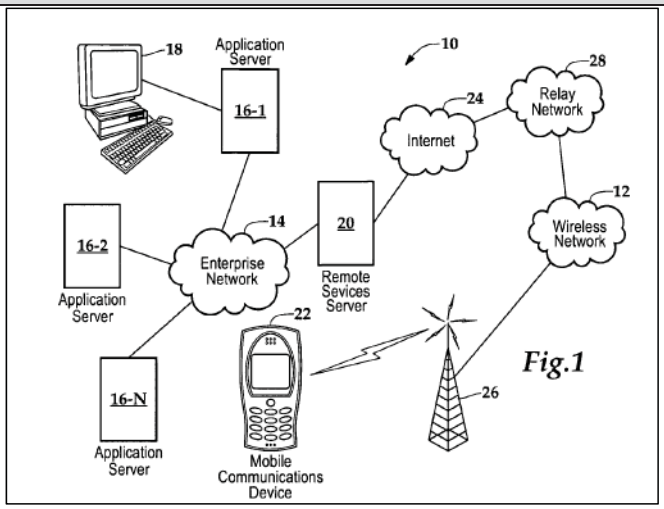

108
APPLICATIONS
110
112
114
116
Email
Calendar
Contacts
Browser
106
Integration Layer
120
PRV Logic
100
Multi-Layer Transport Stack (TS)
118
Registration Logic
102
Integration Layer
104
Radio Layer
Services
Layer 4
Security Compression and Routing
Layer 3
Datagram Segment and Reassembly
Layer 2
Wireless Transport
Layer 1

Fig.3

’619 Patent – Claim 22	Munje
	Munje, Fig. 3.  *Fig.6* Munje, Fig. 6. “FIG. 3 depicts a software architectural view of a mobile communications device operable according to one embodiment for provisioning certain aspects of the MCD regardless of the manufacturer of the MCD or the wireless service provider. A multi-layer transport stack (TS) 100 is operable to provide a generic data transport protocol for any type of corporate data, including email, via a reliable, secure and seamless continuous connection to a wireless packet data service network. As illustrated in the embodiment of FIG. 3, an integration layer 102 is operable as an interface between the MCD's radio layer 104 and the transport stack 100. Likewise, another integration layer 106 is provided for interfacing between the transport stack 100 and the user applications 108 supported on the MCD, e.g., email 110, calendar/scheduler 112, contact

’619 Patent – Claim 22	Munje
	management 114 and web browser 116. Although not specifically shown, the transport stack 100 may also be interfaced with the MCD's operating system. In another implementation, the transport stack 100 may be provided as part of a data communications client module operable as a host-independent virtual machine on a mobile device. The bottom layer (Layer 1) of the transport stack 100 is operable as an interface to the wireless network's packet layer. Layer 1 handles basic service coordination within the exemplary network environment 10 shown in FIG. 1. For example, when an MCD roams from one carrier network to another, Layer 1 verifies that the packets are relayed to the appropriate wireless network and that any packets that are pending from the previous network are rerouted to the current network. The top layer (Layer 4) exposes various application interfaces to the services supported on the MCD. The remaining two layers, Layer 2 and Layer 3, are responsible for datagram segmentation/reassembly and security, compression and routing, respectively. FIG. 3 also depicts a registration logic module 118 provided as part of the MCD's software environment that is disposed in operable communication with the transport stack 100 as well as the OS environment for effectuating registration procedures, as and when needed, with the serving relay network. In one implementation, where a PIN is not otherwise provided or associated with the MCD, the registration logic module 118 includes logic means operable to execute a registration procedure with the serving relay node to request and receive a PIN, which will allow identification of the MCD by this network node during future communication sessions therebetween.” Munje at 4:26-5:4. “FIG. 6 depicts a message flow diagram with respect to establishing sequential PDP contexts with a MCD that supports a single PDP context such that the MCD can be provisioned over the air via a remote provisioning system that is generally designated 200. MCD 30 establishes a PDP context wherein a PRV request message 202 is transmitted by MCD 30 to a network node, e.g.,

’619 Patent – Claim 22	Munje
	registration server 144, wherein the request message 202 includes a PIN as well as a device identifier as parametric information. Registration server 144 queries suitable service logic, which may be embodied as the provisioning system 158 associated with the relay services network described above, by issuing a PRV query 204 thereto, which includes the parametric information received in the PRV request 202. The provisioning system's PRV logic is operable to validate the request and provide, via a PRV reply 208 to the registration server 144, a message including a URL having session ID parameters appended thereto. Within the first PDP context, this information is then transmitted to MCD 30 via PRV response message 210 from registration server 144. Thereafter, MCD 30 automatically releases the first PDP context 212 and establishes a second PDP context with the PVR system 158. This communication session is established by MCD 30 sending a PRV session request 214 including the URL having session ID parameters. In response thereto, the PVR system 158 is operable to validate 216 the request to, among other things, assure that the session ID has not expire. Upon successful validation, a provisioning session 218 between MCD 30 and PVR system 158 may occur to provision the associated aspects of MCD 30.” Munje at 7:62-8:23. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[22e] receive a message for the messaging account;	Munje discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:

’619 Patent – Claim 22	Munje
	 Munje, Fig. 1.

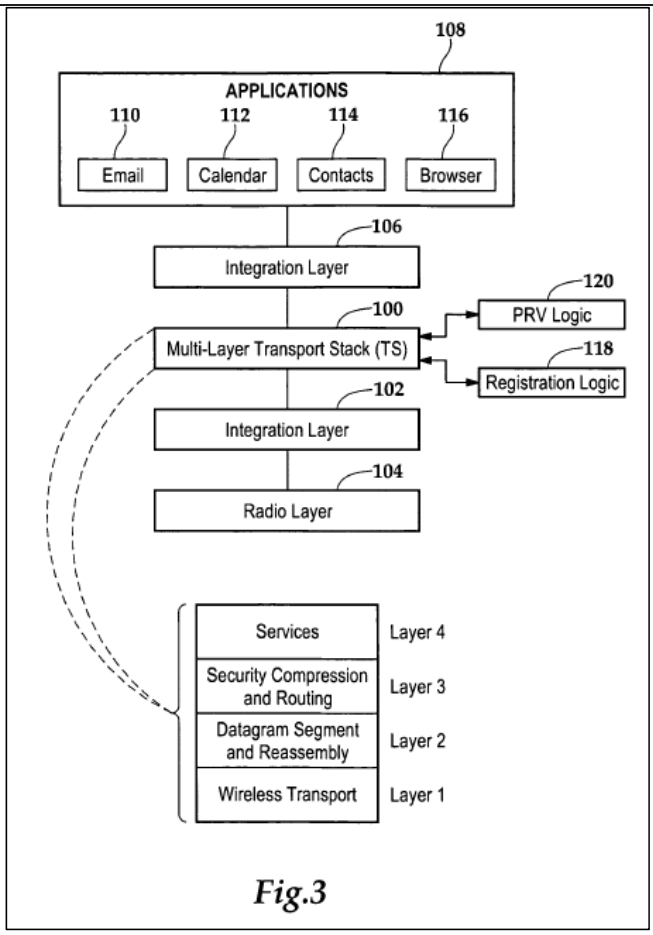
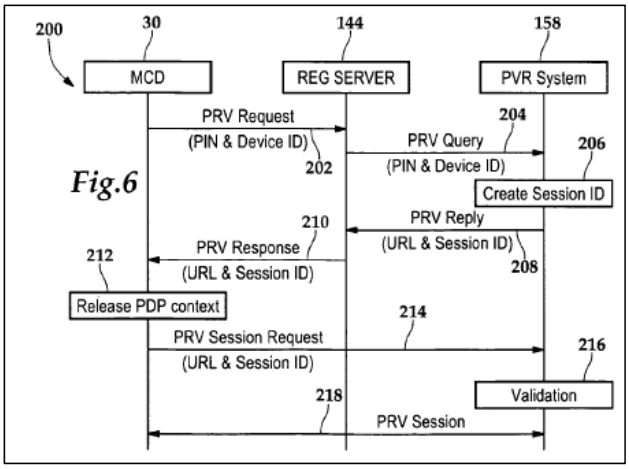
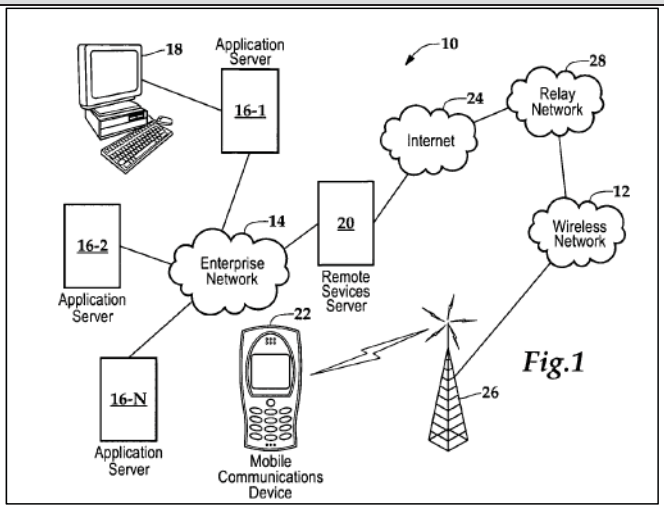

108
APPLICATIONS
110
112
114
116
Email
Calendar
Contacts
Browser
106
Integration Layer
120
PRV Logic
100
Multi-Layer Transport Stack (TS)
118
Registration Logic
102
Integration Layer
104
Radio Layer
Services
Layer 4
Security Compression and Routing
Layer 3
Datagram Segment and Reassembly
Layer 2
Wireless Transport
Layer 1

Fig.3

’619 Patent – Claim 22	Munje
	Munje, Fig. 3.  Munje, Fig. 6. “Referring now to the drawings, and more particularly to FIG. 1, depicted therein is an exemplary network environment 10 including a wireless packet data service network 12 wherein an embodiment of the present method may be practiced. An enterprise network 14 for serving a plurality of corporate users, which may be a packet-switched network, can include one or more geographic sites and be organized as a local area network (LAN), a wide area network (WAN), a metropolitan area network (MAN) or the like. A number of application servers 16-1 through 16-N disposed as part of the enterprise network 14 are operable to provide or effectuate a host of internal and external services such as email, video mail, Internet access, corporate data access, messaging, calendaring and scheduling, information management and the like.

’619 Patent – Claim 22	Munje
	Accordingly, a diverse array of personal information appliances 18 such as desktop computers, laptop computers, palmtop computers or the like may be operably networked to one or more of the application servers 16-i, i=1, 2, . . . , N, with respect to the services supported in the enterprise network 14.” Munje at 2:49-3:1. “Additionally, a remote services server 20 may be interfaced with the enterprise network 14 for enabling a corporate user to access or effectuate any of the services from a remote location using a suitable single PDP context mobile communications device (MCD) 22. A secure communication link with end-to-end encryption may be established that is mediated through an external IP network, i.e., a public packet-switched network such as the Internet 24, as well as the wireless packet data service network 12 operable with MCD 22 via suitable wireless network infrastructure that includes a base station 26 . In one embodiment, a trusted relay network 28 may be disposed between the Internet 24 and the infrastructure of wireless packet data service network 12. By way of example, MCD 22 may be a data-enabled handheld device capable of receiving and sending messages, web browsing, interfacing with corporate application servers and the like.” Munje at 3:1-17. “FIG. 3 depicts a software architectural view of a mobile communications device operable according to one embodiment for provisioning certain aspects of the MCD regardless of the manufacturer of the MCD or the wireless service provider. A multi-layer transport stack (TS) 100 is operable to provide a generic data transport protocol for any type of corporate data, including email, via a reliable, secure and seamless continuous connection to a wireless packet data service network. As illustrated in the embodiment of FIG. 3, an integration layer 102 is operable as an interface between the MCD's radio layer 104 and the transport stack 100. Likewise, another integration layer 106 is provided for interfacing between the transport stack 100 and the user applications 108 supported on the MCD, e.g., email 110 , calendar/scheduler 112, contact management 114 and web browser 116. Although not specifically shown, the

’619 Patent – Claim 22	Munje
	transport stack 100 may also be interfaced with the MCD's operating system. In another implementation, the transport stack 100 may be provided as part of a data communications client module operable as a host-independent virtual machine on a mobile device.” Munje at 4:26-5:4. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[22f] encrypt the message using an encryption key; and	Munje discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:

’619 Patent – Claim 22	Munje
	 Munje, Fig. 1.

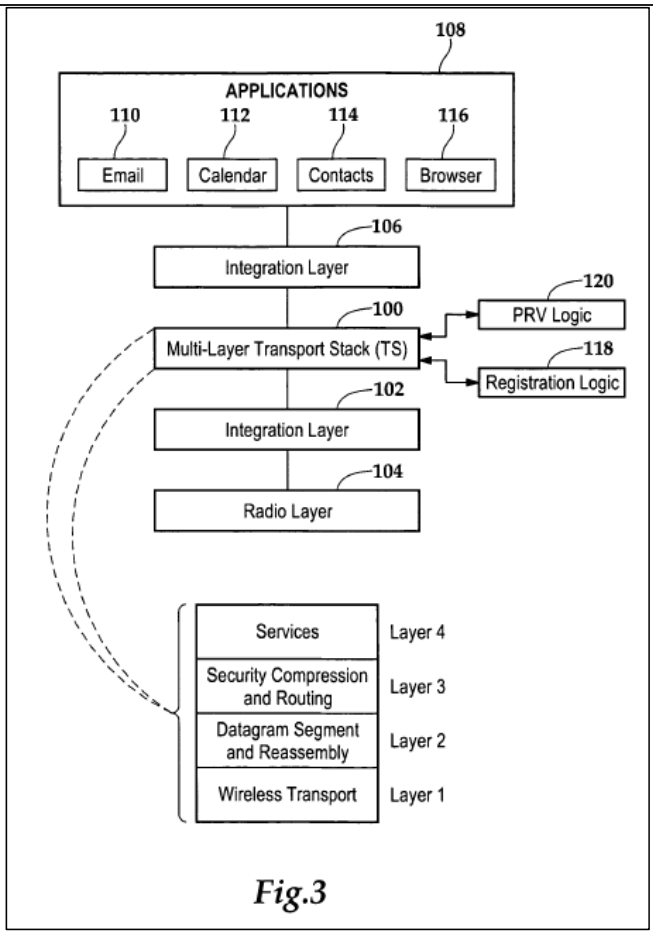
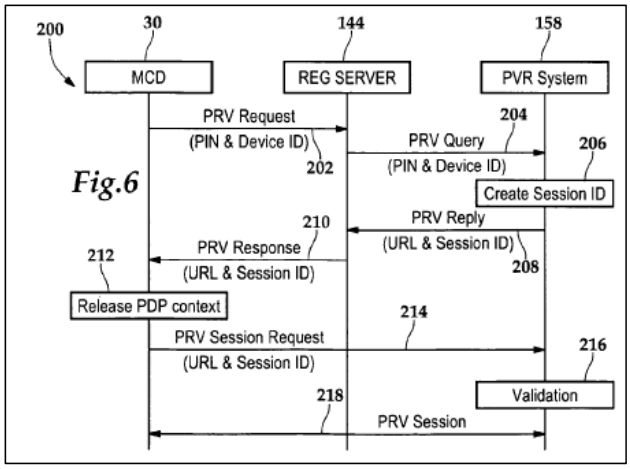
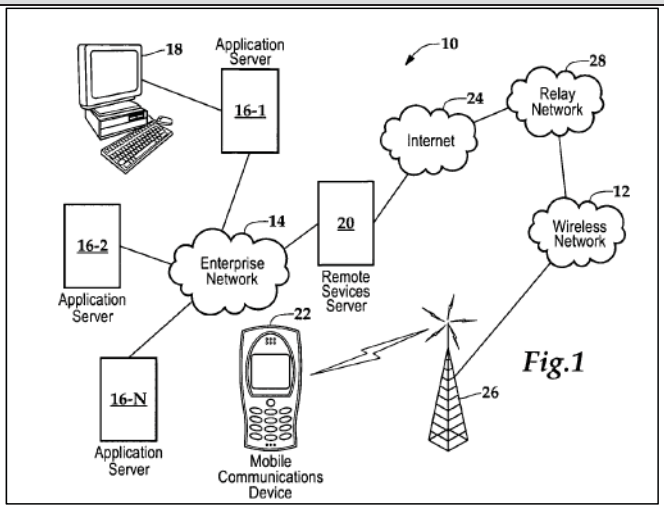

108
APPLICATIONS
110
112
114
116
Email
Calendar
Contacts
Browser
106
Integration Layer
120
PRV Logic
100
Multi-Layer Transport Stack (TS)
118
Registration Logic
102
Integration Layer
104
Radio Layer
Services
Layer 4
Security Compression and Routing
Layer 3
Datagram Segment and Reassembly
Layer 2
Wireless Transport
Layer 1

Fig.3

’619 Patent – Claim 22	Munje
	Munje, Fig. 3.  Munje, Fig. 6. “Referring now to the drawings, and more particularly to FIG. 1, depicted therein is an exemplary network environment 10 including a wireless packet data service network 12 wherein an embodiment of the present method may be practiced. An enterprise network 14 for serving a plurality of corporate users, which may be a packet-switched network, can include one or more geographic sites and be organized as a local area network (LAN), a wide area network (WAN), a metropolitan area network (MAN) or the like. A number of application servers 16-1 through 16-N disposed as part of the enterprise network 14 are operable to provide or effectuate a host of internal and external services such as email, video mail, Internet access, corporate data access, messaging, calendaring and scheduling, information management and the like.

’619 Patent – Claim 22	Munje
	Accordingly, a diverse array of personal information appliances 18 such as desktop computers, laptop computers, palmtop computers or the like may be operably networked to one or more of the application servers 16-i, i=1, 2, . . . , N, with respect to the services supported in the enterprise network 14.” Munje at 2:49-3:1. “Additionally, a remote services server 20 may be interfaced with the enterprise network 14 for enabling a corporate user to access or effectuate any of the services from a remote location using a suitable single PDP context mobile communications device (MCD) 22. A secure communication link with end-to-end encryption may be established that is mediated through an external IP network, i.e., a public packet-switched network such as the Internet 24, as well as the wireless packet data service network 12 operable with MCD 22 via suitable wireless network infrastructure that includes a base station 26 . In one embodiment, a trusted relay network 28 may be disposed between the Internet 24 and the infrastructure of wireless packet data service network 12. By way of example, MCD 22 may be a data-enabled handheld device capable of receiving and sending messages, web browsing, interfacing with corporate application servers and the like.” Munje at 3:1-17. “FIG. 3 depicts a software architectural view of a mobile communications device operable according to one embodiment for provisioning certain aspects of the MCD regardless of the manufacturer of the MCD or the wireless service provider. A multi-layer transport stack (TS) 100 is operable to provide a generic data transport protocol for any type of corporate data, including email, via a reliable, secure and seamless continuous connection to a wireless packet data service network. As illustrated in the embodiment of FIG. 3, an integration layer 102 is operable as an interface between the MCD's radio layer 104 and the transport stack 100. Likewise, another integration layer 106 is provided for interfacing between the transport stack 100 and the user applications 108 supported on the MCD, e.g., email 110 , calendar/scheduler 112, contact management 114 and web browser 116. Although not specifically shown, the

’619 Patent – Claim 22	Munje
	transport stack 100 may also be interfaced with the MCD's operating system. In another implementation, the transport stack 100 may be provided as part of a data communications client module operable as a host-independent virtual machine on a mobile device.” Munje at 4:26-5:4. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[22g] send the message to the remote device,	Munje discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:

’619 Patent – Claim 22	Munje
	 Munje, Fig. 1.

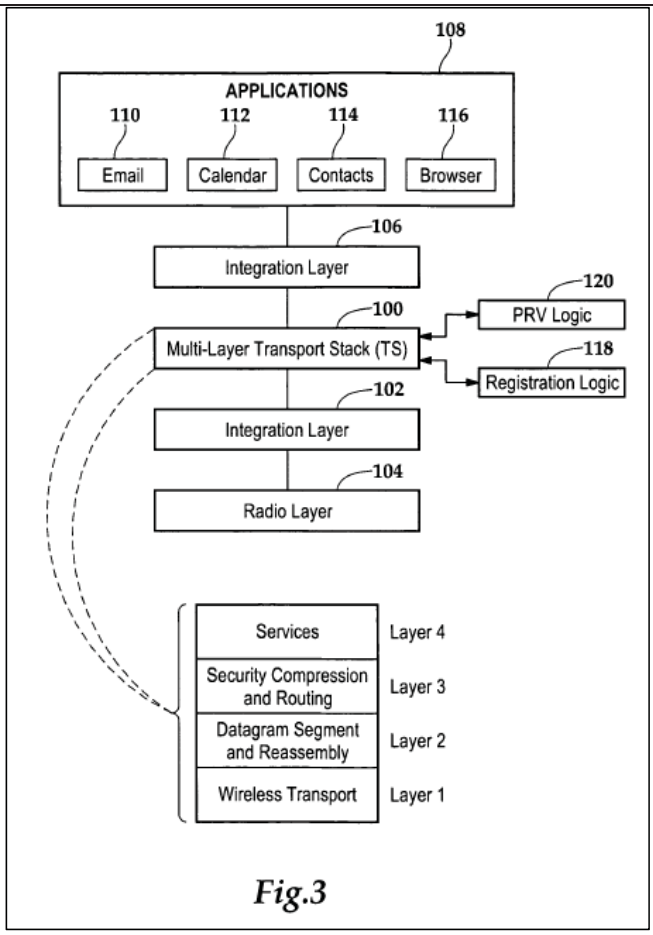
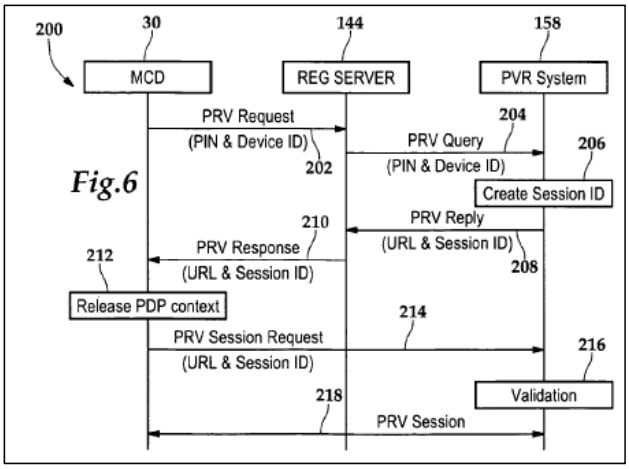
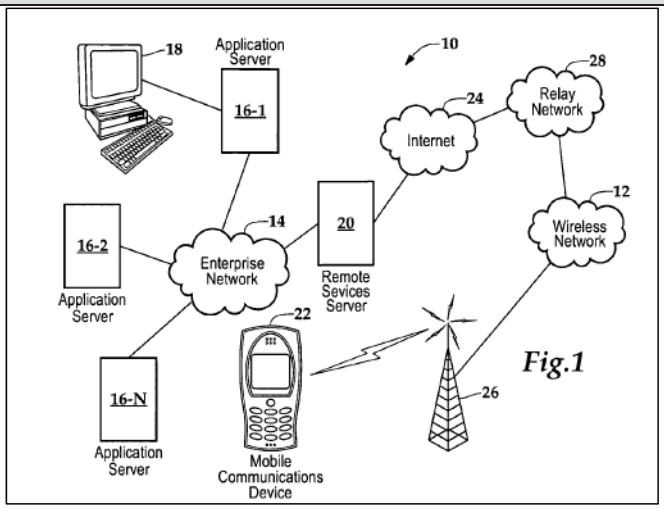

108
APPLICATIONS
110
112
114
116
Email
Calendar
Contacts
Browser
106
Integration Layer
120
PRV Logic
100
Multi-Layer Transport Stack (TS)
118
Registration Logic
102
Integration Layer
104
Radio Layer
Services
Layer 4
Security Compression and Routing
Layer 3
Datagram Segment and Reassembly
Layer 2
Wireless Transport
Layer 1

Fig.3

’619 Patent – Claim 22	Munje
	Munje, Fig. 3.  Munje, Fig. 6. “Referring now to the drawings, and more particularly to FIG. 1, depicted therein is an exemplary network environment 10 including a wireless packet data service network 12 wherein an embodiment of the present method may be practiced. An enterprise network 14 for serving a plurality of corporate users, which may be a packet-switched network, can include one or more geographic sites and be organized as a local area network (LAN), a wide area network (WAN), a metropolitan area network (MAN) or the like. A number of application servers 16-1 through 16-N disposed as part of the enterprise network 14 are operable to provide or effectuate a host of internal and external services such as email, video mail, Internet access, corporate data access, messaging, calendaring and scheduling, information management and the like.

’619 Patent – Claim 22	Munje
	Accordingly, a diverse array of personal information appliances 18 such as desktop computers, laptop computers, palmtop computers or the like may be operably networked to one or more of the application servers 16-i, i=1, 2, . . . , N, with respect to the services supported in the enterprise network 14.” Munje at 2:49-3:1. “Additionally, a remote services server 20 may be interfaced with the enterprise network 14 for enabling a corporate user to access or effectuate any of the services from a remote location using a suitable single PDP context mobile communications device (MCD) 22. A secure communication link with end-to-end encryption may be established that is mediated through an external IP network, i.e., a public packet-switched network such as the Internet 24, as well as the wireless packet data service network 12 operable with MCD 22 via suitable wireless network infrastructure that includes a base station 26 . In one embodiment, a trusted relay network 28 may be disposed between the Internet 24 and the infrastructure of wireless packet data service network 12. By way of example, MCD 22 may be a data-enabled handheld device capable of receiving and sending messages, web browsing, interfacing with corporate application servers and the like.” Munje at 3:1-17. “FIG. 3 depicts a software architectural view of a mobile communications device operable according to one embodiment for provisioning certain aspects of the MCD regardless of the manufacturer of the MCD or the wireless service provider. A multi-layer transport stack (TS) 100 is operable to provide a generic data transport protocol for any type of corporate data, including email, via a reliable, secure and seamless continuous connection to a wireless packet data service network. As illustrated in the embodiment of FIG. 3, an integration layer 102 is operable as an interface between the MCD's radio layer 104 and the transport stack 100. Likewise, another integration layer 106 is provided for interfacing between the transport stack 100 and the user applications 108 supported on the MCD, e.g., email 110 , calendar/scheduler 112, contact management 114 and web browser 116. Although not specifically shown, the

’619 Patent – Claim 22	Munje
	transport stack 100 may also be interfaced with the MCD's operating system. In another implementation, the transport stack 100 may be provided as part of a data communications client module operable as a host-independent virtual machine on a mobile device.” Munje at 4:26-5:4. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[22h] wherein the device is authenticated to access the messaging account.	Munje discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:

’619 Patent – Claim 22	Munje
	 Munje, Fig. 1.

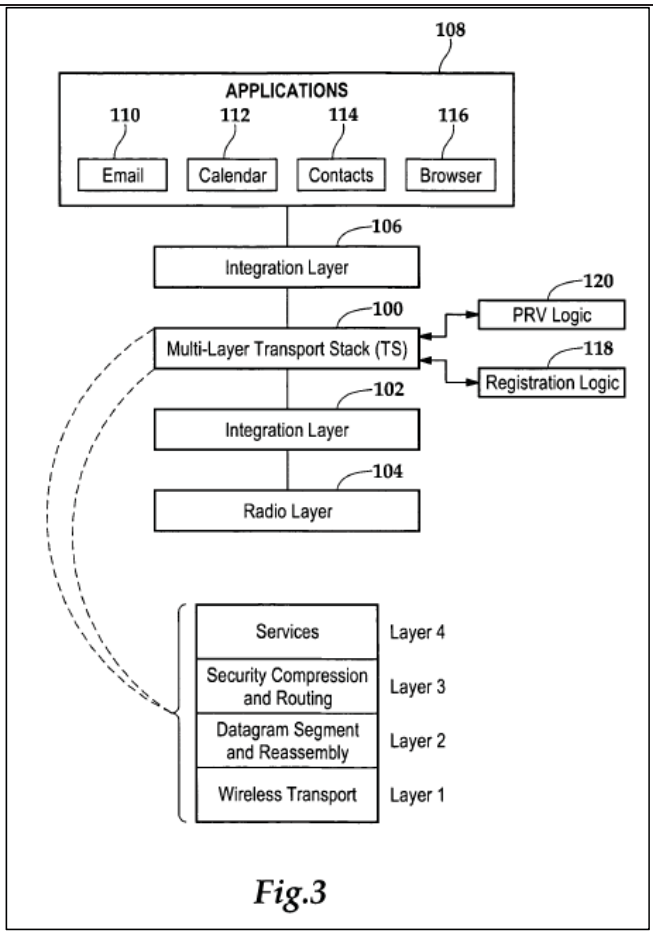
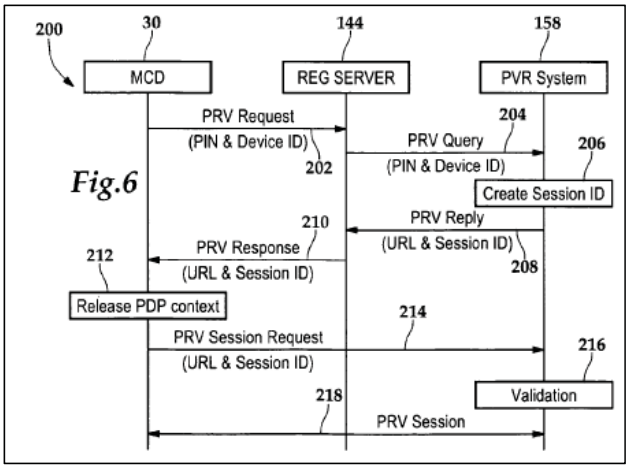

108
APPLICATIONS
110
112
114
116
Email
Calendar
Contacts
Browser
106
Integration Layer
120
PRV Logic
100
Multi-Layer Transport Stack (TS)
118
Registration Logic
102
Integration Layer
104
Radio Layer
Services
Layer 4
Security Compression and Routing
Layer 3
Datagram Segment and Reassembly
Layer 2
Wireless Transport
Layer 1

Fig.3

’619 Patent – Claim 22	Munje
	Munje, Fig. 3.  Munje, Fig. 6. “FIG. 3 depicts a software architectural view of a mobile communications device operable according to one embodiment for provisioning certain aspects of the MCD regardless of the manufacturer of the MCD or the wireless service provider. A multi-layer transport stack (TS) 100 is operable to provide a generic data transport protocol for any type of corporate data, including email, via a reliable, secure and seamless continuous connection to a wireless packet data service network. As illustrated in the embodiment of FIG. 3, an integration layer 102 is operable as an interface between the MCD's radio layer 104 and the transport stack 100. Likewise, another integration layer 106 is provided for interfacing between the transport stack 100 and the user applications 108 supported on the MCD, e.g., email 110, calendar/scheduler 112, contact

’619 Patent – Claim 22	Munje
	management 114 and web browser 116. Although not specifically shown, the transport stack 100 may also be interfaced with the MCD's operating system. In another implementation, the transport stack 100 may be provided as part of a data communications client module operable as a host-independent virtual machine on a mobile device. The bottom layer (Layer 1) of the transport stack 100 is operable as an interface to the wireless network's packet layer. Layer 1 handles basic service coordination within the exemplary network environment 10 shown in FIG. 1. For example, when an MCD roams from one carrier network to another, Layer 1 verifies that the packets are relayed to the appropriate wireless network and that any packets that are pending from the previous network are rerouted to the current network. The top layer (Layer 4) exposes various application interfaces to the services supported on the MCD. The remaining two layers, Layer 2 and Layer 3, are responsible for datagram segmentation/reassembly and security, compression and routing, respectively. FIG. 3 also depicts a registration logic module 118 provided as part of the MCD's software environment that is disposed in operable communication with the transport stack 100 as well as the OS environment for effectuating registration procedures, as and when needed, with the serving relay network. In one implementation, where a PIN is not otherwise provided or associated with the MCD, the registration logic module 118 includes logic means operable to execute a registration procedure with the serving relay node to request and receive a PIN, which will allow identification of the MCD by this network node during future communication sessions therebetween.” Munje at 4:26-5:4. “Additionally, a remote services server 20 may be interfaced with the enterprise network 14 for enabling a corporate user to access or effectuate any of the services from a remote location using a suitable single PDP context mobile communications device (MCD) 22. A secure communication link with end-to-end encryption may be established that is mediated through an external

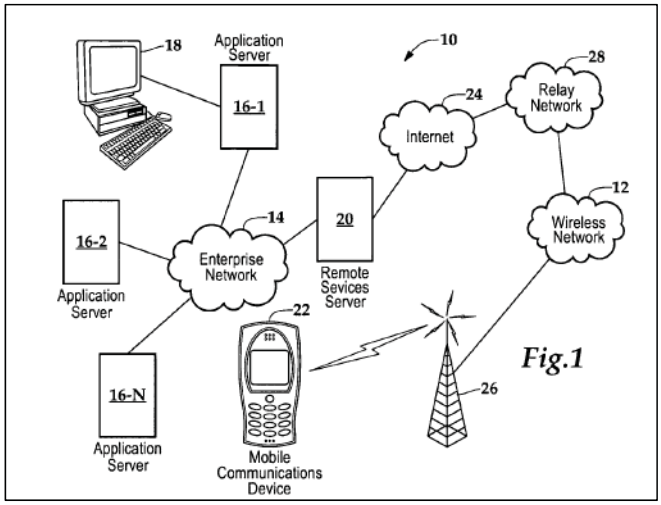
’619 Patent – Claim 22	Munje
	IP network, i.e., a public packet-switched network such as the Internet 24, as well as the wireless packet data service network 12 operable with MCD 22 via suitable wireless network infrastructure that includes a base station 26. In one embodiment, a trusted relay network 28 may be disposed between the Internet 24 and the infrastructure of wireless packet data service network 12. By way of example, MCD 22 may be a data-enabled handheld device capable of receiving and sending messages, web browsing, interfacing with corporate application servers and the like.” Munje at 3:1-17. “FIG. 3 also depicts a registration logic module 118 provided as part of the MCD's software environment that is disposed in operable communication with the transport stack 100 as well as the OS environment for effectuating registration procedures, as and when needed, with the serving relay network. In one implementation, where a PIN is not otherwise provided or associated with the MCD, the registration logic module 118 includes logic means operable to execute a registration procedure with the serving relay node to request and receive a PIN, which will allow identification of the MCD by this network node during future communication sessions therebetween. A PRV logic module 120 provided as part of the MCD's software environment is disposed in operable communication with the transport stack 100 as well as the OS environment. In one embodiment, the PRV logic module 120 comprises logic operable to generate a request including the PIN and at least one hardware device identifier associated with the MCD for transmission in a message to a network node such as the above mentioned serving relay node with an associated registration server, provisioning server and the like. As stated above, the PIN may be a required parameter in communications between an MCD and the serving relay node for identification and verification purposes.” Munje at 4:60-5:16. “Additionally, a database 142 may be provided in operable connection with the relay node 132 for handling and managing MCD location information.

’619 Patent – Claim 22	Munje
	Preferably, this location information is stored by PIN of the MCDs, wherein the records maintain a particular device's last known location. A registration server 144 is operable for providing registration services for MCDs when they are initially activated or when the user re-registers due to moving to a different wireless network coverage area. In one implementation, the location information of registration server 144 may be programmed into an MCD. When the MCD registers successfully, registration server 144 is operable to provide the serving relay node's location, whereupon data sessions may be engaged by the MCD.” Munje at 5:65-6:11. “FIG. 5 depicts a flowchart of an embodiment for establishing sequential PDP contexts with a MCD that supports a single PDP context such that the MCD can be provisioned over the air via a remote provisioning system. In the present embodiment, the communication sessions may be both web based and non web based communication sessions preferably using Wireless Application Protocol (WAP) or other suitable communication protocol. Prior to full utilization of the MCD, certain aspect of the device's overall functionality may need to be provisioned such as particular parameters to enable information to be pushed to the MCD. The provisioning of these aspects of the MCD may require authentication of the device, via a PIN, a device identifier or both, prior to provisioning. When the MCD is manufactured, one or more device identifiers such as IMEI, IMSI, ESN, MIN or the like are typically associated with the device. A PIN for these desires services, on the other hand, may not be assigned to the device upon manufacturing requiring the user to acquire such a PIN directly from the service provider via an over the air request and response sequence, which may take place with little or no user intervention. Additionally, once the MCD is deployed, it may be provided with an IP address since it is an IP appliance operable with a wireless packet data service network. Once the device has acquired the PIN relating to the aspects of the device the user desires to provision, it is now desirable to make the provisioning process as seamless as possible such as through the use of a web browser.

’619 Patent – Claim 22	Munje
	It has been found, however, that many web browsers used in MCDs are not capable of retrieving and using PIN and device identifier information. In addition, it has been found that many MCDs are capable of only a single PDP context. The present disclosure, however, provides for sequential PDP contexts on the MCD and for communicating the PIN information to the web browser to allow the web browser to establish a communication session with the appropriate provisioning system. As such, those of ordinary skill in the art should recognized that the present disclosure is not only applicable to single PDP context MCDs but also to any MCD/network system wherein the two required PDP contexts cannot simultaneously be active including, but not limited to, a MCD currently conducting its maximum number of PDP contexts, a network capable of supporting only one PDP context with a given MCD or the like. Specifically, as detailed in method 170 of FIG. 5, once the MCD has the appropriate PIN, the transport stack of the MCD establishes a first data context, which is preferably a non web based PDP context with the registration server (block 172). The transport stack accesses the PIN and device identifier information and transmits a request for parameters to the registration server (block 174). In one embodiment, this request for parameter includes the PIN and a device identifier. This information is then communicated from the registration server to the provisioning system which may be colocated, integrate or otherwise communicably associated with the registration server. The provisioning system can then generate the requested parameters which, in the present example, are a URL associated with the provisioning system and a session ID appended thereto which is preferably based upon the PIN and the device identifier such as by using a hashing technique. Preferably, the provisioning system starts a clock to establish a time frame within which the session ID will be valid. The provisioning system than communicates the requested parameters to the registration server which is still in communication with the MCD via the first data context. The registration server then provides a response including the requested parameters (the URL with session ID

’619 Patent – Claim 22	Munje
	parameters) to the MCD which receives this information via the transport stack (block 176). Once the MCD has obtained the requested parameters, the first data context between the MCD and the registration server is automatically released (block 178). The requested parameters are then passed to the web browser which automatically launches the web page associated with the URL, which includes the session ID such that the device information of the MCD is known to the provisioning system. This establishes a second data context, which is preferably a web based PDP context with the provisioning system (block 180). In this communication session, the aspects of the MCD that are associated with this service provider can now be provisioned over the air using well known data entry techniques via the web browser (block 182). As such, the MCD can be seamlessly provisioned by establishing one data context with a registration server to transmit a request for parameters and receive a response including the parameters then automatically releasing that data context and establishing a second data context by transmitting the parameters to a provisioning system.” Munje at 6:44-7:61. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

’619 Patent – Claim 23	Munje
[23] The device of claim 22, wherein the information including the service activation code	Munje discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:

’619 Patent – Claim 23	Munje
is received by the device in response to user input at the remote device.	*See* [22pre]-[22h], *above*.  Munje, Fig. 1.

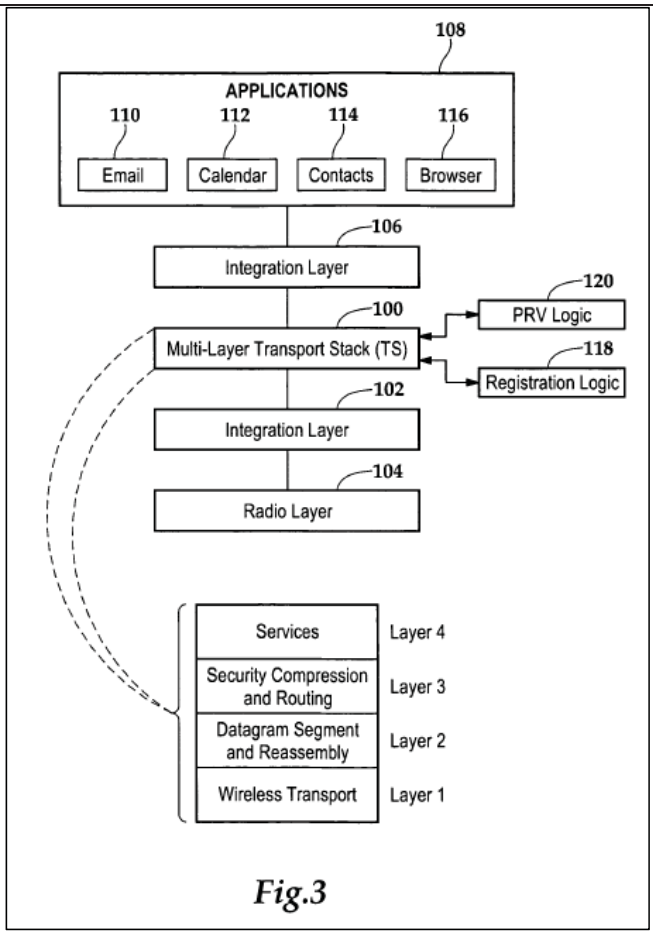
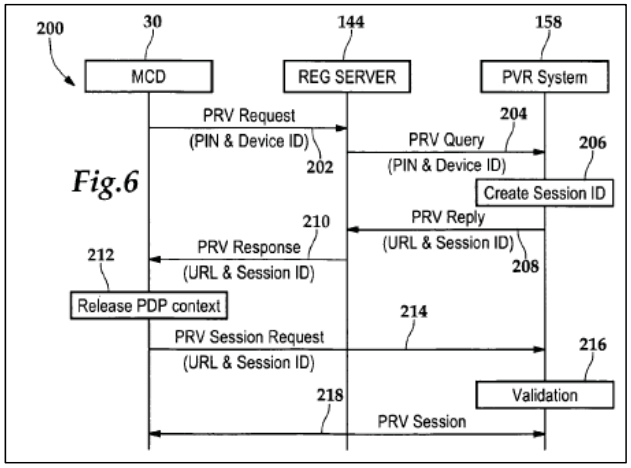

108
APPLICATIONS
110
112
114
116
Email
Calendar
Contacts
Browser
106
Integration Layer
120
PRV Logic
100
Multi-Layer Transport Stack (TS)
118
Registration Logic
102
Integration Layer
104
Radio Layer
Services
Layer 4
Security Compression and Routing
Layer 3
Datagram Segment and Reassembly
Layer 2
Wireless Transport
Layer 1

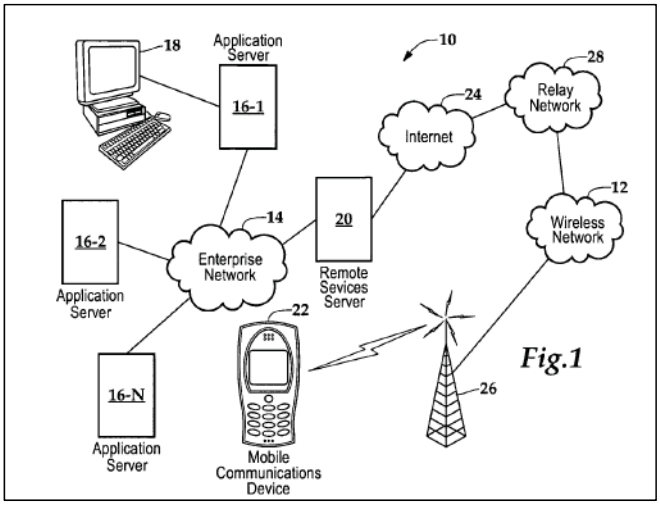
Fig.3

’619 Patent – Claim 23	Munje
	Munje, Fig. 3.  Munje, Fig. 6. “FIG. 3 also depicts a registration logic module 118 provided as part of the MCD's software environment that is disposed in operable communication with the transport stack 100 as well as the OS environment for effectuating registration procedures, as and when needed, with the serving relay network. In one implementation, where a PIN is not otherwise provided or associated with the MCD, the registration logic module 118 includes logic means operable to execute a registration procedure with the serving relay node to request and receive a PIN, which will allow identification of the MCD by this network node during future communication sessions there between. A PRV logic module 120 provided as part of the MCD's software environment

’619 Patent – Claim 23	Munje
	is disposed in operable communication with the transport stack 100 as well as the OS environment. In one embodiment, the PRV logic module 120 comprises logic operable to generate a request including the PIN and at least one hardware device identifier associated with the MCD for transmission in a message to a network node such as the above mentioned serving relay node with an associated registration server, provisioning server and the like. As stated above, the PIN may be a required parameter in communications between an MCD and the serving relay node for identification and verification purposes.” Munje at 4:65-5:16. “Specifically, as detailed in method 170 of FIG. 5, once the MCD has the appropriate PIN, the transport stack of the MCD establishes a first data context, which is preferably a non web based PDP context with the registration server (block 172). The transport stack accesses the PIN and device identifier information and transmits a request for parameters to the registration server (block 174). In one embodiment, this request for parameter includes the PIN and a device identifier. This information is then communicated from the registration server to the provisioning system which may be colocated, integrate or otherwise communicably associated with the registration server. The provisioning system can then generate the requested parameters which, in the present example, are a URL associated with the provisioning system and a session ID appended thereto which is preferably based upon the PIN and the device identifier such as by using a hashing technique.” Munje at 7:19-34. “FIG. 6 depicts a message flow diagram with respect to establishing sequential PDP contexts with a MCD that supports a single PDP context such that the MCD can be provisioned over the air via a remote provisioning system that is generally designated 200. MCD 30 establishes a PDP context wherein a PRV request message 202 is transmitted by MCD 30 to a network node, e.g., registration server 144, wherein the request message 202 includes a PIN as well as a device identifier as parametric information. Registration server 144 queries suitable service logic, which may be embodied as the provisioning system 158

'619 Patent – Claim 23	Munje
	associated with the relay services network described above, by issuing a PRV query 204 thereto, which includes the parametric information received in the PRV request 202. The provisioning system's PRV logic is operable to validate the request and provide, via a PRV reply 208 to the registration server 144, a message including a URL having session ID parameters appended thereto. Within the first PDP context, this information is then transmitted to MCD 30 via PRV response message 210 from registration server 144. Thereafter, MCD 30 automatically releases the first PDP context 212 and establishes a second PDP context with the PVR system 158. This communication session is established by MCD 30 sending a PRV session request 214 including the URL having session ID parameters. In response thereto, the PVR system 158 is operable to validate 216 the request to, among other things, assure that the session ID has not expire. Upon successful validation, a provisioning session 218 between MCD 30 and PVR system 158 may occur to provision the associated aspects of MCD 30." Munje at 7:62-8:23. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

'619 Patent – Claim 24	Munje
[24] The device of claim 22, wherein the information including the service activation code is received by the device in an off-line	Munje discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:

’619 Patent – Claim 24	Munje
communication.	*See* [22pre]-[22h], *above*.  Munje, Fig. 1.

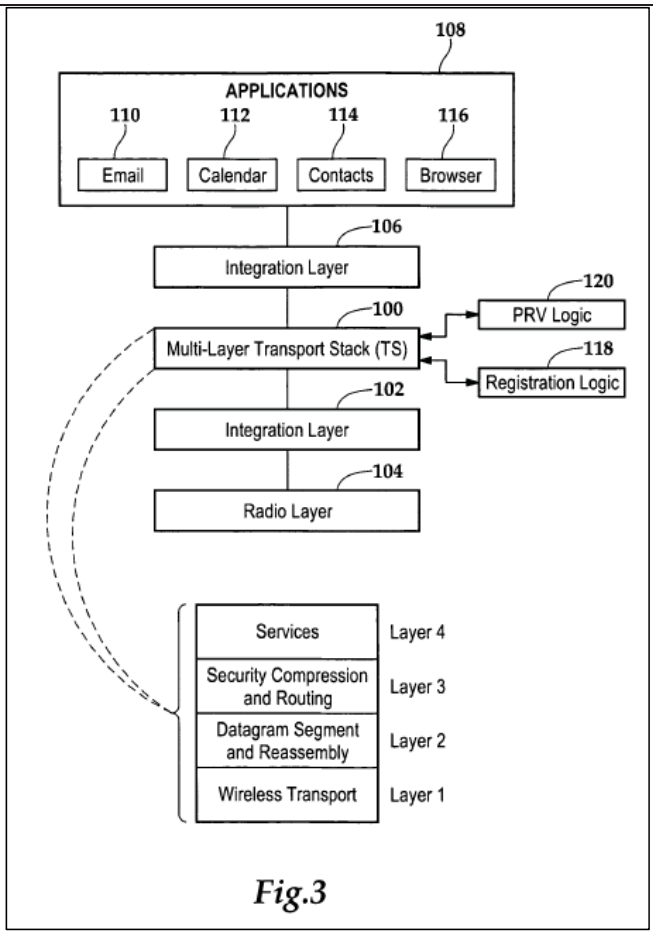
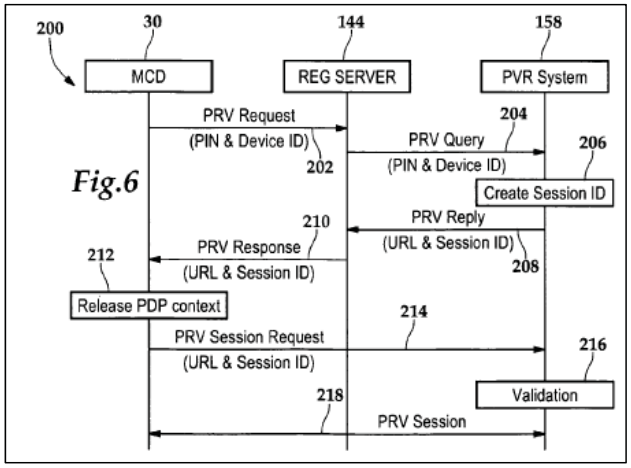
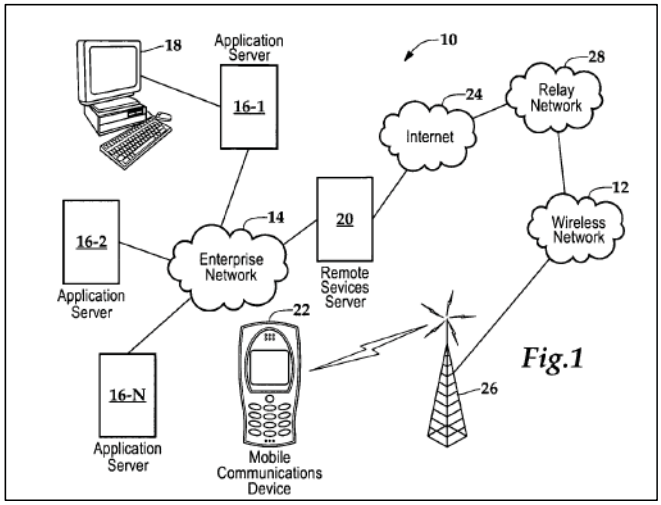

108
APPLICATIONS
110
112
114
116
Email
Calendar
Contacts
Browser
106
Integration Layer
120
PRV Logic
100
Multi-Layer Transport Stack (TS)
118
Registration Logic
102
Integration Layer
104
Radio Layer
Services
Layer 4
Security Compression and Routing
Layer 3
Datagram Segment and Reassembly
Layer 2
Wireless Transport
Layer 1

Fig.3

’619 Patent – Claim 24	Munje
	Munje, Fig. 3.  Munje, Fig. 6. “In certain embodiments of the method, the first network node is operable as part of a relay network. The second node 5 may be operable as part of a provisioning system. In certain embodiments, the first and second data contexts may be PDP contexts. In one embodiment, the first data context may be non web based while the second data context is web based.” Munje at 2:3-8. “FIG. 5 depicts a flowchart of an embodiment for establishing sequential PDP contexts with a MCD that supports a single PDP context such that the MCD can be provisioned over the air via a remote provisioning system. In the present embodiment, the communication sessions may be both web based and non web based communication sessions preferably using Wireless Application Protocol

'619 Patent – Claim 24	Munje
	(WAP) or other suitable communication protocol. Prior to full utilization of the MCD, certain aspect of the device's overall functionality may need to be provisioned such as particular parameters to enable information to be pushed to the MCD." Munje at 6:44-53. "Specifically, as detailed in method 170 of FIG. 5, once the MCD has the appropriate PIN, the transport stack of the MCD establishes a first data context, which is preferably a non web based PDP context with the registration server (block 172). The transport stack accesses the PIN and device identifier information and transmits a request for parameters to the registration server (block 174). In one embodiment, this request for parameter includes the PIN and a device identifier. This information is then communicated from the registration server to the provisioning system which may be colocated, integrate or otherwise communicably associated with the registration server. The provisioning system can then generate the requested parameters which, in the present example, are a URL associated with the provisioning system and a session ID appended thereto which is preferably based upon the PIN and the device identifier such as by using a hashing technique." Munje at 7:19-34. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

'619 Patent – Claim 25	Munje
[25] The device of claim 24, wherein the off-line	Munje discloses this claim limitation. For example, see the following

’619 Patent – Claim 25	Munje
communication involves a local connection.	passages and/or figures, as well as all related disclosures: *See* [22pre]-[22h] and 24 *above*.  Munje, Fig. 1.

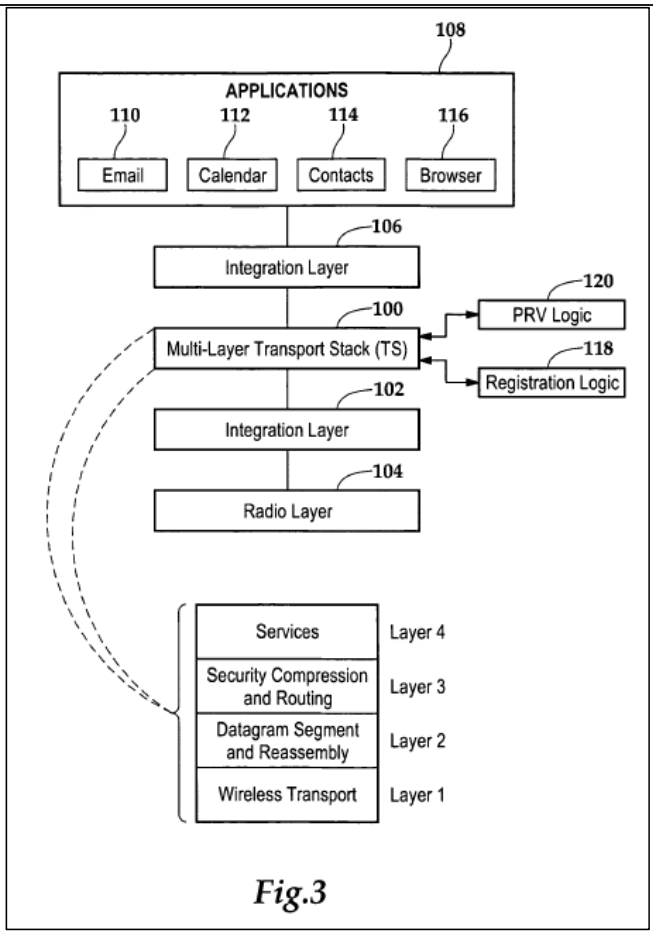
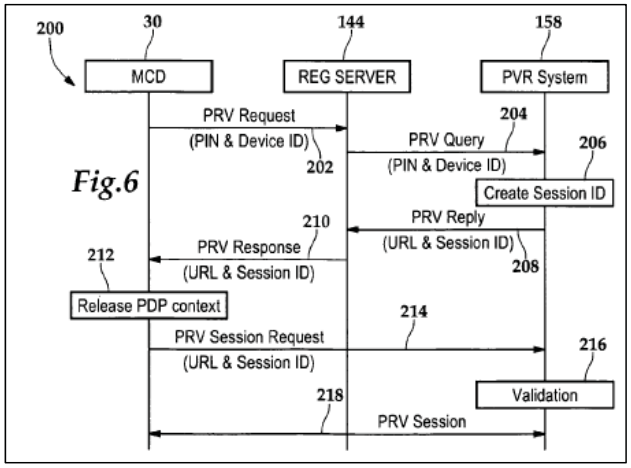
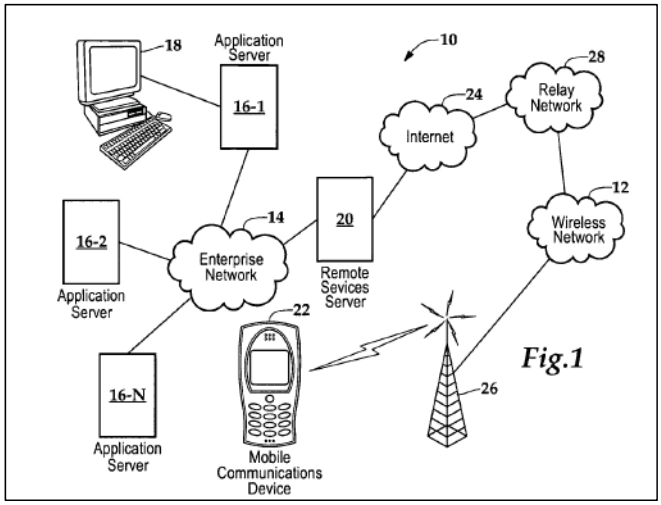

108
APPLICATIONS
110
112
114
116
Email
Calendar
Contacts
Browser
106
Integration Layer
120
PRV Logic
100
Multi-Layer Transport Stack (TS)
118
Registration Logic
102
Integration Layer
104
Radio Layer
Services
Layer 4
Security Compression and Routing
Layer 3
Datagram Segment and Reassembly
Layer 2
Wireless Transport
Layer 1

Fig.3

’619 Patent – Claim 25	Munje
	Munje, Fig. 3.  Munje, Fig. 6. “In certain embodiments of the method, the first network node is operable as part of a relay network. The second node 5 may be operable as part of a provisioning system. In certain embodiments, the first and second data contexts may be PDP contexts. In one embodiment, the first data context may be non web based while the second data context is web based.” Munje at 2:3-8. “FIG. 5 depicts a flowchart of an embodiment for establishing sequential PDP contexts with a MCD that supports a single PDP context such that the MCD can be provisioned over the air via a remote provisioning system. In the present embodiment, the communication sessions may be both web based and non web based communication sessions preferably using Wireless Application Protocol

’619 Patent – Claim 25	Munje
	(WAP) or other suitable communication protocol. Prior to full utilization of the MCD, certain aspect of the device's overall functionality may need to be provisioned such as particular parameters to enable information to be pushed to the MCD.” Munje at 6:44-53. “Specifically, as detailed in method 170 of FIG. 5, once the MCD has the appropriate PIN, the transport stack of the MCD establishes a first data context, which is preferably a non web based PDP context with the registration server (block 172). The transport stack accesses the PIN and device identifier information and transmits a request for parameters to the registration server (block 174). In one embodiment, this request for parameter includes the PIN and a device identifier. This information is then communicated from the registration server to the provisioning system which may be colocated, integrate or otherwise communicably associated with the registration server. The provisioning system can then generate the requested parameters which, in the present example, are a URL associated with the provisioning system and a session ID appended thereto which is preferably based upon the PIN and the device identifier such as by using a hashing technique.” Munje at 7:19-34. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

’619 Patent – Claim 26	Munje
[26] The device of claim 24, wherein the off-line	Munje discloses this claim limitation. For example, see the following

’619 Patent – Claim 26	Munje
communication prevents eavesdropping of the service activation code.	passages and/or figures, as well as all related disclosures: *See* [22pre]-[22h] and [24], *above*.  Munje, Fig. 1.

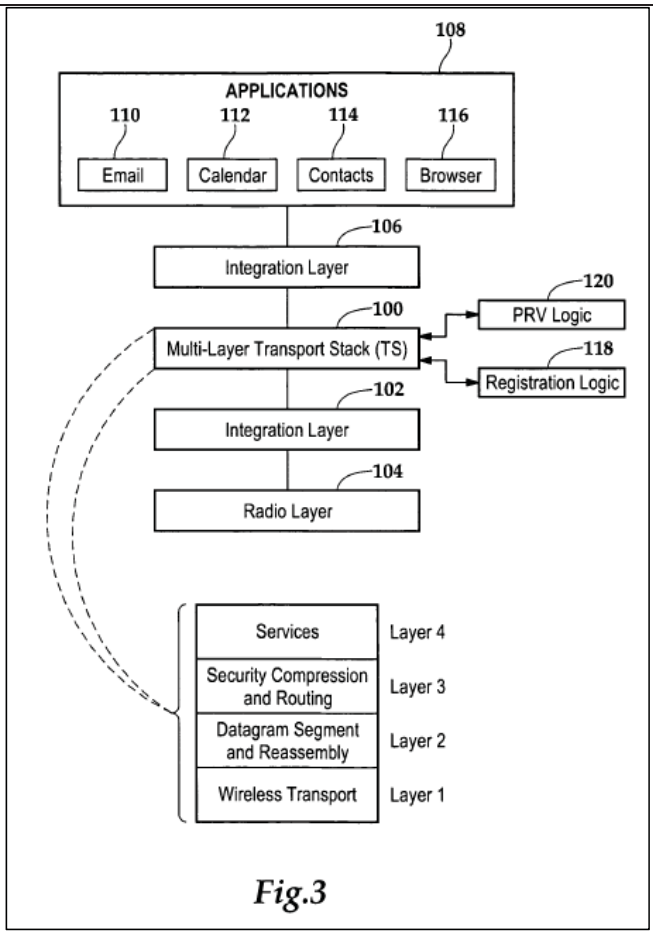
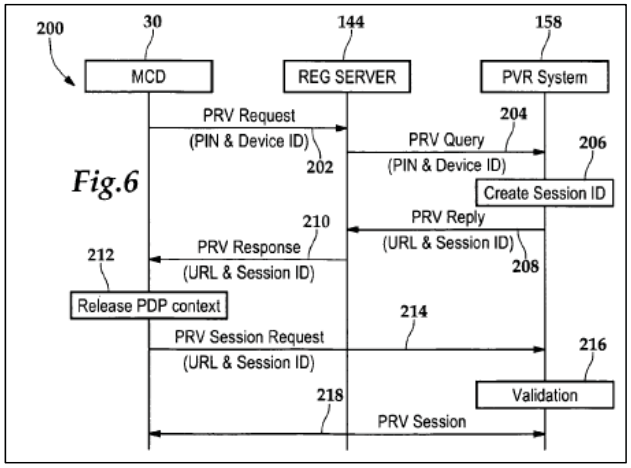
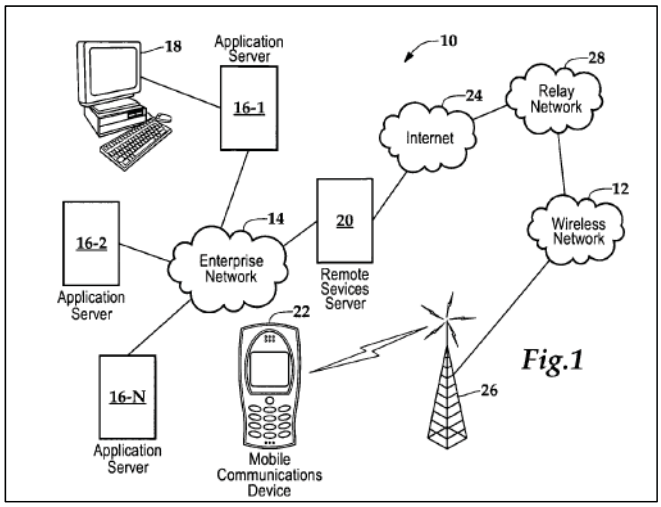

108
APPLICATIONS
110
112
114
116
Email
Calendar
Contacts
Browser
106
Integration Layer
120
PRV Logic
100
Multi-Layer Transport Stack (TS)
118
Registration Logic
102
Integration Layer
104
Radio Layer
Services
Layer 4
Security Compression and Routing
Layer 3
Datagram Segment and Reassembly
Layer 2
Wireless Transport
Layer 1

Fig.3

’619 Patent – Claim 26	Munje
	Munje, Fig. 3.  Munje, Fig. 6. “In certain embodiments of the method, the first network node is operable as part of a relay network. The second node 5 may be operable as part of a provisioning system. In certain embodiments, the first and second data contexts may be PDP contexts. In one embodiment, the first data context may be non web based while the second data context is web based.” Munje at 2:3-8. “FIG. 5 depicts a flowchart of an embodiment for establishing sequential PDP contexts with a MCD that supports a single PDP context such that the MCD can be provisioned over the air via a remote provisioning system. In the present embodiment, the communication sessions may be both web based and non web based communication sessions preferably using Wireless Application Protocol

’619 Patent – Claim 26	Munje
	(WAP) or other suitable communication protocol. Prior to full utilization of the MCD, certain aspect of the device's overall functionality may need to be provisioned such as particular parameters to enable information to be pushed to the MCD.” Munje at 6:44-53 “Specifically, as detailed in method 170 of FIG. 5, once the MCD has the appropriate PIN, the transport stack of the MCD establishes a first data context, which is preferably a non web based PDP context with the registration server (block 172). The transport stack accesses the PIN and device identifier information and transmits a request for parameters to the registration server (block 174). In one embodiment, this request for parameter includes the PIN and a device identifier. This information is then communicated from the registration server to the provisioning system which may be colocated, integrate or otherwise communicably associated with the registration server. The provisioning system can then generate the requested parameters which, in the present example, are a URL associated with the provisioning system and a session ID appended thereto which is preferably based upon the PIN and the device identifier such as by using a hashing technique.” Munje at 7:19-34. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

’619 Patent – Claim 27	Munje
[27] The device of claim 22, wherein the authentication of the device relies on the authentication of the messaging account.	Munje discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22pre]-[22h], *above*.  Munje, Fig. 1.

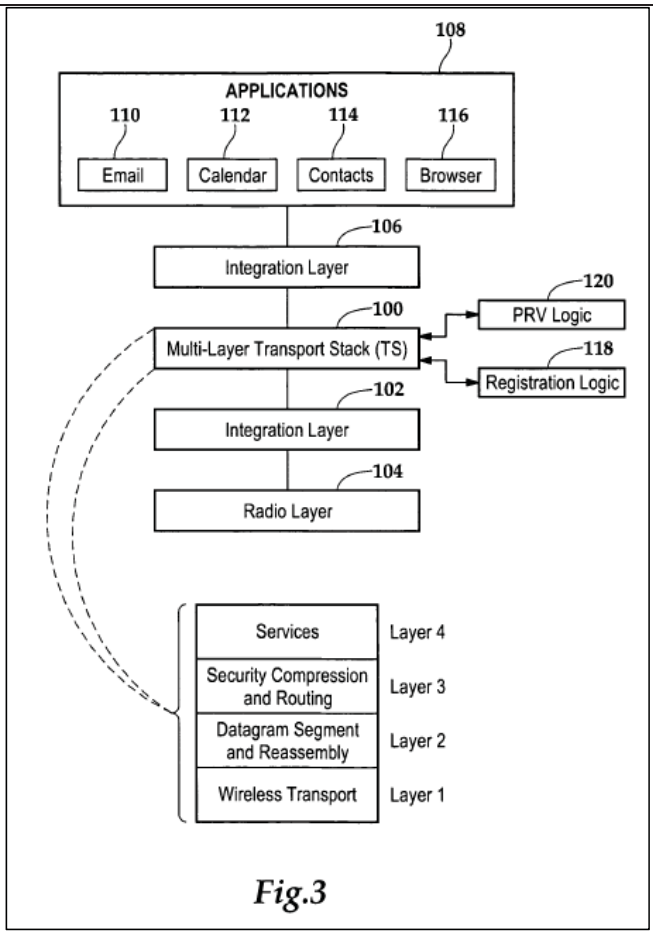
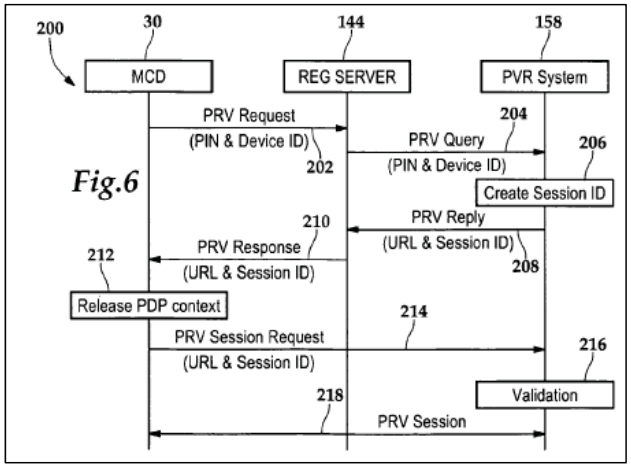

108
APPLICATIONS
110
112
114
116
Email
Calendar
Contacts
Browser
106
Integration Layer
120
PRV Logic
100
Multi-Layer Transport Stack (TS)
118
Registration Logic
102
Integration Layer
104
Radio Layer
Services
Layer 4
Security Compression and Routing
Layer 3
Datagram Segment and Reassembly
Layer 2
Wireless Transport
Layer 1

Fig.3

’619 Patent – Claim 27	Munje
	Munje, Fig. 3.  Munje, Fig. 6. “FIG. 3 depicts a software architectural view of a mobile communications device operable according to one embodiment for provisioning certain aspects of the MCD regardless of the manufacturer of the MCD or the wireless service provider. A multi-layer transport stack (TS) 100 is operable to provide a generic data transport protocol for any type of corporate data, including email, via a reliable, secure and seamless continuous connection to a wireless packet data service network. As illustrated in the embodiment of FIG. 3, an integration layer 102 is operable as an interface between the MCD's radio layer 104 and the transport stack 100. Likewise, another integration layer 106 is provided for interfacing between the transport stack 100 and the user applications 108 supported on the MCD, e.g., email 110, calendar/scheduler 112, contact

’619 Patent – Claim 27	Munje
	management 114 and web browser 116. Although not specifically shown, the transport stack 100 may also be interfaced with the MCD's operating system. In another implementation, the transport stack 100 may be provided as part of a data communications client module operable as a host-independent virtual machine on a mobile device. The bottom layer (Layer 1) of the transport stack 100 is operable as an interface to the wireless network's packet layer. Layer 1 handles basic service coordination within the exemplary network environment 10 shown in FIG. 1. For example, when an MCD roams from one carrier network to another, Layer 1 verifies that the packets are relayed to the appropriate wireless network and that any packets that are pending from the previous network are rerouted to the current network. The top layer (Layer 4) exposes various application interfaces to the services supported on the MCD. The remaining two layers, Layer 2 and Layer 3, are responsible for datagram segmentation/reassembly and security, compression and routing, respectively. FIG. 3 also depicts a registration logic module 118 provided as part of the MCD's software environment that is disposed in operable communication with the transport stack 100 as well as the OS environment for effectuating registration procedures, as and when needed, with the serving relay network. In one implementation, where a PIN is not otherwise provided or associated with the MCD, the registration logic module 118 includes logic means operable to execute a registration procedure with the serving relay node to request and receive a PIN, which will allow identification of the MCD by this network node during future communication sessions therebetween.” Munje at 4:26-5:4. “Additionally, a remote services server 20 may be interfaced with the enterprise network 14 for enabling a corporate user to access or effectuate any of the services from a remote location using a suitable single PDP context mobile communications device (MCD) 22. A secure communication link with end-to-end encryption may be established that is mediated through an external

’619 Patent – Claim 27	Munje
	IP network, i.e., a public packet-switched network such as the Internet 24, as well as the wireless packet data service network 12 operable with MCD 22 via suitable wireless network infrastructure that includes a base station 26. In one embodiment, a trusted relay network 28 may be disposed between the Internet 24 and the infrastructure of wireless packet data service network 12. By way of example, MCD 22 may be a data-enabled handheld device capable of receiving and sending messages, web browsing, interfacing with corporate application servers and the like.” Munje at 3:1-17. “FIG. 3 also depicts a registration logic module 118 provided as part of the MCD's software environment that is disposed in operable communication with the transport stack 100 as well as the OS environment for effectuating registration procedures, as and when needed, with the serving relay network. In one implementation, where a PIN is not otherwise provided or associated with the MCD, the registration logic module 118 includes logic means operable to execute a registration procedure with the serving relay node to request and receive a PIN, which will allow identification of the MCD by this network node during future communication sessions therebetween. A PRV logic module 120 provided as part of the MCD's software environment is disposed in operable communication with the transport stack 100 as well as the OS environment. In one embodiment, the PRV logic module 120 comprises logic operable to generate a request including the PIN and at least one hardware device identifier associated with the MCD for transmission in a message to a network node such as the above mentioned serving relay node with an associated registration server, provisioning server and the like. As stated above, the PIN may be a required parameter in communications between an MCD and the serving relay node for identification and verification purposes.” Munje at 4:60-5:16. “Additionally, a database 142 may be provided in operable connection with the relay node 132 for handling and managing MCD location information.

’619 Patent – Claim 27	Munje
	Preferably, this location information is stored by PIN of the MCDs, wherein the records maintain a particular device's last known location. A registration server 144 is operable for providing registration services for MCDs when they are initially activated or when the user re-registers due to moving to a different wireless network coverage area. In one implementation, the location information of registration server 144 may be programmed into an MCD. When the MCD registers successfully, registration server 144 is operable to provide the serving relay node's location, whereupon data sessions may be engaged by the MCD.” Munje at 5:65-6:11. “FIG. 5 depicts a flowchart of an embodiment for establishing sequential PDP contexts with a MCD that supports a single PDP context such that the MCD can be provisioned over the air via a remote provisioning system. In the present embodiment, the communication sessions may be both web based and non web based communication sessions preferably using Wireless Application Protocol (WAP) or other suitable communication protocol. Prior to full utilization of the MCD, certain aspect of the device's overall functionality may need to be provisioned such as particular parameters to enable information to be pushed to the MCD. The provisioning of these aspects of the MCD may require authentication of the device, via a PIN, a device identifier or both, prior to provisioning. When the MCD is manufactured, one or more device identifiers such as IMEI, IMSI, ESN, MIN or the like are typically associated with the device. A PIN for these desires services, on the other hand, may not be assigned to the device upon manufacturing requiring the user to acquire such a PIN directly from the service provider via an over the air request and response sequence, which may take place with little or no user intervention. Additionally, once the MCD is deployed, it may be provided with an IP address since it is an IP appliance operable with a wireless packet data service network. Once the device has acquired the PIN relating to the aspects of the device the user desires to provision, it is now desirable to make the provisioning process as seamless as possible such as through the use of a web browser.

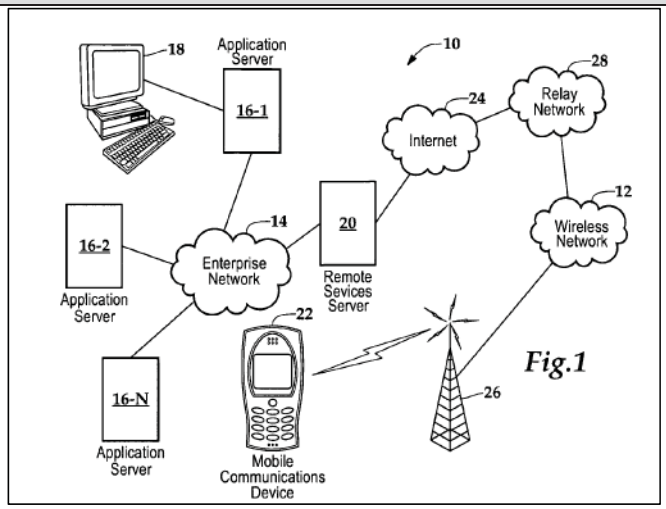
’619 Patent – Claim 27	Munje
	It has been found, however, that many web browsers used in MCDs are not capable of retrieving and using PIN and device identifier information. In addition, it has been found that many MCDs are capable of only a single PDP context. The present disclosure, however, provides for sequential PDP contexts on the MCD and for communicating the PIN information to the web browser to allow the web browser to establish a communication session with the appropriate provisioning system. As such, those of ordinary skill in the art should recognized that the present disclosure is not only applicable to single PDP context MCDs but also to any MCD/network system wherein the two required PDP contexts cannot simultaneously be active including, but not limited to, a MCD currently conducting its maximum number of PDP contexts, a network capable of supporting only one PDP context with a given MCD or the like. Specifically, as detailed in method 170 of FIG. 5, once the MCD has the appropriate PIN, the transport stack of the MCD establishes a first data context, which is preferably a non web based PDP context with the registration server (block 172). The transport stack accesses the PIN and device identifier information and transmits a request for parameters to the registration server (block 174). In one embodiment, this request for parameter includes the PIN and a device identifier. This information is then communicated from the registration server to the provisioning system which may be colocated, integrate or otherwise communicably associated with the registration server. The provisioning system can then generate the requested parameters which, in the present example, are a URL associated with the provisioning system and a session ID appended thereto which is preferably based upon the PIN and the device identifier such as by using a hashing technique. Preferably, the provisioning system starts a clock to establish a time frame within which the session ID will be valid. The provisioning system than communicates the requested parameters to the registration server which is still in communication with the MCD via the first data context. The registration server then provides a response including the requested parameters (the URL with session ID

’619 Patent – Claim 27	Munje
	parameters) to the MCD which receives this information via the transport stack (block 176). Once the MCD has obtained the requested parameters, the first data context between the MCD and the registration server is automatically released (block 178). The requested parameters are then passed to the web browser which automatically launches the web page associated with the URL, which includes the session ID such that the device information of the MCD is known to the provisioning system. This establishes a second data context, which is preferably a web based PDP context with the provisioning system (block 180). In this communication session, the aspects of the MCD that are associated with this service provider can now be provisioned over the air using well known data entry techniques via the web browser (block 182). As such, the MCD can be seamlessly provisioned by establishing one data context with a registration server to transmit a request for parameters and receive a response including the parameters then automatically releasing that data context and establishing a second data context by transmitting the parameters to a provisioning system.” Munje at 6:44-7:61. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

’619 Patent – Claim 28	Munje
[28] The device of claim 27, wherein the authentication of the messaging account includes	Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in

’619 Patent – Claim 28	Munje
a username and password.	Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

’619 Patent – Claim 32	Munje
[32] The device of claim 22, wherein the encryption key is closely related to the service activation code.	Munje discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22pre]-[22h], *above*.

’619 Patent – Claim 32	Munje
	 Munje, Fig. 1.

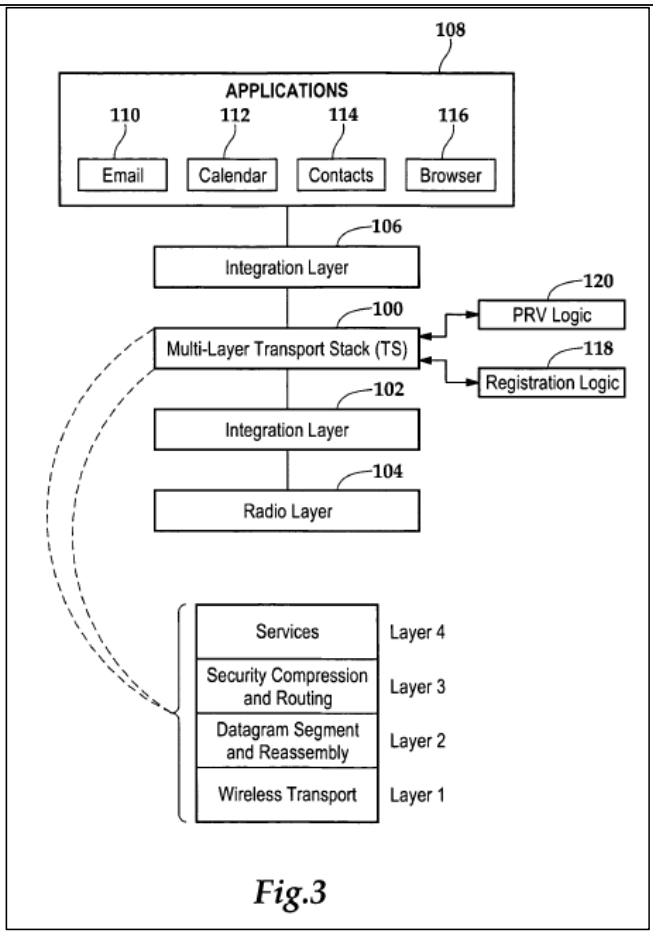
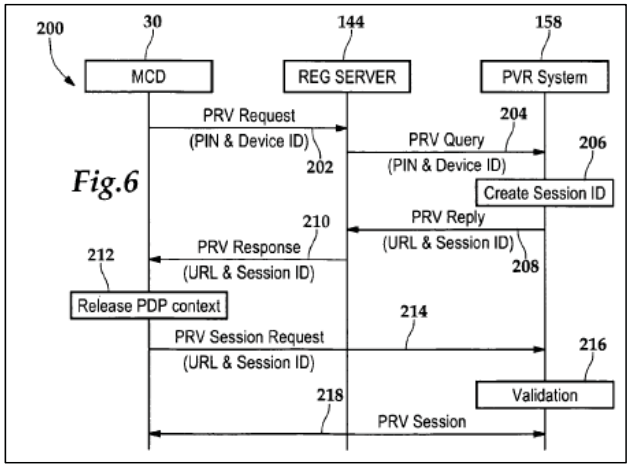

108
APPLICATIONS
110
112
114
116
Email
Calendar
Contacts
Browser
106
Integration Layer
120
PRV Logic
100
Multi-Layer Transport Stack (TS)
118
Registration Logic
102
Integration Layer
104
Radio Layer
Services
Layer 4
Security Compression and Routing
Layer 3
Datagram Segment and Reassembly
Layer 2
Wireless Transport
Layer 1

Fig.3

’619 Patent – Claim 32	Munje
	Munje, Fig. 3.  Fig.6 Munje, Fig. 6. “Additionally, a remote services server 20 may be interfaced with the enterprise network 14 for enabling a corporate user to access or effectuate any of the services from a remote location using a suitable single PDP context mobile communications device (MCD) 22. A secure communication link with end-to-end encryption may be established that is mediated through an external IP network, i.e., a public packet-switched network such as the Internet 24, as well as the wireless packet data service network 12 operable with MCD 22 via suitable wireless network infrastructure that includes a base station 26. In one embodiment, a trusted relay network 28 may be disposed between the Internet 24 and the infrastructure of wireless packet data service network 12. By way of example, MCD 22 may be a data-enabled handheld device capable of receiving

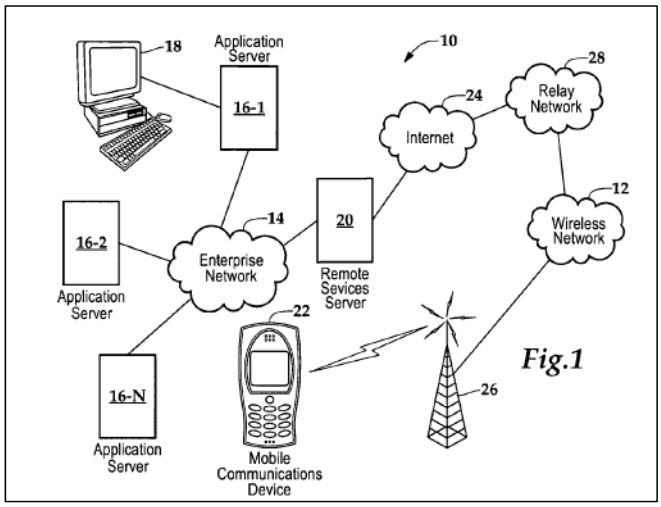
’619 Patent – Claim 32	Munje
	and sending messages, web browsing, interfacing with corporate application servers and the like.” Munje at 3:1-17. “FIG. 3 also depicts a registration logic module 118 provided as part of the MCD's software environment that is disposed in operable communication with the transport stack 100 as well as the OS environment for effectuating registration procedures, as and when needed, with the serving relay network. In one implementation, where a PIN is not otherwise provided or associated with the MCD, the registration logic module 118 includes logic means operable to execute a registration procedure with the serving relay node to request and receive a PIN, which will allow identification of the MCD by this network node during future communication sessions therebetween. A PRV logic module 120 provided as part of the MCD's software environment is disposed in operable communication with the transport stack 100 as well as the OS environment. In one embodiment, the PRV logic module 120 comprises logic operable to generate a request including the PIN and at least one hardware device identifier associated with the MCD for transmission in a message to a network node such as the above mentioned serving relay node with an associated registration server, provisioning server and the like. As stated above, the PIN may be a required parameter in communications between an MCD and the serving relay node for identification and verification purposes.” Munje at 4:60-5:16. “Additionally, a database 142 may be provided in operable connection with the relay node 132 for handling and managing MCD location information. Preferably, this location information is stored by PIN of the MCDs, wherein the records maintain a particular device's last known location. A registration server 144 is operable for providing registration services for MCDs when they are initially activated or when the user re-registers due to moving to a different wireless network coverage area. In one implementation, the location information of registration server 144 may be programmed into an MCD.

’619 Patent – Claim 32	Munje
	When the MCD registers successfully, registration server 144 is operable to provide the serving relay node's location, whereupon data sessions may be engaged by the MCD.” Munje at 5:65-6:11. “FIG. 5 depicts a flowchart of an embodiment for establishing sequential PDP contexts with a MCD that supports a single PDP context such that the MCD can be provisioned over the air via a remote provisioning system. In the present embodiment, the communication sessions may be both web based and non web based communication sessions preferably using Wireless Application Protocol (WAP) or other suitable communication protocol. Prior to full utilization of the MCD, certain aspect of the device's overall functionality may need to be provisioned such as particular parameters to enable information to be pushed to the MCD. The provisioning of these aspects of the MCD may require authentication of the device, via a PIN, a device identifier or both, prior to provisioning. When the MCD is manufactured, one or more device identifiers such as IMEI, IMSI, ESN, MIN or the like are typically associated with the device. A PIN for these desires services, on the other hand, may not be assigned to the device upon manufacturing requiring the user to acquire such a PIN directly from the service provider via an over the air request and response sequence, which may take place with little or no user intervention. Additionally, once the MCD is deployed, it may be provided with an IP address since it is an IP appliance operable with a wireless packet data service network. Once the device has acquired the PIN relating to the aspects of the device the user desires to provision, it is now desirable to make the provisioning process as seamless as possible such as through the use of a web browser. It has been found, however, that many web browsers used in MCDs are not capable of retrieving and using PIN and device identifier information. In addition, it has been found that many MCDs are capable of only a single PDP context. The present disclosure, however, provides for sequential PDP contexts on the MCD and for communicating the PIN information to the web browser to allow the web browser to establish a communication session with the

’619 Patent – Claim 32	Munje
	appropriate provisioning system. As such, those of ordinary skill in the art should recognized that the present disclosure is not only applicable to single PDP context MCDs but also to any MCD/network system wherein the two required PDP contexts cannot simultaneously be active including, but not limited to, a MCD currently conducting its maximum number of PDP contexts, a network capable of supporting only one PDP context with a given MCD or the like. Specifically, as detailed in method 170 of FIG. 5, once the MCD has the appropriate PIN, the transport stack of the MCD establishes a first data context, which is preferably a non web based PDP context with the registration server (block 172). The transport stack accesses the PIN and device identifier information and transmits a request for parameters to the registration server (block 174). In one embodiment, this request for parameter includes the PIN and a device identifier. This information is then communicated from the registration server to the provisioning system which may be colocated, integrate or otherwise communicably associated with the registration server. The provisioning system can then generate the requested parameters which, in the present example, are a URL associated with the provisioning system and a session ID appended thereto which is preferably based upon the PIN and the device identifier such as by using a hashing technique. Preferably, the provisioning system starts a clock to establish a time frame within which the session ID will be valid. The provisioning system than communicates the requested parameters to the registration server which is still in communication with the MCD via the first data context. The registration server then provides a response including the requested parameters (the URL with session ID parameters) to the MCD which receives this information via the transport stack (block 176). Once the MCD has obtained the requested parameters, the first data context between the MCD and the registration server is automatically released (block 178). The requested parameters are then passed to the web browser which automatically launches the web page associated with the URL, which includes the session ID such that the device information of the MCD is

’619 Patent – Claim 32	Munje
	known to the provisioning system. This establishes a second data context, which is preferably a web based PDP context with the provisioning system (block 180). In this communication session, the aspects of the MCD that are associated with this service provider can now be provisioned over the air using well known data entry techniques via the web browser (block 182). As such, the MCD can be seamlessly provisioned by establishing one data context with a registration server to transmit a request for parameters and receive a response including the parameters then automatically releasing that data context and establishing a second data context by transmitting the parameters to a provisioning system.” Munje at 6:44-7:61. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

’619 Patent – Claim 33	Munje
[33a] The device of claim 22, wherein the device is further operable to:	Munje discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22pre]-[22h], *above*. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person

’619 Patent – Claim 33	Munje
	of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[33b] store an association between at least two of the encryption key, the messaging account, an identifier of the remote device, and the service activation code.	Munje discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22pre]-[22h], *above*.  Munje, Fig. 1.

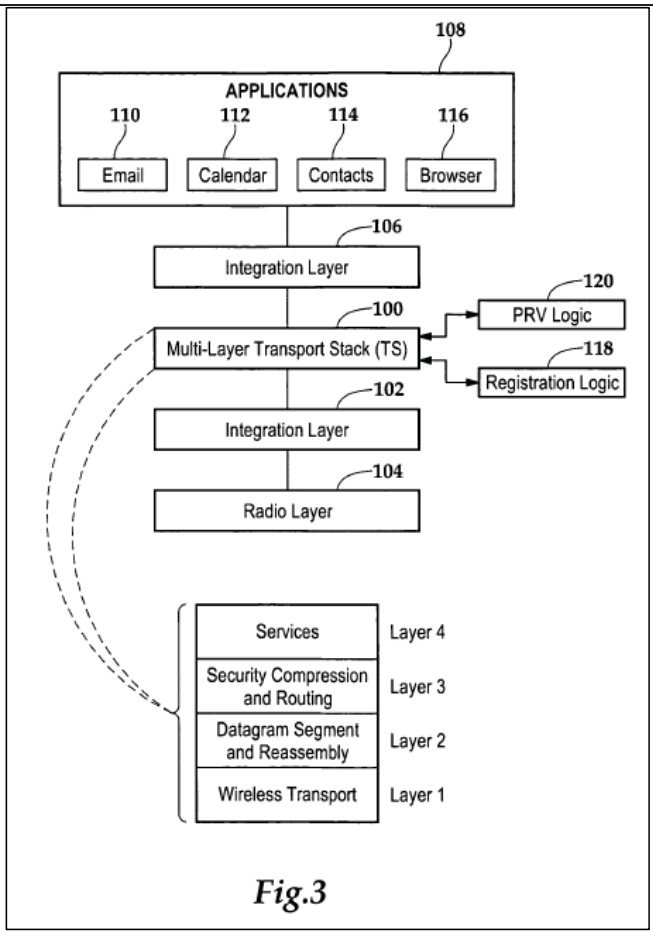
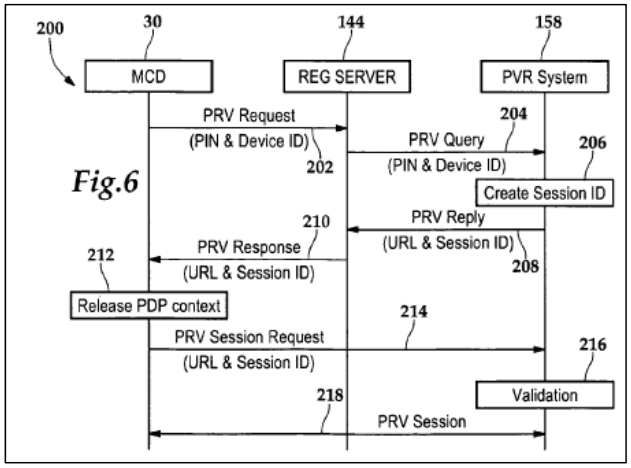

108
APPLICATIONS
110
112
114
116
Email
Calendar
Contacts
Browser
106
Integration Layer
120
PRV Logic
100
Multi-Layer Transport Stack (TS)
118
Registration Logic
102
Integration Layer
104
Radio Layer
Services
Layer 4
Security Compression and Routing
Layer 3
Datagram Segment and Reassembly
Layer 2
Wireless Transport
Layer 1

Fig.3

’619 Patent – Claim 33	Munje
	Munje, Fig. 3.  Munje, Fig. 6. “Additionally, a remote services server 20 may be interfaced with the enterprise network 14 for enabling a corporate user to access or effectuate any of the services from a remote location using a suitable single PDP context mobile communications device (MCD) 22. A secure communication link with end-to-end encryption may be established that is mediated through an external IP network, i.e., a public packet-switched network such as the Internet 24, as well as the wireless packet data service network 12 operable with MCD 22 via suitable wireless network infrastructure that includes a base station 26. In one embodiment, a trusted relay network 28 may be disposed between the Internet 24 and the infrastructure of wireless packet data service network 12. By way of example, MCD 22 may be a data-enabled handheld device capable of receiving

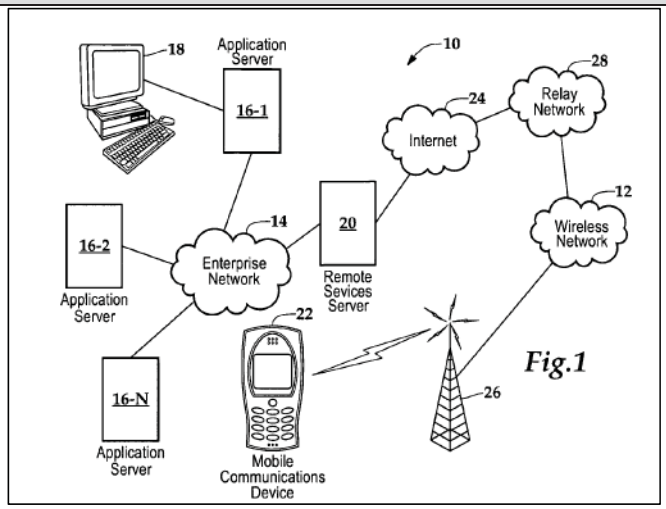
’619 Patent – Claim 33	Munje
	and sending messages, web browsing, interfacing with corporate application servers and the like.” Munje at 3:1-17. “FIG. 3 also depicts a registration logic module 118 provided as part of the MCD's software environment that is disposed in operable communication with the transport stack 100 as well as the OS environment for effectuating registration procedures, as and when needed, with the serving relay network. In one implementation, where a PIN is not otherwise provided or associated with the MCD, the registration logic module 118 includes logic means operable to execute a registration procedure with the serving relay node to request and receive a PIN, which will allow identification of the MCD by this network node during future communication sessions therebetween. A PRV logic module 120 provided as part of the MCD's software environment is disposed in operable communication with the transport stack 100 as well as the OS environment. In one embodiment, the PRV logic module 120 comprises logic operable to generate a request including the PIN and at least one hardware device identifier associated with the MCD for transmission in a message to a network node such as the above mentioned serving relay node with an associated registration server, provisioning server and the like. As stated above, the PIN may be a required parameter in communications between an MCD and the serving relay node for identification and verification purposes.” Munje at 4:60-5:16. “Additionally, a database 142 may be provided in operable connection with the relay node 132 for handling and managing MCD location information. Preferably, this location information is stored by PIN of the MCDs, wherein the records maintain a particular device's last known location. A registration server 144 is operable for providing registration services for MCDs when they are initially activated or when the user re-registers due to moving to a different wireless network coverage area. In one implementation, the location information of registration server 144 may be programmed into an MCD.

’619 Patent – Claim 33	Munje
	When the MCD registers successfully, registration server 144 is operable to provide the serving relay node's location, whereupon data sessions may be engaged by the MCD.” Munje at 5:65-6:11. “FIG. 5 depicts a flowchart of an embodiment for establishing sequential PDP contexts with a MCD that supports a single PDP context such that the MCD can be provisioned over the air via a remote provisioning system. In the present embodiment, the communication sessions may be both web based and non web based communication sessions preferably using Wireless Application Protocol (WAP) or other suitable communication protocol. Prior to full utilization of the MCD, certain aspect of the device's overall functionality may need to be provisioned such as particular parameters to enable information to be pushed to the MCD. The provisioning of these aspects of the MCD may require authentication of the device, via a PIN, a device identifier or both, prior to provisioning. When the MCD is manufactured, one or more device identifiers such as IMEI, IMSI, ESN, MIN or the like are typically associated with the device. A PIN for these desires services, on the other hand, may not be assigned to the device upon manufacturing requiring the user to acquire such a PIN directly from the service provider via an over the air request and response sequence, which may take place with little or no user intervention. Additionally, once the MCD is deployed, it may be provided with an IP address since it is an IP appliance operable with a wireless packet data service network. Once the device has acquired the PIN relating to the aspects of the device the user desires to provision, it is now desirable to make the provisioning process as seamless as possible such as through the use of a web browser. It has been found, however, that many web browsers used in MCDs are not capable of retrieving and using PIN and device identifier information. In addition, it has been found that many MCDs are capable of only a single PDP context. The present disclosure, however, provides for sequential PDP contexts on the MCD and for communicating the PIN information to the web browser to allow the web browser to establish a communication session with the

’619 Patent – Claim 33	Munje
	appropriate provisioning system. As such, those of ordinary skill in the art should recognized that the present disclosure is not only applicable to single PDP context MCDs but also to any MCD/network system wherein the two required PDP contexts cannot simultaneously be active including, but not limited to, a MCD currently conducting its maximum number of PDP contexts, a network capable of supporting only one PDP context with a given MCD or the like. Specifically, as detailed in method 170 of FIG. 5, once the MCD has the appropriate PIN, the transport stack of the MCD establishes a first data context, which is preferably a non web based PDP context with the registration server (block 172). The transport stack accesses the PIN and device identifier information and transmits a request for parameters to the registration server (block 174). In one embodiment, this request for parameter includes the PIN and a device identifier. This information is then communicated from the registration server to the provisioning system which may be colocated, integrate or otherwise communicably associated with the registration server. The provisioning system can then generate the requested parameters which, in the present example, are a URL associated with the provisioning system and a session ID appended thereto which is preferably based upon the PIN and the device identifier such as by using a hashing technique. Preferably, the provisioning system starts a clock to establish a time frame within which the session ID will be valid. The provisioning system than communicates the requested parameters to the registration server which is still in communication with the MCD via the first data context. The registration server then provides a response including the requested parameters (the URL with session ID parameters) to the MCD which receives this information via the transport stack (block 176). Once the MCD has obtained the requested parameters, the first data context between the MCD and the registration server is automatically released (block 178). The requested parameters are then passed to the web browser which automatically launches the web page associated with the URL, which includes the session ID such that the device information of the MCD is

'619 Patent – Claim 33	Munje
	known to the provisioning system. This establishes a second data context, which is preferably a web based PDP context with the provisioning system (block 180). In this communication session, the aspects of the MCD that are associated with this service provider can now be provisioned over the air using well known data entry techniques via the web browser (block 182). As such, the MCD can be seamlessly provisioned by establishing one data context with a registration server to transmit a request for parameters and receive a response including the parameters then automatically releasing that data context and establishing a second data context by transmitting the parameters to a provisioning system." Munje at 6:44-7:61. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

'619 Patent – Claim 36	Munje
[36] The device of claim 22, wherein a control message is received from the remote device upon user interaction with the message.	Munje discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:

’619 Patent – Claim 36	Munje
	 Munje, Fig. 1.

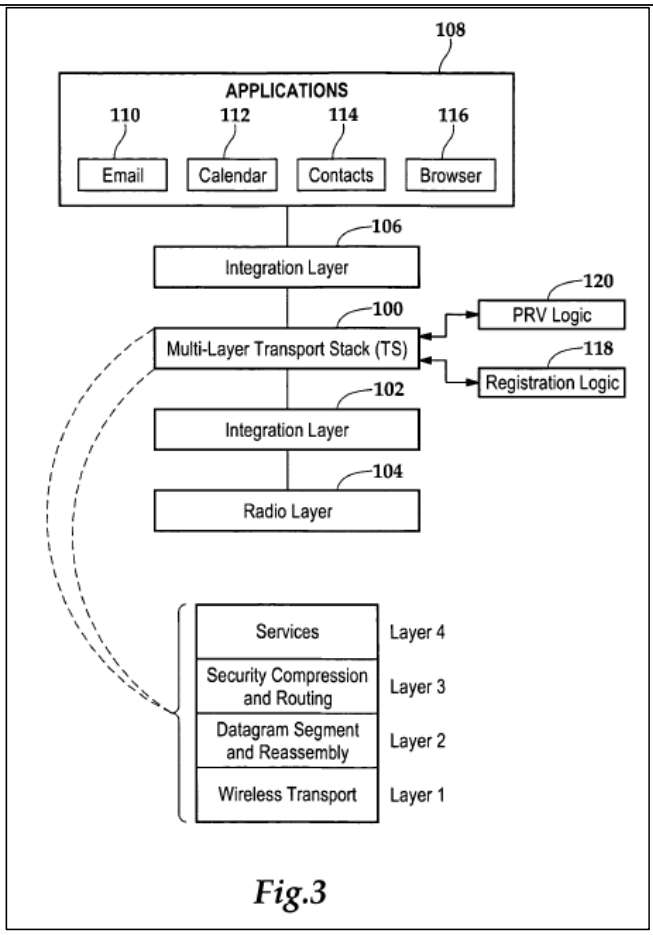
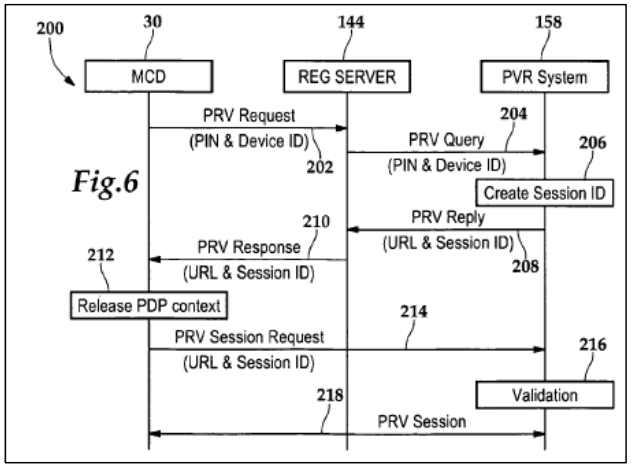
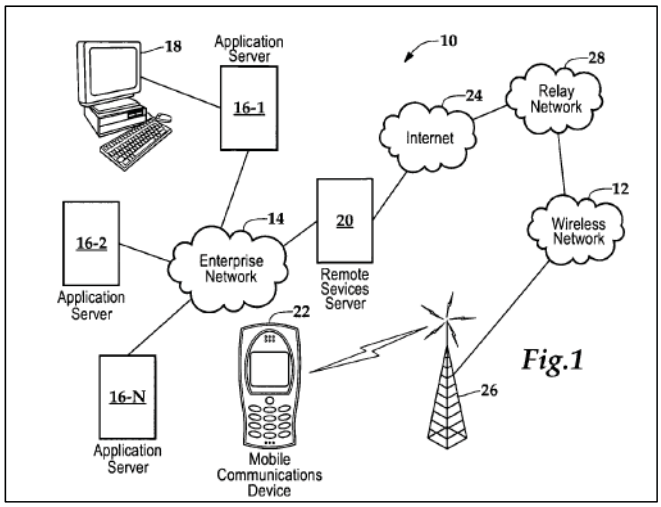

108
APPLICATIONS
110
112
114
116
Email
Calendar
Contacts
Browser
106
Integration Layer
120
PRV Logic
100
Multi-Layer Transport Stack (TS)
118
Registration Logic
102
Integration Layer
104
Radio Layer
Services
Layer 4
Security Compression and Routing
Layer 3
Datagram Segment and Reassembly
Layer 2
Wireless Transport
Layer 1

Fig.3

’619 Patent – Claim 36	Munje
	Munje, Fig. 3.  Munje, Fig. 6. “FIG. 6 depicts a message flow diagram with respect to establishing sequential PDP contexts with a MCD that supports a single PDP context such that the MCD can be provisioned over the air via a remote provisioning system that is generally designated 200. MCD 30 establishes a PDP context wherein a PRV request message 202 is transmitted by MCD 30 to a network node, e.g., registration server 144, wherein the request message 202 includes a PIN as well as a device identifier as parametric information. Registration server 144 queries suitable service logic, which may be embodied as the provisioning system 158 associated with the relay services network described above, by issuing a PRV query 204 thereto, which includes the parametric information received in the PRV request 202. The provisioning system's PRV logic is operable to validate

’619 Patent – Claim 36	Munje
	the request and provide, via a PRV reply 208 to the registration server 144, a message including a URL having session ID parameters appended thereto. Within the first PDP context, this information is then transmitted to MCD 30 via PRV response message 210 from registration server 144. Thereafter, MCD 30 automatically releases the first PDP context 212 and establishes a second PDP context with the PVR system 158. This communication session is established by MCD 30 sending a PRV session request 214 including the URL having session ID parameters. In response thereto, the PVR system 158 is operable to validate 216 the request to, among other things, assure that the session ID has not expire. Upon successful validation, a provisioning session 218 between MCD 30 and PVR system 158 may occur to provision the associated aspects of MCD 30.” Munje at 7:62-8:23. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

’619 Patent – Claim 37	Munje
[37pre] 37. A method for sharing a messaging account, the method comprising:	To the extent the preamble is limiting, Munje discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:  Munje, Fig. 1.

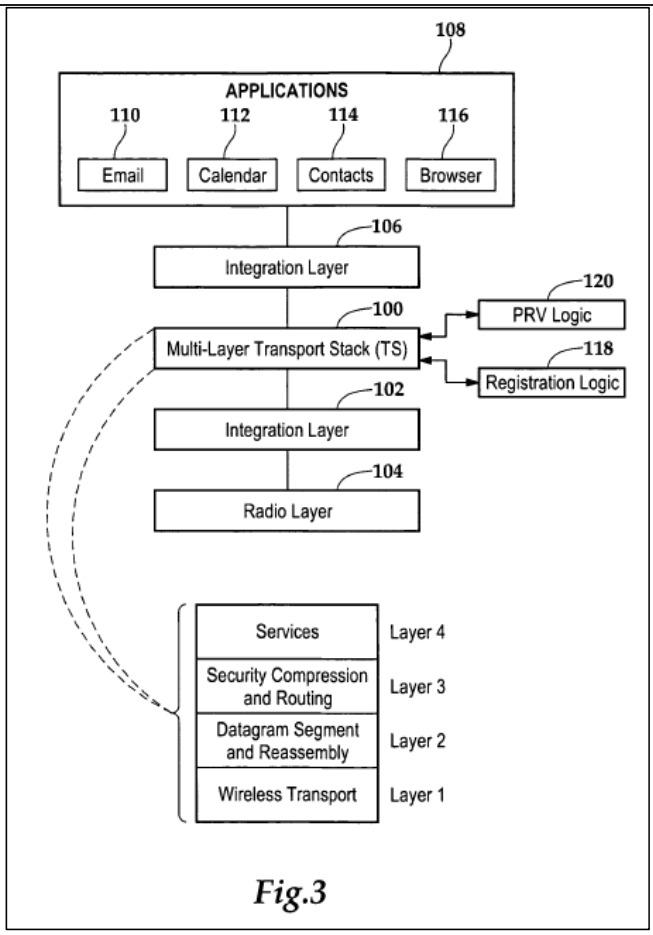
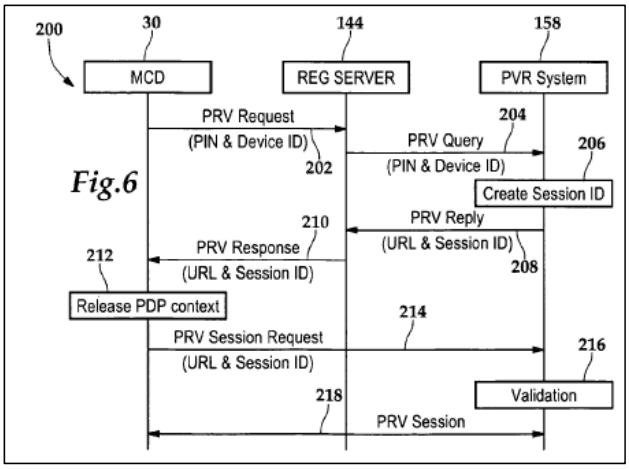

108
APPLICATIONS
110
112
114
116
Email
Calendar
Contacts
Browser
106
Integration Layer
120
PRV Logic
100
Multi-Layer Transport Stack (TS)
118
Registration Logic
102
Integration Layer
104
Radio Layer
Services
Layer 4
Security Compression and Routing
Layer 3
Datagram Segment and Reassembly
Layer 2
Wireless Transport
Layer 1

Fig.3

’619 Patent – Claim 37	Munje
	Munje, Fig. 3.  Munje, Fig. 6. “Referring now to the drawings, and more particularly to FIG. 1, depicted therein is an exemplary network environment 10 including a wireless packet data service network 12 wherein an embodiment of the present method may be practiced. An enterprise network 14 for serving a plurality of corporate users, which may be a packet-switched network, can include one or more geographic sites and be organized as a local area network (LAN), a wide area network (WAN), a metropolitan area network (MAN) or the like. A number of application servers 16-1 through 16-N disposed as part of the enterprise network 14 are operable to provide or effectuate a host of internal and external services such as email, video mail, Internet access, corporate data access, messaging, calendaring and scheduling, information management and the like.

’619 Patent – Claim 37	Munje
	Accordingly, a diverse array of personal information appliances 18 such as desktop computers, laptop computers, palmtop computers or the like may be operably networked to one or more of the application servers 16-i, i=1, 2, . . . , N, with respect to the services supported in the enterprise network 14.” Munje at 2:49-67. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[37a] authenticating a device for access to the messaging account;	Munje discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22h], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[37b] optically receiving information including a displayed service activation code from a remote device;	Munje discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:

’619 Patent – Claim 37	Munje
	See [22c], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[37c] registering the remote device for access to the messaging account using the service activation code;	Munje discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22d], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[37d] receiving a message for the messaging account;	Munje discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22e], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill

’619 Patent – Claim 37	Munje
	in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[37e] encrypting the message using an encryption key; and	Munje discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22f], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[37f] sending the message to the remote device.	Munje discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22g], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and

'619 Patent – Claim 37	Munje
	Exhibit 619-B.

'619 Patent – Claim 38	Munje
[38] The method of claim 37, wherein the information including the service activation code is received by the device in response to user input at the remote device.	Munje discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [23], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

'619 Patent – Claim 39	Munje
[39] The method of claim 38, wherein the information including the service activation code is received by the device in an off-line communication.	Munje discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [24], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person

'619 Patent – Claim 39	Munje
	of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

'619 Patent – Claim 40	Munje
[40] The method of claim 39, wherein the off-line communication prevents eavesdropping of the service activation code.	Munje discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [26], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

'619 Patent – Claim 41	Munje
[41] The method of claim 37, wherein the authentication of the device relies on the authentication of the messaging system.	Munje discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [27], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill

’619 Patent – Claim 41	Munje
	in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

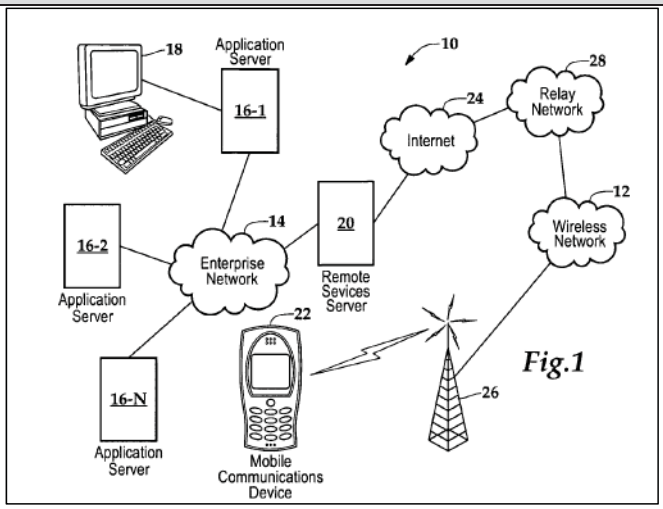
’619 Patent – Claim 42	Munje
[42] The method of claim 41, wherein the authentication of the messaging system includes a username and password.	Munje discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [28], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

’619 Patent – Claim 46	Munje
[46] The method of claim 37, wherein the encryption key is closely related to the service activation code.	Munje discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [32], above.

’619 Patent – Claim 46	Munje
	Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

’619 Patent – Claim 50	Munje
[50] The method of claim 37, wherein a control message is received from the remote device upon user interaction with the message.	Munje discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [36], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

’619 Patent – Claim 51	Munje
[51pre] 51. A non-transient computer-readable medium containing program instructions for	To the extent the preamble is limiting, Munje discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:

’619 Patent – Claim 51	Munje
causing a device to perform a method, the method comprising:	 Munje, Fig. 1.

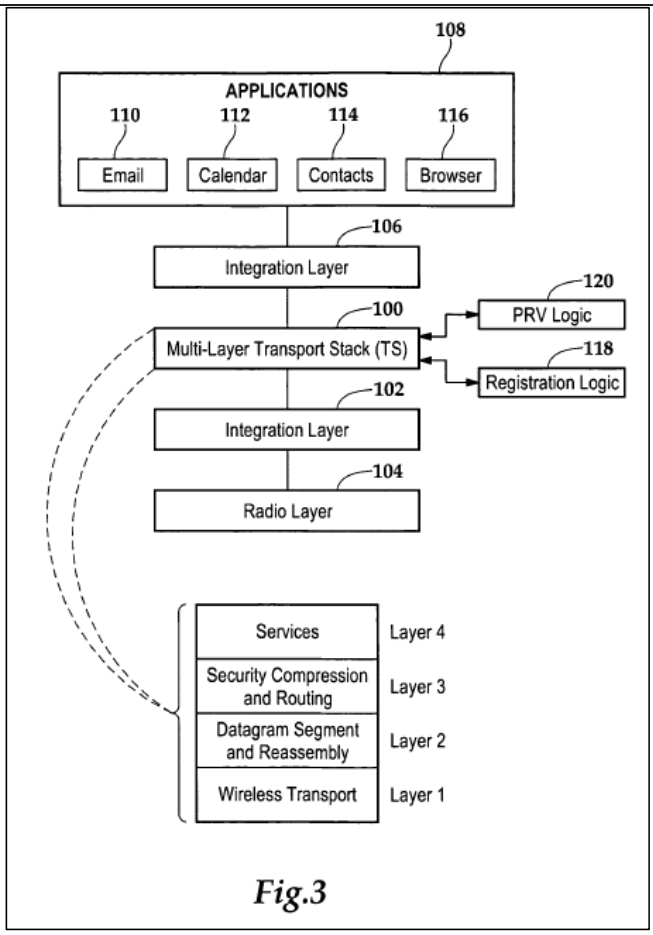
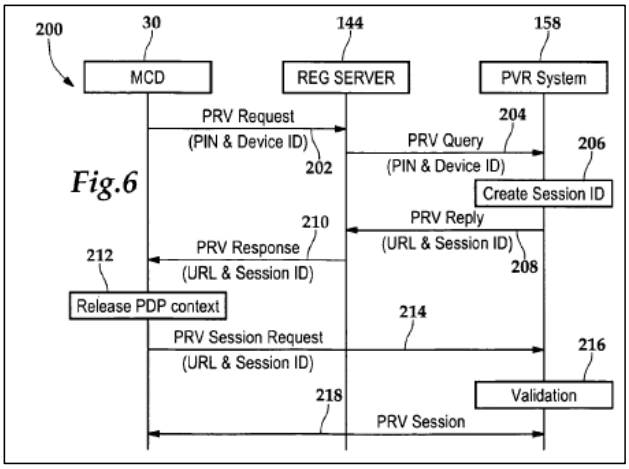


Fig.3

106

EXHIBIT 619-A05

’619 Patent – Claim 51	Munje
	Munje, Fig. 3.  Munje, Fig. 6. “Referring now to the drawings, and more particularly to FIG. 1, depicted therein is an exemplary network environment 10 including a wireless packet data service network 12 wherein an embodiment of the present method may be practiced. An enterprise network 14 for serving a plurality of corporate users, which may be a packet-switched network, can include one or more geographic sites and be organized as a local area network (LAN), a wide area network (WAN), a metropolitan area network (MAN) or the like. A number of application servers 16-1 through 16-N disposed as part of the enterprise network 14 are operable to provide or effectuate a host of internal and external services such as email, video mail, Internet access, corporate data access, messaging, calendaring and scheduling, information management and the like.

’619 Patent – Claim 51	Munje
	Accordingly, a diverse array of personal information appliances 18 such as desktop computers, laptop computers, palmtop computers or the like may be operably networked to one or more of the application servers 16-i, i=1, 2, . . . , N, with respect to the services supported in the enterprise network 14.” Munje at 2:49-67. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[51a] optically receiving information including a displayed service activation code from a remote device;	Munje discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22c], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[51b] registering the remote device for access to a messaging account using the service activation code;	Munje discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:

’619 Patent – Claim 51	Munje
	See [22d], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[51c] receiving a message for the messaging account;	Munje discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22e], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[51d] encrypting the message using an encryption key; and	Munje discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22f], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill

’619 Patent – Claim 51	Munje
	in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[51e] sending the message to the remote device,	Munje discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22g], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[51f] wherein the device is authenticated to access the messaging account.	Munje discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22h], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and

’619 Patent – Claim 51	Munje
	Exhibit 619-B.

’619 Patent – Claim 52	Munje
[52] The method of claim 51, wherein a control message is received from the remote device upon user interaction with the message.	Munje discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [36], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

EXHIBIT 619-A06

Invalidity Contentions for U.S. Patent No. 10,027,619 ("the '619 patent")

Based on: U.S. Patent App. No. 2004/0205248 to Little et al. ("Little")

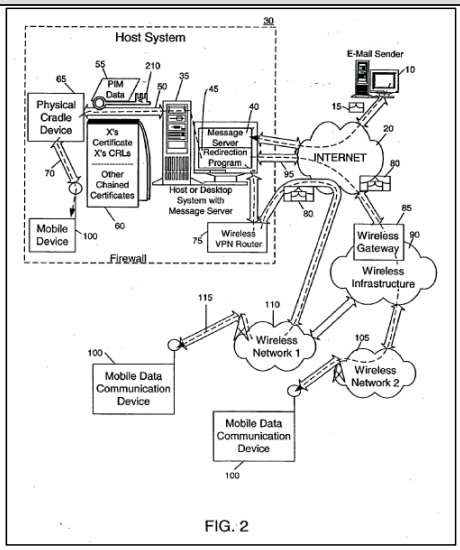
Based on SEVEN's apparent positions as to the scope of the patent's claims, as best they can be deciphered, the reference(s) charted below anticipate(s) or at least render(s) obvious the identified claims. The portions of the prior art reference cited below are not exhaustive but are exemplary in nature. Where Apple identifies a portion of the prior art reference's text, the identification should be understood as referencing any corresponding figure or diagram, and vice versa.

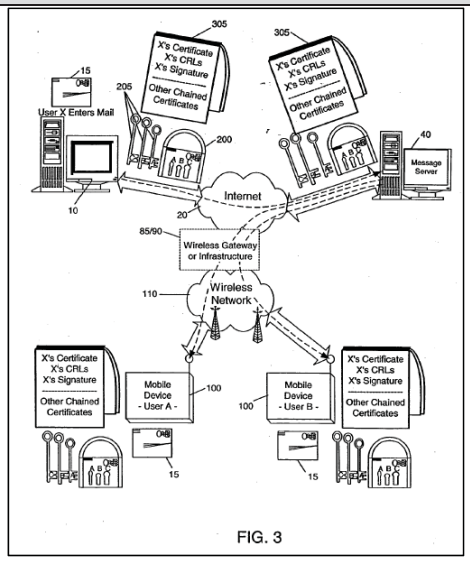
This disclosure is not an admission that Apple concedes any claim construction implied or suggested by SEVEN's apparent positions as to the scope of the patent's claims, nor is it an admission by Apple that any of its products are covered by or infringe the patent's claims, particularly when they are properly construed and applied. Apple is not taking any claim construction positions through this disclosure, including whether the preamble is a limitation.

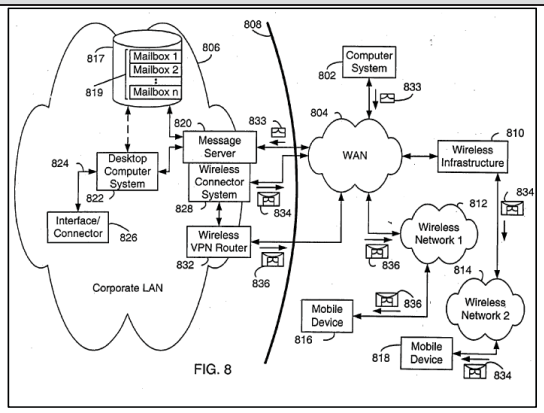
Apple reserves the right to rely on additional citations or sources of evidence that also may be applicable, or that may become applicable in light of claim construction, changes in SEVEN's infringement contentions, and/or information obtained during discovery as the case progresses. Apple further reserves the right to amend or supplement this claim chart at a later date as more fully set forth in the Invalidity Contentions.

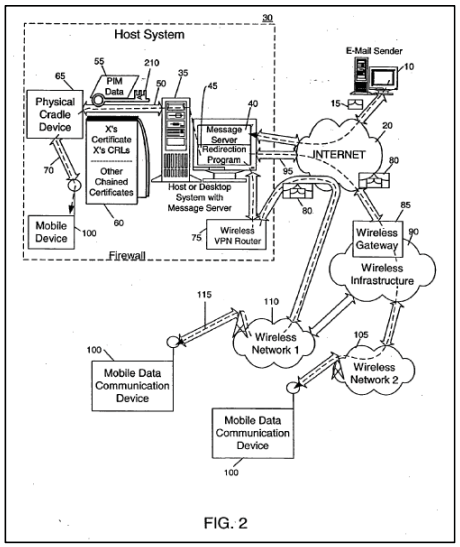
Little qualifies as prior art under at least pre-AIA 35 U.S.C. §§ 102(a), (b) and/or (e). Little is a U.S. Patent Application that was filed on July 10, 2002 and published on October 14, 2004.

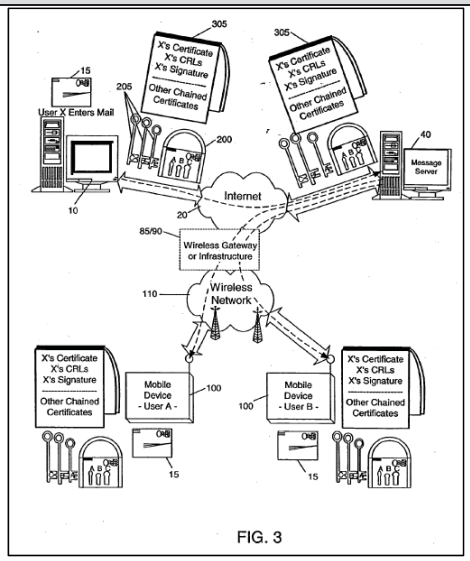
'619 Patent – Claim 22	Little
[22pre] A device comprising:	To the extent the preamble is limiting, Little discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:

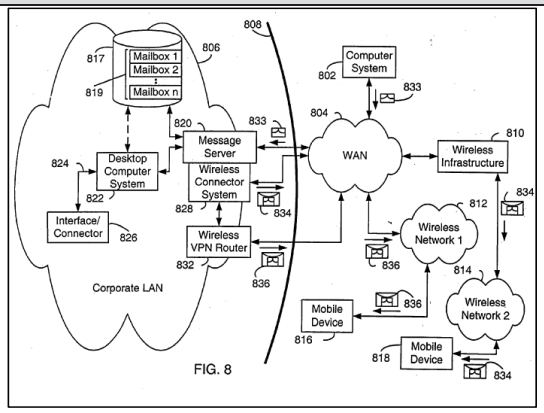
’619 Patent – Claim 22	Little
	 Little, Fig. 2.

’619 Patent – Claim 22	Little
	 FIG. 3 Little, Fig. 3.

’619 Patent – Claim 22	Little
	 FIG. 8 Little, Fig. 8. “Operation of the system in FIG. 8 will now be described using an example of an e-mail message 833 sent from-the computer system 812 and addressed to at least one recipient having both an account and mailbox 819 or like data store associated with the message server 820 and a mobile device 816 or 818. However, the e-mail message 833 is intended for illustrative purposes only. The exchange of other types of information between the corporate LAN 806 is preferably also enabled by the wireless connector system 828.” Little at [0076]. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine

’619 Patent – Claim 22	Little
	references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[22a] a radio;	Little discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:  Little, Fig. 2.

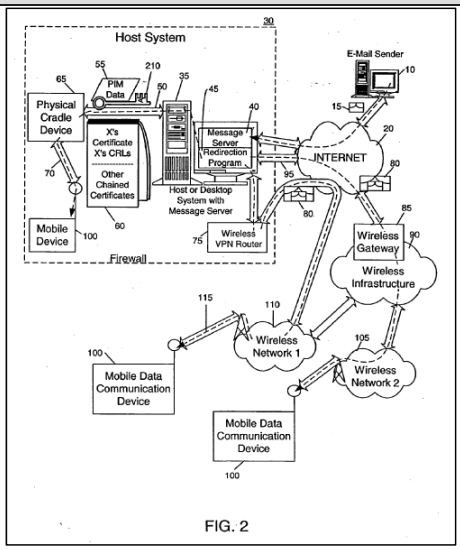
’619 Patent – Claim 22	Little
	 FIG. 3 Little, Fig. 3.

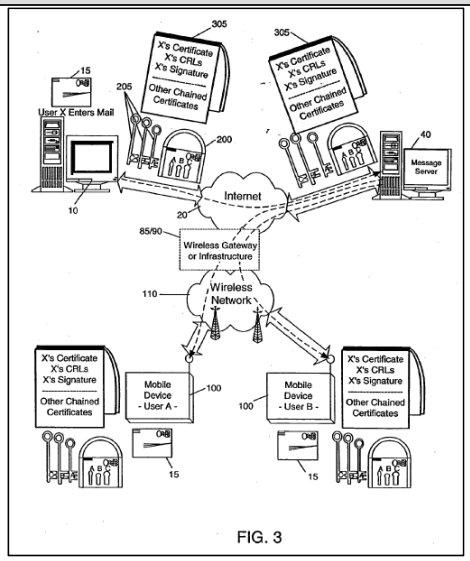
’619 Patent – Claim 22	Little
	 FIG. 8 Little, Fig. 8. “The wireless gateway 85 and infrastructure 90 provide a link between the Internet 20 and wireless network 105. The wireless infrastructure 90 may determine the most likely network for locating a given user and track users as they roam between countries or networks. A message is then delivered to the mobile device 100 via wireless transmission, typically at a radio frequency (RF), from a base station in the wireless network 105 to the mobile device 100. The particular network 105 may be virtually any wireless network over which messages may be exchanged with a mobile communication device.” Little at [0025]. “Regardless of the specific mechanism controlling the forwarding of messages to a mobile device 100, the message 15, or possibly a translated or reformatted version thereof, is sent to the wireless gateway 85. The wireless infrastructure 90 includes a series of connections to wireless network 105. These connections could be Integrated Services Digital Network (ISDN), Frame Relay or T1

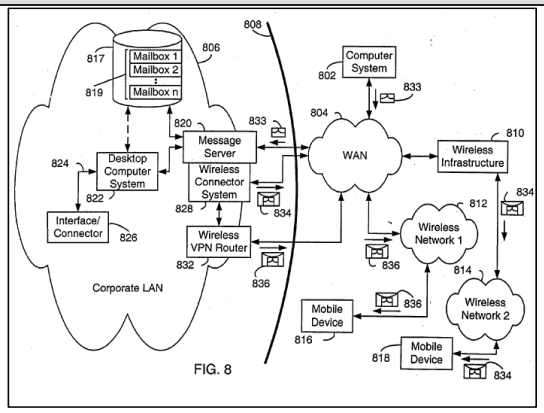
’619 Patent – Claim 22	Little
	connections using the TCP/IP protocol used throughout the Internet The term “wireless network” may include different types of networks, such as (1) data-centric wireless networks, (2) voice-centric wireless networks and (3) dual-mode networks that can support both voice and data communications over the same physical base stations. The newest of these combined dual-mode networks include, but are not limited to (1) modern Code Division Multiple Access (CDMA) networks, (2) the Groupe Special Mobile or the Global System for Mobile Communications (GSM) and the General Packet Radio Service (GPRS) network both developed by the standards committee of CEPT, and (3) the future third-generation (3G) networks like Enhanced Data-rates for Global Evolution (EDGE) and Universal Mobile Telecommunications Systems (UMTS). GPRS is a data overlay on the very popular GSM wireless network, operating in virtually every country in Europe. Some older examples of data-centric network include the Mobitex™ Radio Network, and the DataTAC™ Radio Network. Examples of older voice-centric data networks include Personal Communication Systems (PCS) networks like GSM and TDMA systems that have been available in North America and world-wide for nearly 10 years.” Little at [0027]. “Within the corporate LAN 806, the wireless connector system 828 operates in conjunction with the message server 820. The wireless connector system 828 may reside on the same computer system as the message server 820, or may instead be implemented on a different computer system. Software implementing the wireless connector system 828 may also be partially or entirely integrated with the message server 820. The wireless connector system 828 and the message server 820 are preferably designed to cooperate and interact to allow the pushing of information to mobile devices 816, 818. In such an installation, the wireless connector system 828 is preferably configured to send information that is stored in one or more data stores associated with the corporate LAN 806 to one or more mobile devices 816, 818, through the corporate firewall 808 and via the WAN 804 and one of the wireless networks 812, 814. For example, a user that has an account and associated mailbox 819

’619 Patent – Claim 22	Little
	in the data store 817 may also have a mobile device, such as 816. As described above, messages received by the message server 820 that identify a user, account or mailbox 819 are stored to a corresponding mailbox 819 by the message server 820. If a user has a mobile device, such as 816, messages received by the message server 820 and stored to the user's mailbox 819 are preferably detected by the wireless connector system 828 and sent to the user's mobile device 816. This type of functionality represents a “push” message sending technique. The wireless connector system 828 may instead employ a “pull” technique, in which items stored in a mailbox 819 are sent to a mobile device 816, 818 responsive to a request or access operation made using the mobile device, or some combination of both techniques. The use of a wireless connector 828 thereby enables a messaging system including a message server 820 to be extended so that each user's mobile device 816, 818 has access to stored messages of the message server 820. Although the systems and methods described herein are not restricted solely to a push-based technique, a more detailed description of push-based messaging may be found in the United States Patent and Applications incorporated by reference above. This push technique uses a wireless friendly encoding, compression and encryption technique to deliver all information to a mobile device, thus effectively extending the company firewall 808 to include the mobile devices 816, 818.” Little at [0067] - [0068]. “Another method for data exchange with a mobile device 816, 818 is over-the-air, through the wireless connector system 828 and using wireless networks 812, 814. As shown in FIG. 8, this could involve a Wireless VPN router 832, if available in the network 806, or, alternatively, a traditional WAN connection to wireless infrastructure 810 that provides an interface to one or more wireless networks 812, 814. The Wireless VPN router 832 provides for creation of a VPN connection directly through a specific wireless network 812 to a wireless device 816. Such a Wireless VPN router 832 may be used in conjunction with a static addressing scheme. For example, if the wireless network 812 is an IP-

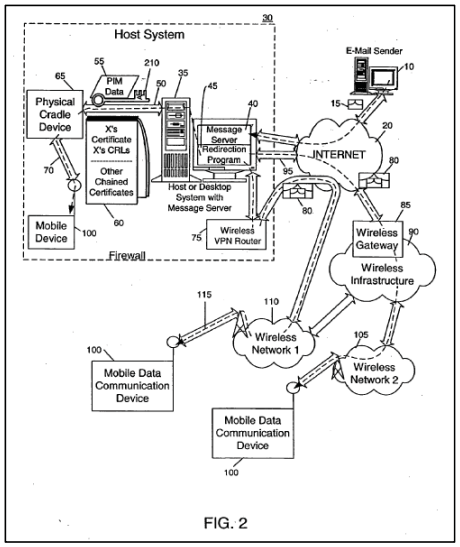
’619 Patent – Claim 22	Little
	based wireless network, then IPV6 would provide enough IP addresses to dedicate an IP address to every mobile device 816 configured to operate within the network 812 and thus make it possible to push information to a mobile device 816 at any time. A primary advantage of using a wireless VPN router 832 is that it could be an off-the-shelf VPN component which would not require wireless infrastructure 810. A VPN connection may use a TCP/IP or UDP/IP connection to deliver messages directly to and from a mobile device 816.” Little at [0072]. “The wireless connector system 828 sends or mirrors, via a wireless network 812 or 814, certain user-selected data items or parts of data items from the corporate LAN 806 to the user's mobile device 816 or 818, preferably upon detecting that one or more triggering events has occurred.” Little at [0079]. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[22b] a processor and memory containing instructions executable by the processor whereby the device is operable to:	Little discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:

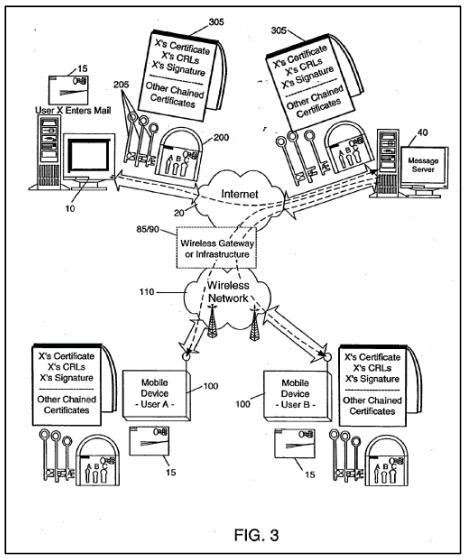
’619 Patent – Claim 22	Little
	 FIG. 2 Little, Fig. 2.

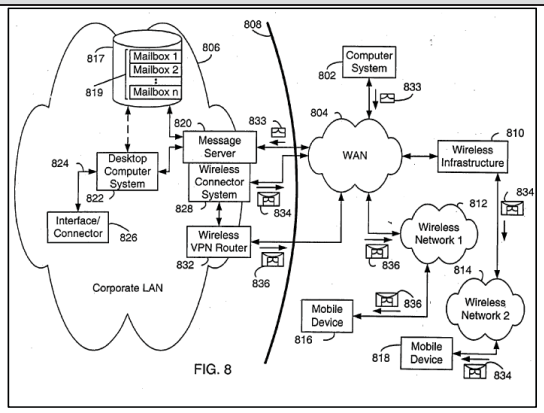
’619 Patent – Claim 22	Little
	 FIG. 3 Little, Fig. 3.

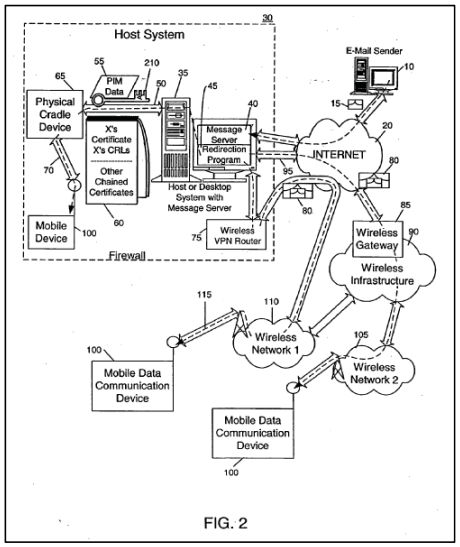
’619 Patent – Claim 22	Little
	 FIG. 8 Little, Fig. 8. “The central host system 30 will typically be a corporate office or other LAN, but may instead be a home office computer or some other secure system where mail messages are being exchanged. Within the host system 30 is the message server 40, running on some computer within the firewall of the host system, that acts as the main interface for the host system to exchange e-mail with the Internet 20. In the system of FIG. 2, the redirection program 45 enables redirection of data items from the server 40 to a mobile device 100. Although the redirection program 45 is shown to reside on the same machine as the message server 40 for ease of presentation, there is no requirement that it must reside on the message server. The redirection program 45 and the message server 40 are designed to co-operate and interact to allow the pushing of information to mobile devices 100. In this installation, the redirection program 45 takes confidential and non-confidential corporate information for a specific user and redirects it out through the corporate firewall to mobile devices 100. A more detailed description of the redirection software 45 may be found in the

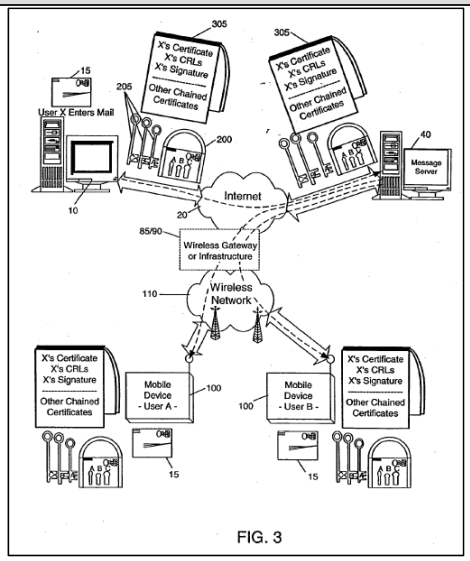
’619 Patent – Claim 22	Little
	commonly assigned U.S. Pat. No. 6,219,694 (“the ′694 Patent”), entitled “System and Method for Pushing Information From A Host System To A Mobile Data Communication Device Having A Shared Electronic Address”, and issued to the assignee of the instant application on Apr. 17, 2001, and U.S. patent applications Ser. No. 09/401,868, Ser. No. 09/545,963, Ser. No. 09/528,495, Ser. No. 09/545,962, and Ser. No. 09/649,755, all of which are hereby incorporated into the present application by reference. This push technique may use a wireless friendly encoding, compression and encryption technique to deliver all information to a mobile device thus effectively extending the security firewall to include each mobile device 100 associated with the host system.” Little at [0029]. “E-mail messages such as 833 normally use traditional SMTP, RFC822 headers and MIME body parts to define the format of the e-mail message. These techniques are all well known to one in the art. The e-mail message 833 arrives at the message server 820, which determines into which mailboxes 819 the e-mail message 833 should be stored. As described above, a message such as the e-mail message 833 may include a user name, a user account, a mailbox identifier, or other type of identifier that may be mapped to a particular account or associated mailbox 819 by the message server 820. For an e-mail message 833, recipients are typically identified using e-mail addresses corresponding to a user account and thus a mailbox 819.” Little at [0078]. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

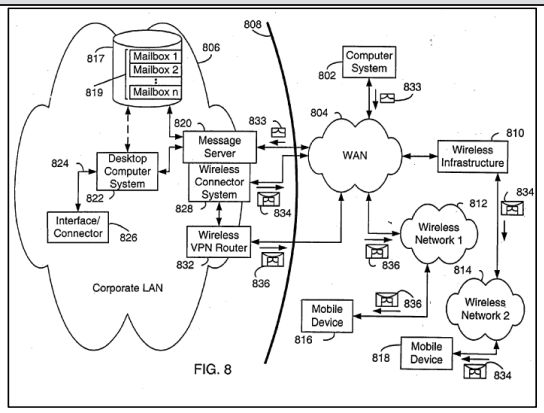
’619 Patent – Claim 22	Little
[22c] optically receive information including a displayed service activation code from a remote device;	This claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[22d] register the remote device for access to a messaging account using the service activation code;	Little discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:  FIG. 2

’619 Patent – Claim 22	Little
	Little, Fig. 2.  FIG. 3 Little, Fig. 3.

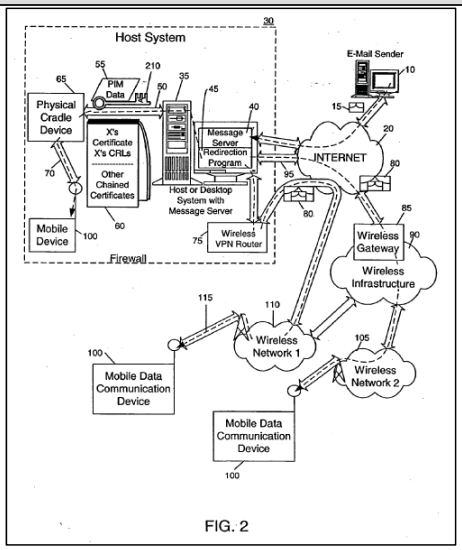
’619 Patent – Claim 22	Little
	 FIG. 8 Little, Fig. 8. “Depending upon the type of network or networks 1119, the access requirements for the mobile device 100 may also vary. For example, in the Mobitex and DataTAC data networks, mobile devices are registered on the network using a unique identification number associated with each mobile device. In GPRS data networks, however, network access is associated with a subscriber or user of a mobile device. A GPRS device typically requires a subscriber identity module (‘SIM’), which is required in order to operate a mobile device on a GPRS network. Local or non-network communication functions (if any) may be operable, without the SIM device, but a mobile device will be unable to carry out any functions involving communications over the data network 1119, other than any legally required operations, such as ‘911’ emergency calling.” Little at [0105]. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in

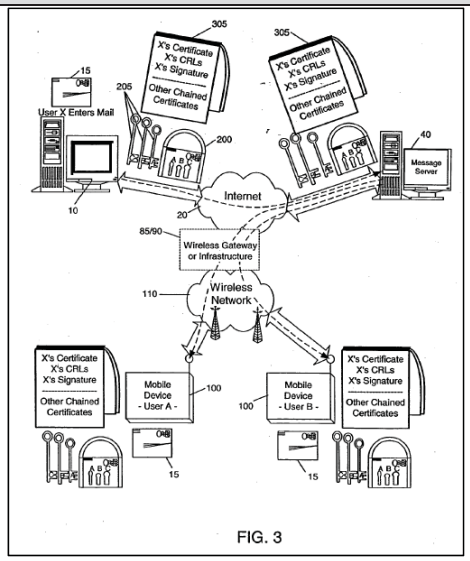
’619 Patent – Claim 22	Little
	Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[22e] receive a message for the messaging account;	Little discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:  FIG. 2 Little, Fig. 2.

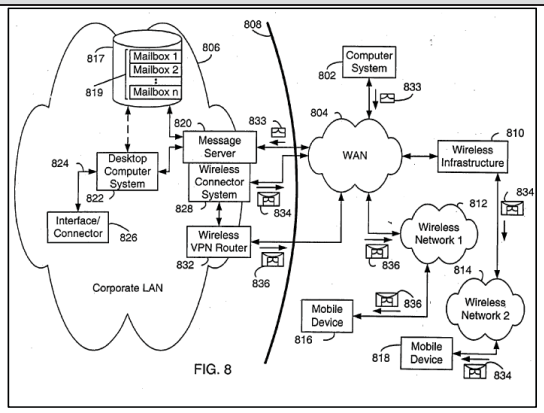
’619 Patent – Claim 22	Little
	 FIG. 3 Little, Fig. 3.

’619 Patent – Claim 22	Little
	 FIG. 8 Little, Fig. 8. “In the automatic redirection system of FIG. 2, a composed e-mail message 15 leaving the e-mail sender 10 arrives to the message server 40 and is redirected by the redirection program 45 to the mobile device 100. As this redirection takes place, the message 15 is re-enveloped, as indicated at 80, and a possibly proprietary compression and encryption algorithm can then be applied to the original message 15. In this way, messages being read on the mobile device 100 are no less secure than if they were read on a desktop workstation such as 35 within the firewall. All messages exchanged between the redirection program 45 and the mobile device 100 may use this message repackaging technique. Another goal of this outer envelope is to maintain the addressing information of the original message except the sender's and the receiver's address. This allows reply messages to reach the appropriate destination, and also allows the ‘from’ field to reflect the mobile user's desktop address. Using the user's e-mail address from the mobile device 100 allows the received message to appear as though the message originated from the user's desktop

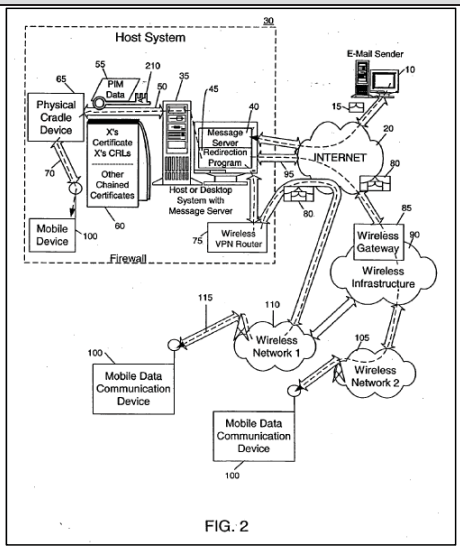
’619 Patent – Claim 22	Little
	system 35 rather than the mobile device 100.” Little at [0031]. “E-mail messages such as 833 normally use traditional SMTP, RFC822 headers and MIME body parts to define the format of the e-mail message. These techniques are all well known to one in the art. The e-mail message 833 arrives at the message server 820, which determines into which mailboxes 819 the e-mail message 833 should be stored. As described above, a message such as the e-mail message 833 may include a user name, a user account, a mailbox identifier, or other type of identifier that may be mapped to a particular account or associated mailbox 819 by the message server 820. For an e-mail message 833, recipients are typically identified using e-mail addresses corresponding to a user account and thus a mailbox 819.” Little at [0078]. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[22f] encrypt the message using an encryption key; and	Little discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:

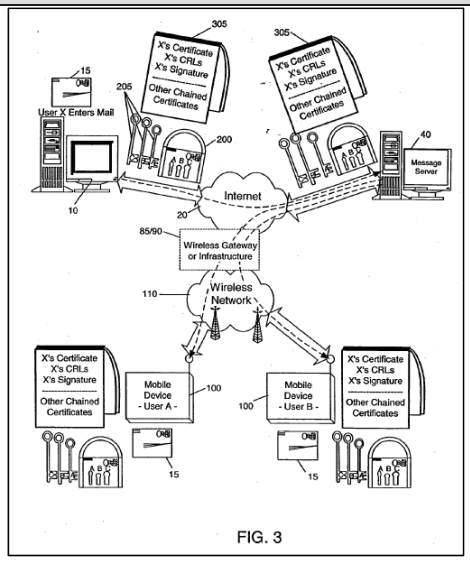
’619 Patent – Claim 22	Little
	 FIG. 2 Little, Fig. 2.

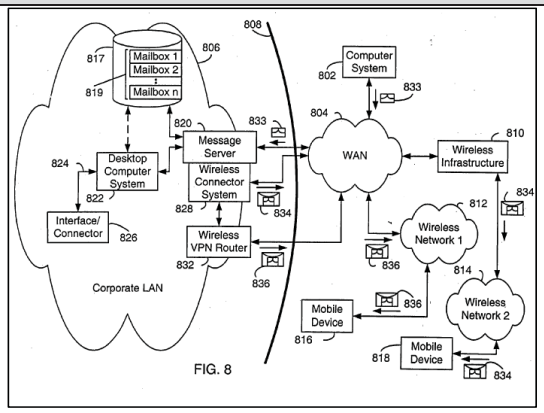
’619 Patent – Claim 22	Little
	 FIG. 3 Little, Fig. 3.

’619 Patent – Claim 22	Little
	 FIG. 8 Little, Fig. 8. “In the automatic redirection system of FIG. 2, a composed e-mail message 15 leaving the e-mail sender 10 arrives to the message server 40 and is redirected by the redirection program 45 to the mobile device 100. As this redirection takes place, the message 15 is re-enveloped, as indicated at 80, and a possibly proprietary compression and encryption algorithm can then be applied to the original message 15. In this way, messages being read on the mobile device 100 are no less secure than if they were read on a desktop workstation such as 35 within the firewall. All messages exchanged between the redirection program 45 and the mobile device 100 may use this message repackaging technique. Another goal of this outer envelope is to maintain the addressing information of the original message except the sender's and the receiver's address. This allows reply messages to reach the appropriate destination, and also allows the “from” field to reflect the mobile user's desktop address. Using the user's e-mail address from the mobile device 100 allows the received message to appear as though the message originated from the user's desktop

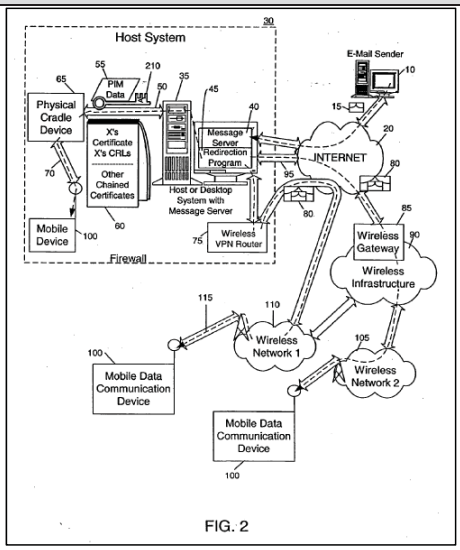
'619 Patent – Claim 22	Little
	system 35 rather than the mobile device 100." Little at [0031]. "Repackaging of the e-mail message 833 is indicated at 834 and 836. Repackaging techniques may be similar for any available transfer paths or may be dependent upon the particular transfer path, either the wireless infrastructure 810 or the wireless VPN router 832. For example, the e-mail message 833 is preferably compressed and encrypted, either before or after being repackaged at 834, to thereby effectively provide for secure transfer to the mobile device 818. Compression reduces the bandwidth required to send the message, whereas encryption ensures confidentiality of any messages or other information sent to mobile devices 816 and 818. In contrast, messages transferred via a VPN router 832 might only be compressed and not encrypted, since a VPN connection established by the VPN router 832 is inherently secure. Messages are thereby securely sent, via either encryption at the wireless connector system 828, which may be considered a non-standard VPN tunnel or a VPN-like connection for example, or the VPN router 832, to mobile devices 816 and 818. Accessing messages using a mobile device 816 or 818 is thus no less secure than accessing mailboxes at the LAN 806 using the desktop computer system 822." Little at [0081]. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[22g] send the message to the remote device,	Little discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:

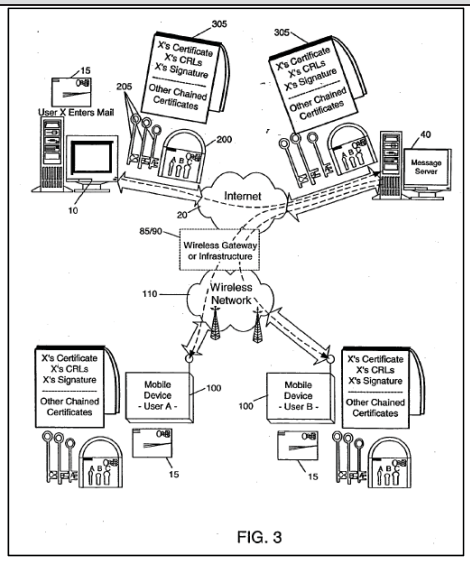
’619 Patent – Claim 22	Little
	 Little, Fig. 2.

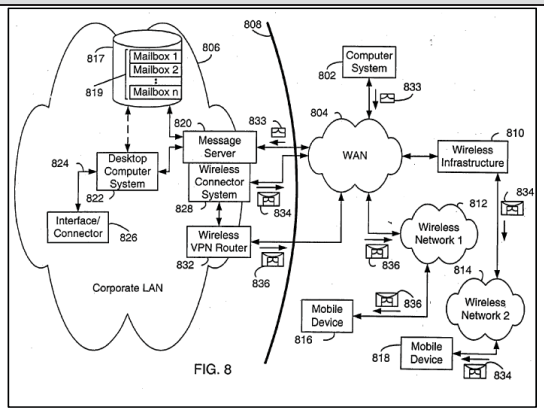
’619 Patent – Claim 22	Little
	 FIG. 3 Little, Fig. 3.

’619 Patent – Claim 22	Little
	 FIG. 8 Little, Fig. 8. “In the automatic redirection system of FIG. 2, a composed e-mail message 15 leaving the e-mail sender 10 arrives to the message server 40 and is redirected by the redirection program 45 to the mobile device 100. As this redirection takes place, the message 15 is re-enveloped, as indicated at 80, and a possibly proprietary compression and encryption algorithm can then be applied to the original message 15. In this way, messages being read on the mobile device 100 are no less secure than if they were read on a desktop workstation such as 35 within the firewall. All messages exchanged between the redirection program 45 and the mobile device 100 may use this message repackaging technique. Another goal of this outer envelope is to maintain the addressing information of the original message except the sender's and the receiver's address. This allows reply messages to reach the appropriate destination, and also allows the “from” field to reflect the mobile user's desktop address. Using the user's e-mail address from the mobile device 100 allows the received message to appear as though the message originated from the user's desktop

’619 Patent – Claim 22	Little
	system 35 rather than the mobile device 100.” Little at [0031]. “Repackaging of the e-mail message 833 is indicated at 834 and 836. Repackaging techniques may be similar for any available transfer paths or may be dependent upon the particular transfer path, either the wireless infrastructure 810 or the wireless VPN router 832. For example, the e-mail message 833 is preferably compressed and encrypted, either before or after being repackaged at 834, to thereby effectively provide for secure transfer to the mobile device 818. Compression reduces the bandwidth required to send the message, whereas encryption ensures confidentiality of any messages or other information sent to mobile devices 816 and 818. In contrast, messages transferred via a VPN router 832 might only be compressed and not encrypted, since a VPN connection established by the VPN router 832 is inherently secure. Messages are thereby securely sent, via either encryption at the wireless connector system 828, which may be considered a non-standard VPN tunnel or a VPN-like connection for example, or the VPN router 832, to mobile devices 816 and 818. Accessing messages using a mobile device 816 or 818 is thus no less secure than accessing mailboxes at the LAN 806 using the desktop computer system 822.” Little at [0081]. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[22h] wherein the device is authenticated to access the messaging account.	Little discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:

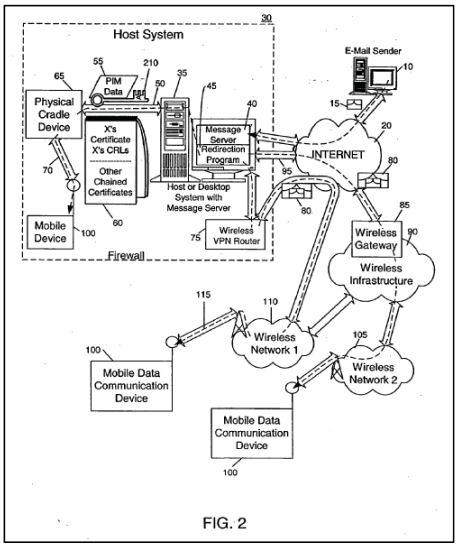
’619 Patent – Claim 22	Little
	 Little, Fig. 2.

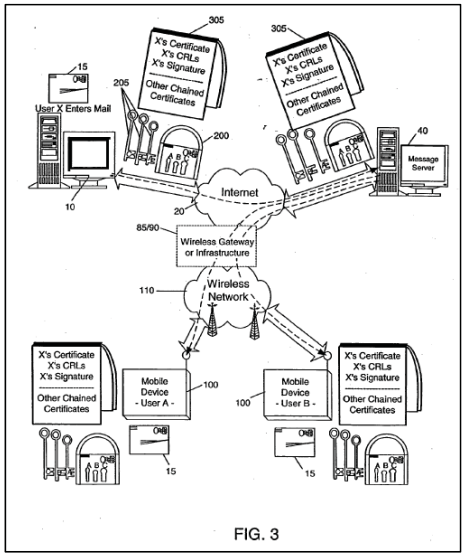
’619 Patent – Claim 22	Little
	 FIG. 3 Little, Fig. 3.

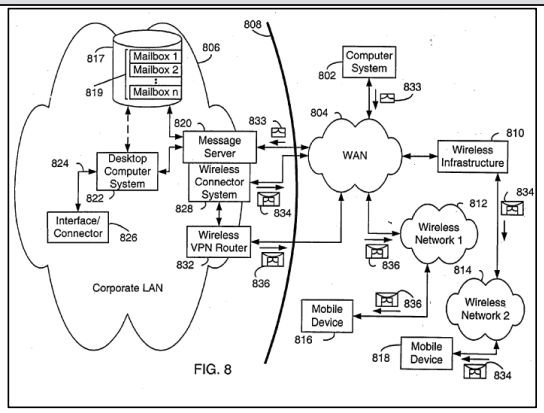
’619 Patent – Claim 22	Little
	 FIG. 8 Little, Fig. 8. “In the automatic redirection system of FIG. 2, a composed e-mail message 15 leaving the e-mail sender 10 arrives to the message server 40 and is redirected by the redirection program 45 to the mobile device 100. As this redirection takes place, the message 15 is re-enveloped, as indicated at 80, and a possibly proprietary compression and encryption algorithm can then be applied to the original message 15. In this way, messages being read on the mobile device 100 are no less secure than if they were read on a desktop workstation such as 35 within the firewall. All messages exchanged between the redirection program 45 and the mobile device 100 may use this message repackaging technique. Another goal of this outer envelope is to maintain the addressing information of the original message except the sender's and the receiver's address. This allows reply messages to reach the appropriate destination, and also allows the “from” field to reflect the mobile user's desktop address. Using the user's e-mail address from the mobile device 100 allows the received message to appear as though the message originated from the user's desktop

’619 Patent – Claim 22	Little
	system 35 rather than the mobile device 100.” Little at [0031]. “E-mail messages such as 833 normally use traditional SMTP, RFC822 headers and MIME body parts to define the format of the e-mail message. These techniques are all well known to one in the art. The e-mail message 833 arrives at the message server 820, which determines into which mailboxes 819 the e-mail message 833 should be stored. As described above, a message such as the e-mail message 833 may include a user name, a user account, a mailbox identifier, or other type of identifier that may be mapped to a particular account or associated mailbox 819 by the message server 820. For an e-mail message 833, recipients are typically identified using e-mail addresses corresponding to a user account and thus a mailbox 819.” Little at [0078]. “Depending upon the type of network or networks 1119, the access requirements for the mobile device 100 may also vary. For example, in the Mobitex and DataTAC data networks, mobile devices are registered on the network using a unique identification number associated with each mobile device. In GPRS data networks, however, network access is associated with a subscriber or user of a mobile device. A GPRS device typically requires a subscriber identity module (“SIM”), which is required in order to operate a mobile device on a GPRS network. Local or non-network communication functions (if any) may be operable, without the SIM device, but a mobile device will be unable to carry out any functions involving communications over the data network 1119, other than any legally required operations, such as ‘911’ emergency calling.” Little at [0105]. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine

’619 Patent – Claim 22	Little
	references and additional details may be found in the Cover Pleading and Exhibit 619-B.

’619 Patent – Claim 23	Little
[23] The device of claim 22, wherein the information including the service activation code is received by the device in response to user input at the remote device.	Little discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22pre]-[22h], *above*.  FIG. 2

’619 Patent – Claim 23	Little
	Little, Fig. 2.  FIG. 3 Little, Fig. 3.

’619 Patent – Claim 23	Little
	 FIG. 8 Little, Fig. 8. “If the message is not signed, such that X's signature and other signature-related information including X's CRLs, X's Cert and other chained Certs would not be part of the message, or the message was signed before it was encrypted, then when a user of a mobile device 100 opens the message, the appropriate encrypted session key is found and decrypted. However, if the message was signed after being encrypted then the signature is preferably first verified and the correct session key is then found and decrypted. As those skilled in the art will appreciate, session key decryption commonly involves the further security operation of entering a password or passphrase preferably known only to the user of a mobile device.” Little at [0044]. “In the automatic redirection system of FIG. 2, a composed e-mail message 15 leaving the e-mail sender 10 arrives to the message server 40 and is redirected by the redirection program 45 to the mobile device 100. As this redirection takes place, the message 15 is re-enveloped, as indicated at 80, and a possibly

’619 Patent – Claim 23	Little
	proprietary compression and encryption algorithm can then be applied to the original message 15. In this way, messages being read on the mobile device 100 are no less secure than if they were read on a desktop workstation such as 35 within the firewall. All messages exchanged between the redirection program 45 and the mobile device 100 may use this message repackaging technique. Another goal of this outer envelope is to maintain the addressing information of the original message except the sender's and the receiver's address. This allows reply messages to reach the appropriate destination, and also allows the “from” field to reflect the mobile user's desktop address. Using the user's e-mail address from the mobile device 100 allows the received message to appear as though the message originated from the user's desktop system 35 rather than the mobile device 100.” Little at [0031]. “E-mail messages such as 833 normally use traditional SMTP, RFC822 headers and MIME body parts to define the format of the e-mail message. These techniques are all well known to one in the art. The e-mail message 833 arrives at the message server 820, which determines into which mailboxes 819 the e-mail message 833 should be stored. As described above, a message such as the e-mail message 833 may include a user name, a user account, a mailbox identifier, or other type of identifier that may be mapped to a particular account or associated mailbox 819 by the message server 820. For an e-mail message 833, recipients are typically identified using e-mail addresses corresponding to a user account and thus a mailbox 819.” Little at [0078]. “Depending upon the type of network or networks 1119, the access requirements for the mobile device 100 may also vary. For example, in the Mobitex and DataTAC data networks, mobile devices are registered on the network using a unique identification number associated with each mobile device. In GPRS data networks, however, network access is associated with a subscriber or user of a mobile device. A GPRS device typically requires a subscriber identity module (“SIM”), which is required in order to operate a mobile device on a GPRS network. Local or non-network communication

'619 Patent – Claim 23	Little
	functions (if any) may be operable, without the SIM device, but a mobile device will be unable to carry out any functions involving communications over the data network 1119, other than any legally required operations, such as '911' emergency calling." Little at [0105]. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

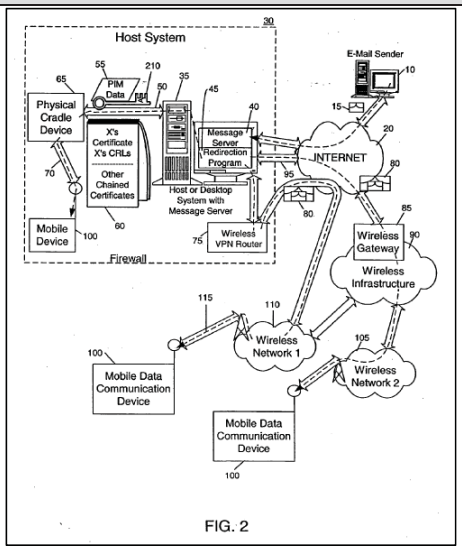
'619 Patent – Claim 24	Little
[24] The device of claim 22, wherein the information including the service activation code is received by the device in an off-line communication.	This claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

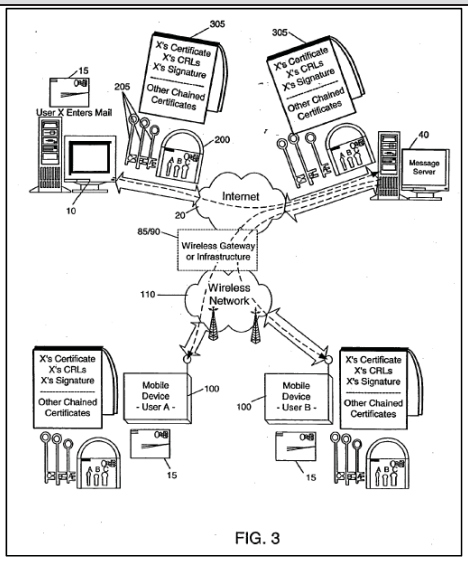
'619 Patent – Claim 25	Little
[25] The device of claim 24, wherein the off-line	This claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A,

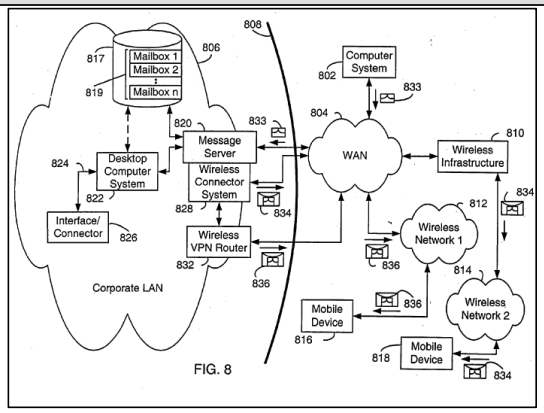
'619 Patent – Claim 25	Little
communication involves a local connection.	and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

'619 Patent – Claim 26	Little
[26] The device of claim 24, wherein the off-line communication prevents eavesdropping of the service activation code.	This claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

'619 Patent – Claim 27	Little
[27] The device of claim 22, wherein the authentication of the device relies on the authentication of the messaging account.	Little discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22pre]-[22h], *above*.

’619 Patent – Claim 27	Little
	 Little, Fig. 2.

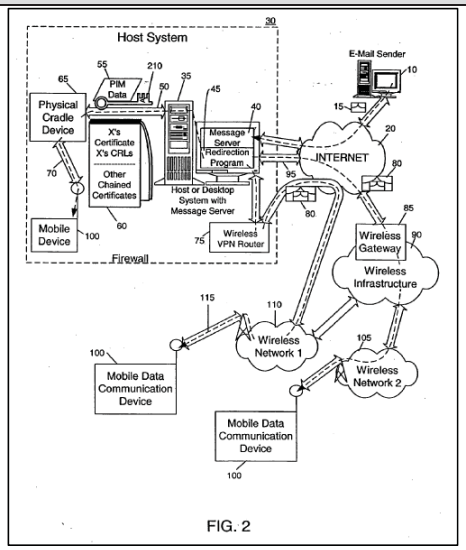
’619 Patent – Claim 27	Little
	 FIG. 3 Little, Fig. 3.

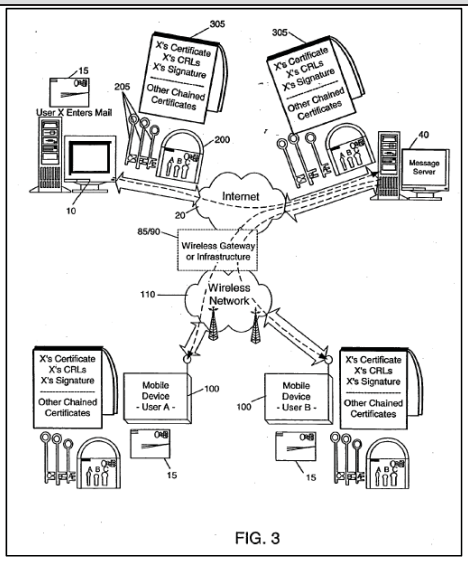
’619 Patent – Claim 27	Little
	 FIG. 8 Little, Fig. 8. “If the message is not signed, such that X's signature and other signature-related information including X's CRLs, X's Cert and other chained Certs would not be part of the message, or the message was signed before it was encrypted, then when a user of a mobile device 100 opens the message, the appropriate encrypted session key is found and decrypted. However, if the message was signed after being encrypted then the signature is preferably first verified and the correct session key is then found and decrypted. As those skilled in the art will appreciate, session key decryption commonly involves the further security operation of entering a password or passphrase preferably known only to the user of a mobile device.” Little at [0044]. “In the automatic redirection system of FIG. 2, a composed e-mail message 15 leaving the e-mail sender 10 arrives to the message server 40 and is redirected by the redirection program 45 to the mobile device 100. As this redirection takes place, the message 15 is re-enveloped, as indicated at 80, and a possibly

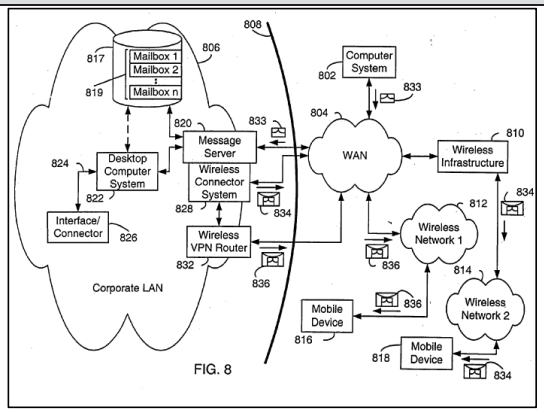
’619 Patent – Claim 27	Little
	proprietary compression and encryption algorithm can then be applied to the original message 15. In this way, messages being read on the mobile device 100 are no less secure than if they were read on a desktop workstation such as 35 within the firewall. All messages exchanged between the redirection program 45 and the mobile device 100 may use this message repackaging technique. Another goal of this outer envelope is to maintain the addressing information of the original message except the sender's and the receiver's address. This allows reply messages to reach the appropriate destination, and also allows the “from” field to reflect the mobile user's desktop address. Using the user's e-mail address from the mobile device 100 allows the received message to appear as though the message originated from the user's desktop system 35 rather than the mobile device 100.” Little at [0031]. “E-mail messages such as 833 normally use traditional SMTP, RFC822 headers and MIME body parts to define the format of the e-mail message. These techniques are all well known to one in the art. The e-mail message 833 arrives at the message server 820, which determines into which mailboxes 819 the e-mail message 833 should be stored. As described above, a message such as the e-mail message 833 may include a user name, a user account, a mailbox identifier, or other type of identifier that may be mapped to a particular account or associated mailbox 819 by the message server 820. For an e-mail message 833, recipients are typically identified using e-mail addresses corresponding to a user account and thus a mailbox 819.” Little at [0078]. “Depending upon the type of network or networks 1119, the access requirements for the mobile device 100 may also vary. For example, in the Mobitex and DataTAC data networks, mobile devices are registered on the network using a unique identification number associated with each mobile device. In GPRS data networks, however, network access is associated with a subscriber or user of a mobile device. A GPRS device typically requires a subscriber identity module (“SIM”), which is required in order to operate a mobile device on a GPRS network. Local or non-network communication

'619 Patent – Claim 27	Little
	functions (if any) may be operable, without the SIM device, but a mobile device will be unable to carry out any functions involving communications over the data network 1119, other than any legally required operations, such as '911' emergency calling." Little at [0105]. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

'619 Patent – Claim 28	Little
[28] The device of claim 27, wherein the authentication of the messaging account includes a username and password.	Little discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22pre]-[22h] and [27], *above*.

’619 Patent – Claim 28	Little
	 Little, Fig. 2.

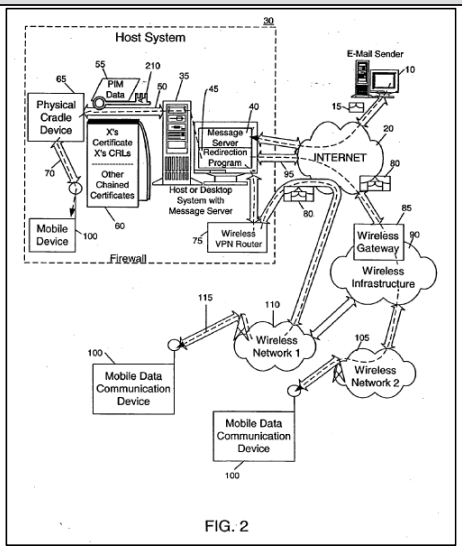
’619 Patent – Claim 28	Little
	 FIG. 3 Little, Fig. 3.

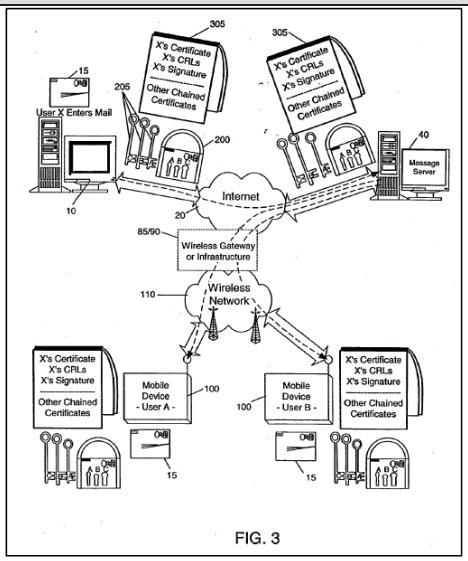
’619 Patent – Claim 28	Little
	 FIG. 8 Little, Fig. 8. “If the message is not signed, such that X's signature and other signature-related information including X's CRLs, X's Cert and other chained Certs would not be part of the message, or the message was signed before it was encrypted, then when a user of a mobile device 100 opens the message, the appropriate encrypted session key is found and decrypted. However, if the message was signed after being encrypted then the signature is preferably first verified and the correct session key is then found and decrypted. As those skilled in the art will appreciate, session key decryption commonly involves the further security operation of entering a password or passphrase preferably known only to the user of a mobile device.” Little at [0044]. “In the automatic redirection system of FIG. 2, a composed e-mail message 15 leaving the e-mail sender 10 arrives to the message server 40 and is redirected by the redirection program 45 to the mobile device 100. As this redirection takes place, the message 15 is re-enveloped, as indicated at 80, and a possibly

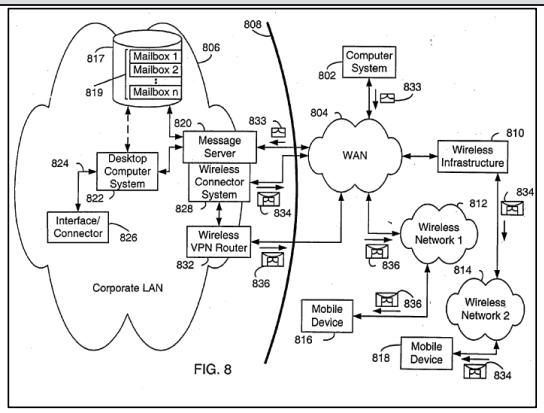
’619 Patent – Claim 28	Little
	proprietary compression and encryption algorithm can then be applied to the original message 15. In this way, messages being read on the mobile device 100 are no less secure than if they were read on a desktop workstation such as 35 within the firewall. All messages exchanged between the redirection program 45 and the mobile device 100 may use this message repackaging technique. Another goal of this outer envelope is to maintain the addressing information of the original message except the sender's and the receiver's address. This allows reply messages to reach the appropriate destination, and also allows the “from” field to reflect the mobile user's desktop address. Using the user's e-mail address from the mobile device 100 allows the received message to appear as though the message originated from the user's desktop system 35 rather than the mobile device 100.” Little at [0031]. “E-mail messages such as 833 normally use traditional SMTP, RFC822 headers and MIME body parts to define the format of the e-mail message. These techniques are all well known to one in the art. The e-mail message 833 arrives at the message server 820, which determines into which mailboxes 819 the e-mail message 833 should be stored. As described above, a message such as the e-mail message 833 may include a user name, a user account, a mailbox identifier, or other type of identifier that may be mapped to a particular account or associated mailbox 819 by the message server 820. For an e-mail message 833, recipients are typically identified using e-mail addresses corresponding to a user account and thus a mailbox 819.” Little at [0078]. “Depending upon the type of network or networks 1119, the access requirements for the mobile device 100 may also vary. For example, in the Mobitex and DataTAC data networks, mobile devices are registered on the network using a unique identification number associated with each mobile device. In GPRS data networks, however, network access is associated with a subscriber or user of a mobile device. A GPRS device typically requires a subscriber identity module (“SIM”), which is required in order to operate a mobile device on a GPRS network. Local or non-network communication

'619 Patent – Claim 28	Little
	functions (if any) may be operable, without the SIM device, but a mobile device will be unable to carry out any functions involving communications over the data network 1119, other than any legally required operations, such as '911' emergency calling." Little at [0105]. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

'619 Patent – Claim 32	Little
[32] The device of claim 22, wherein the encryption key is closely related to the service activation code.	Little discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22pre]-[22h], *above*.

’619 Patent – Claim 32	Little
	 Little, Fig. 2.

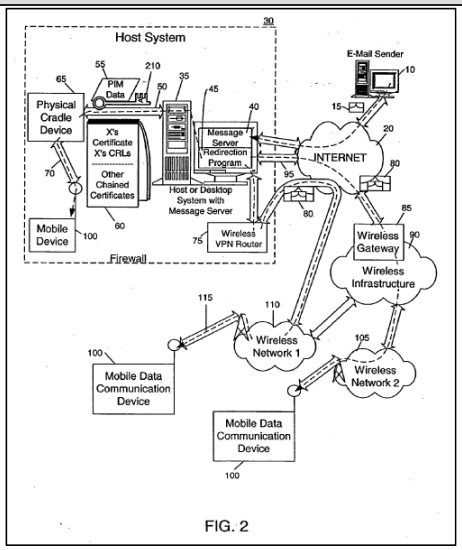
’619 Patent – Claim 32	Little
	 FIG. 3 Little, Fig. 3.

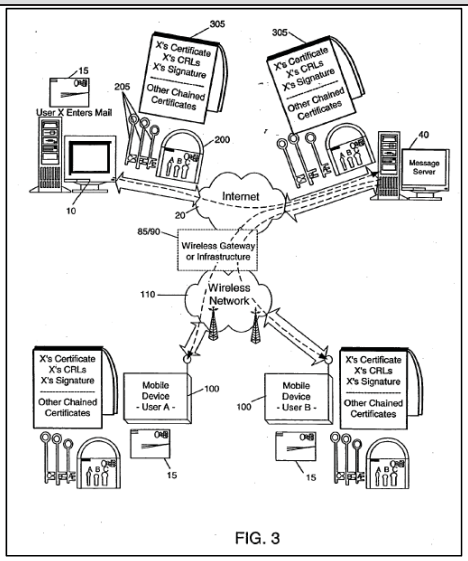
’619 Patent – Claim 32	Little
	 FIG. 8 Little, Fig. 8. “In encrypted S/MIME message operations, a one-time session key is generated and used for each message, and is never re-used for other messages. The session key is then further encrypted using the receiver's public key. If the message is addressed to more than one receiver, the same'session key is encrypted using the public key of each receiver. Only when all receivers have an encoded session key is the message then sent to each receiver. Since the e-mail retains only one form, all encrypted session keys are sent to every receiver, even though they cannot use these other session keys. Each receiver then locates its own session key, possibly based on a generated recipient information summary of the receivers that may be attached to the message, and decrypts the session key using its private key. Once the session key is decrypted, it is then used to decrypt the message body. The S/MIME recipient information attachment can also specify a particular encryption scheme that is used to decrypt the message. This information is normally placed in the header

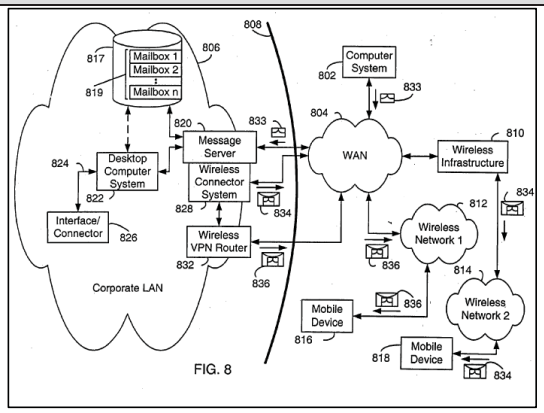
’619 Patent – Claim 32	Little
	of the S/MIME message.” Little at [0037]. “In the automatic redirection system of FIG. 2, a composed e-mail message 15 leaving the e-mail sender 10 arrives to the message server 40 and is redirected by the redirection program 45 to the mobile device 100. As this redirection takes place, the message 15 is re-enveloped, as indicated at 80, and a possibly proprietary compression and encryption algorithm can then be applied to the original message 15. In this way, messages being read on the mobile device 100 are no less secure than if they were read on a desktop workstation such as 35 within the firewall. All messages exchanged between the redirection program 45 and the mobile device 100 may use this message repackaging technique. Another goal of this outer envelope is to maintain the addressing information of the original message except the sender's and the receiver's address. This allows reply messages to reach the appropriate destination, and also allows the “from” field to reflect the mobile user's desktop address. Using the user's e-mail address from the mobile device 100 allows the received message to appear as though the message originated from the user's desktop system 35 rather than the mobile device 100.” Little at [0031]. “E-mail messages such as 833 normally use traditional SMTP, RFC822 headers and MIME body parts to define the format of the e-mail message. These techniques are all well known to one in the art. The e-mail message 833 arrives at the message server 820, which determines into which mailboxes 819 the e-mail message 833 should be stored. As described above, a message such as the e-mail message 833 may include a user name, a user account, a mailbox identifier, or other type of identifier that may be mapped to a particular account or associated mailbox 819 by the message server 820. For an e-mail message 833, recipients are typically identified using e-mail addresses corresponding to a user account and thus a mailbox 819.” Little at [0078]. “Depending upon the type of network or networks 1119, the access requirements for the mobile device 100 may also vary. For example, in the

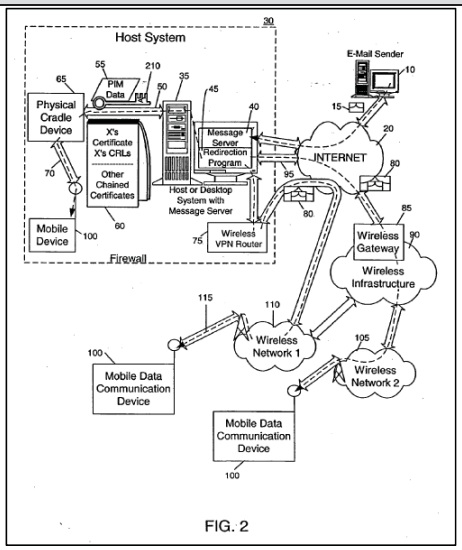
’619 Patent – Claim 32	Little
	Mobitex and DataTAC data networks, mobile devices are registered on the network using a unique identification number associated with each mobile device. In GPRS data networks, however, network access is associated with a subscriber or user of a mobile device. A GPRS device typically requires a subscriber identity module (“SIM”), which is required in order to operate a mobile device on a GPRS network. Local or non-network communication functions (if any) may be operable, without the SIM device, but a mobile device will be unable to carry out any functions involving communications over the data network 1119, other than any legally required operations, such as ‘911’ emergency calling.” Little at [0105]. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

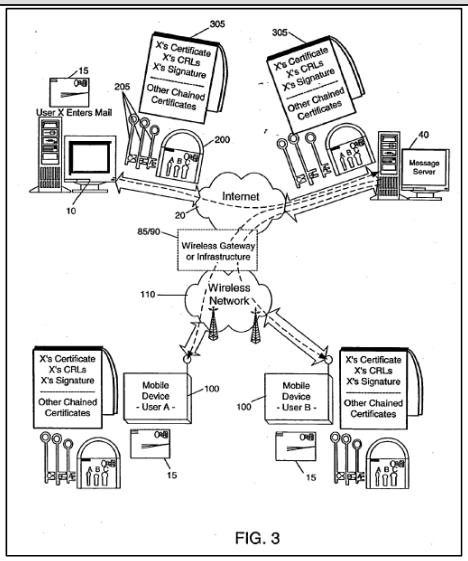
’619 Patent – Claim 33	Little
[33a] The device of claim 22, wherein the device is further operable to:	Little discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22pre]-[22h], *above*.

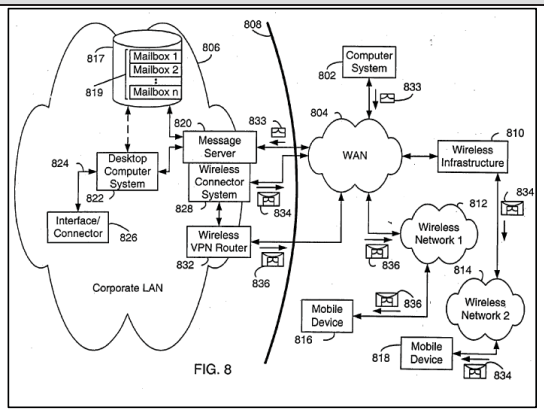
’619 Patent – Claim 33	Little
	 FIG. 2 Little, Fig. 2.

’619 Patent – Claim 33	Little
	 FIG. 3 Little, Fig. 3.

’619 Patent – Claim 33	Little
	 FIG. 8 Little, Fig. 8. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[33b] store an association between at least two of the encryption key, the messaging account, an identifier of the remote device, and the service activation code.	Little discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22pre]-[22h], *above*.

’619 Patent – Claim 33	Little
	 Little, Fig. 2.

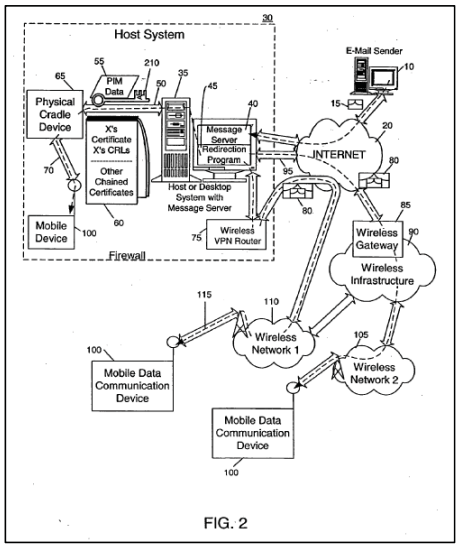
’619 Patent – Claim 33	Little
	 FIG. 3 Little, Fig. 3.

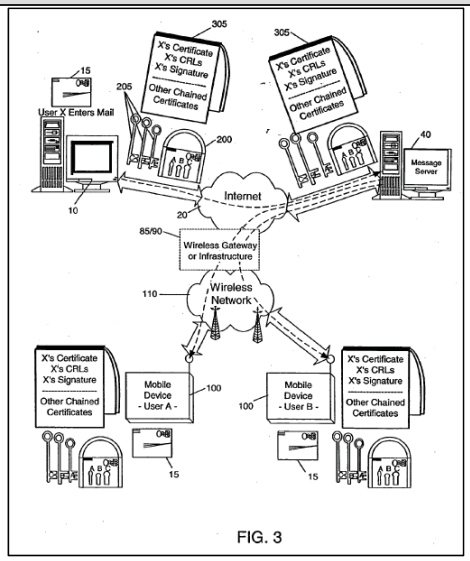
’619 Patent – Claim 33	Little
	 FIG. 8 Little, Fig. 8. “In encrypted S/MIME message operations, a one-time session key is generated and used for each message, and is never re-used for other messages. The session key is then further encrypted using the receiver's public key. If the message is addressed to more than one receiver, the same'session key is encrypted using the public key of each receiver. Only when all receivers have an encoded session key is the message then sent to each receiver. Since the e-mail retains only one form, all encrypted session keys are sent to every receiver, even though they cannot use these other session keys. Each receiver then locates its own session key, possibly based on a generated recipient information summary of the receivers that may be attached to the message, and decrypts the session key using its private key. Once the session key is decrypted, it is then used to decrypt the message body. The S/MIME recipient information attachment can also specify a particular encryption scheme that is used to decrypt the message. This information is normally placed in the header

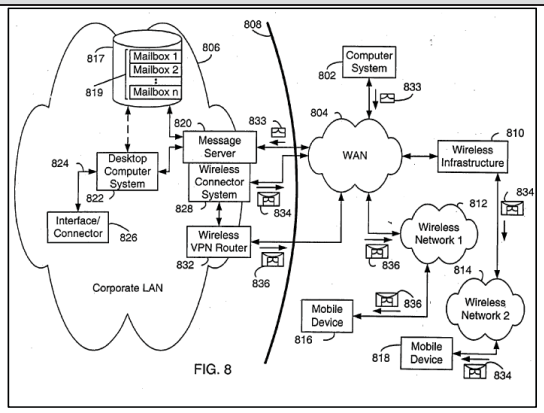
'619 Patent – Claim 33	Little
	of the S/MIME message." Little at [0037]. "E-mail messages such as 833 normally use traditional SMTP, RFC822 headers and MIME body parts to define the format of the e-mail message. These techniques are all well known to one in the art. The e-mail message 833 arrives at the message server 820, which determines into which mailboxes 819 the e-mail message 833 should be stored. As described above, a message such as the e-mail message 833 may include a user name, a user account, a mailbox identifier, or other type of identifier that may be mapped to a particular account or associated mailbox 819 by the message server 820. For an e-mail message 833, recipients are typically identified using e-mail addresses corresponding to a user account and thus a mailbox 819." Little at [0078]. "In the automatic redirection system of FIG. 2, a composed e-mail message 15 leaving the e-mail sender 10 arrives to the message server 40 and is redirected by the redirection program 45 to the mobile device 100. As this redirection takes place, the message 15 is re-enveloped, as indicated at 80, and a possibly proprietary compression and encryption algorithm can then be applied to the original message 15. In this way, messages being read on the mobile device 100 are no less secure than if they were read on a desktop workstation such as 35 within the firewall. All messages exchanged between the redirection program 45 and the mobile device 100 may use this message repackaging technique. Another goal of this outer envelope is to maintain the addressing information of the original message except the sender's and the receiver's address. This allows reply messages to reach the appropriate destination, and also allows the "from" field to reflect the mobile user's desktop address. Using the user's e-mail address from the mobile device 100 allows the received message to appear as though the message originated from the user's desktop system 35 rather than the mobile device 100." Little at [0031]. "Depending upon the type of network or networks 1119, the access requirements for the mobile device 100 may also vary. For example, in the

’619 Patent – Claim 33	Little
	Mobitex and DataTAC data networks, mobile devices are registered on the network using a unique identification number associated with each mobile device. In GPRS data networks, however, network access is associated with a subscriber or user of a mobile device. A GPRS device typically requires a subscriber identity module (“SIM”), which is required in order to operate a mobile device on a GPRS network. Local or non-network communication functions (if any) may be operable, without the SIM device, but a mobile device will be unable to carry out any functions involving communications over the data network 1119, other than any legally required operations, such as ‘911’ emergency calling.” Little at [0105]. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

’619 Patent – Claim 36	Little
[36] The device of claim 22, wherein a control message is received from the remote device upon user interaction with the message.	Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

’619 Patent – Claim 37	Little
[37pre] 37. A method for sharing a messaging account, the method comprising:	To the extent the preamble is limiting, Little discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:  FIG. 2 Little, Fig. 2.

’619 Patent – Claim 37	Little
	 FIG. 3 Little, Fig. 3.

’619 Patent – Claim 37	Little
	 FIG. 8 Little, Fig. 8. “Operation of the system in FIG. 8 will now be described using an example of an e-mail message 833 sent from-the computer system 812 and addressed to at least one recipient having both an account and mailbox 819 or like data store associated with the message server 820 and a mobile device 816 or 818. However, the e-mail message 833 is intended for illustrative purposes only. The exchange of other types of information between the corporate LAN 806 is preferably also enabled by the wireless connector system 828.” Little at [0076]. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine

’619 Patent – Claim 37	Little
	references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[37a] authenticating a device for access to the messaging account;	Little discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22h], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[37b] optically receiving information including a displayed service activation code from a remote device;	Little discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22c], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[37c] registering the remote device for access to the messaging account using the service	Little discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:

'619 Patent – Claim 37	Little
activation code;	*See* [22d], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[37d] receiving a message for the messaging account;	Little discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22e], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[37e] encrypting the message using an encryption key; and	Little discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22f], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill

'619 Patent – Claim 37	Little
	in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[37f] sending the message to the remote device.	Little discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22g], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

'619 Patent – Claim 38	Little
[38] The method of claim 37, wherein the information including the service activation code is received by the device in response to user input at the remote device.	Little discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [23], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person

'619 Patent – Claim 38	Little
	of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

'619 Patent – Claim 39	Little
[39] The method of claim 38, wherein the information including the service activation code is received by the device in an off-line communication.	Little discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [24], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

'619 Patent – Claim 40	Little
[40] The method of claim 39, wherein the off-line communication prevents eavesdropping of the service activation code.	Little discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [26], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in

'619 Patent – Claim 40	Little
	Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

'619 Patent – Claim 41	Little
[41] The method of claim 37, wherein the authentication of the device relies on the authentication of the messaging system.	Little discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [27], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

'619 Patent – Claim 42	Little
[42] The method of claim 41, wherein the authentication of the messaging system includes a username and password.	Little discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [28], above.

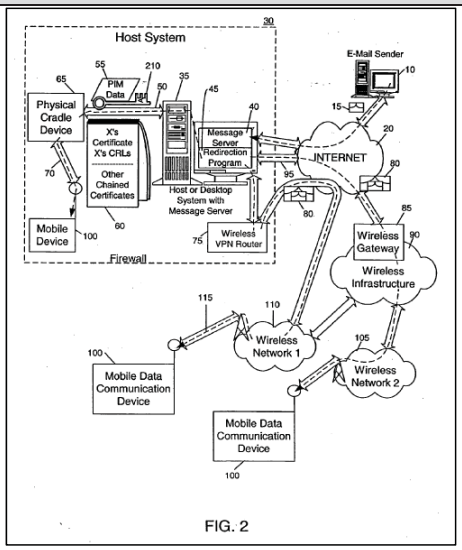
’619 Patent – Claim 42	Little
	Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

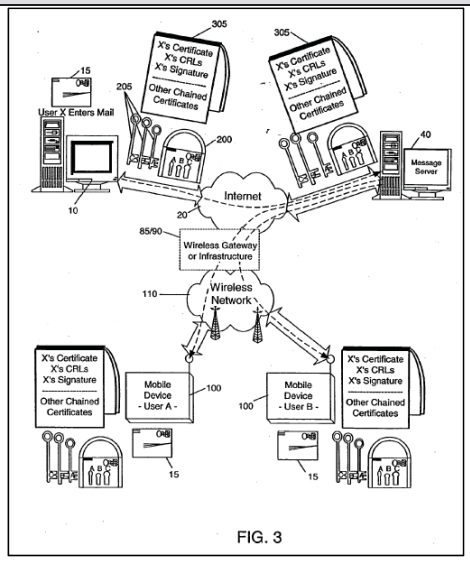
’619 Patent – Claim 46	Little
[46] The method of claim 37, wherein the encryption key is closely related to the service activation code.	Little discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [32], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

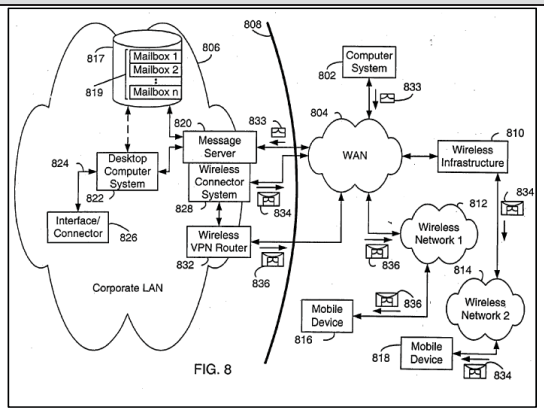
’619 Patent – Claim 50	Little
[50] The method of claim 37, wherein a control message is received from the remote device	Little discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:

’619 Patent – Claim 50	Little
upon user interaction with the message.	*See* [36], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

’619 Patent – Claim 51	Little
[51pre] 51. A non-transient computer-readable medium containing program instructions for causing a device to perform a method, the method comprising:	To the extent the preamble is limiting, Little discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:

’619 Patent – Claim 51	Little
	 FIG. 2 Little, Fig. 2.

’619 Patent – Claim 51	Little
	 FIG. 3 Little, Fig. 3.

’619 Patent – Claim 51	Little
	 FIG. 8 Little, Fig. 8. “Operation of the system in FIG. 8 will now be described using an example of an e-mail message 833 sent from-the computer system 812 and addressed to at least one recipient having both an account and mailbox 819 or like data store associated with the message server 820 and a mobile device 816 or 818. However, the e-mail message 833 is intended for illustrative purposes only. The exchange of other types of information between the corporate LAN 806 is preferably also enabled by the wireless connector system 828.” Little at [0076]. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine

'619 Patent – Claim 51	Little
	references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[51a] optically receiving information including a displayed service activation code from a remote device;	Little discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22c], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[51b] registering the remote device for access to a messaging account using the service activation code;	Little discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22d], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[51c] receiving a message for the messaging account;	Little discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:

’619 Patent – Claim 51	Little
	See [22e], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[51d] encrypting the message using an encryption key; and	Little discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22f], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[51e] sending the message to the remote device,	Little discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22g], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill

'619 Patent – Claim 51	Little
	in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[51f] wherein the device is authenticated to access the messaging account.	Little discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22h], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

'619 Patent – Claim 52	Little
[52] The method of claim 51, wherein a control message is received from the remote device upon user interaction with the message.	Little discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [36], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person

’619 Patent – Claim 52	Little
	of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

EXHIBIT 619-A07

Invalidity Contentions for U.S. Patent No. 10,027,619 ("the '619 patent")

Based on: International Patent Application Pub. No. WO 02/25890 to Hind et al. ("Hind")

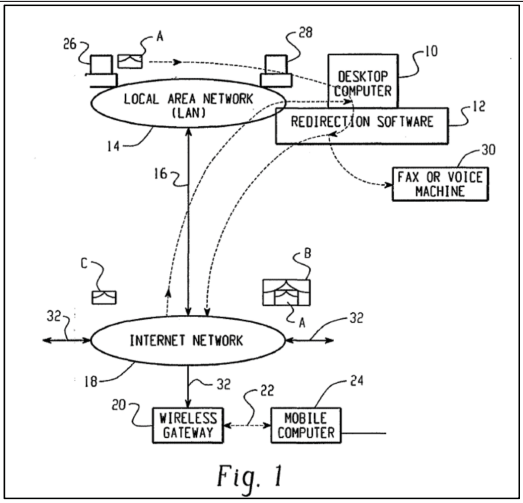
Based on SEVEN's apparent positions as to the scope of the patent's claims, as best they can be deciphered, the reference(s) charted below anticipate(s) or at least render(s) obvious the identified claims. The portions of the prior art reference cited below are not exhaustive but are exemplary in nature. Where Apple identifies a portion of the prior art reference's text, the identification should be understood as referencing any corresponding figure or diagram, and vice versa.

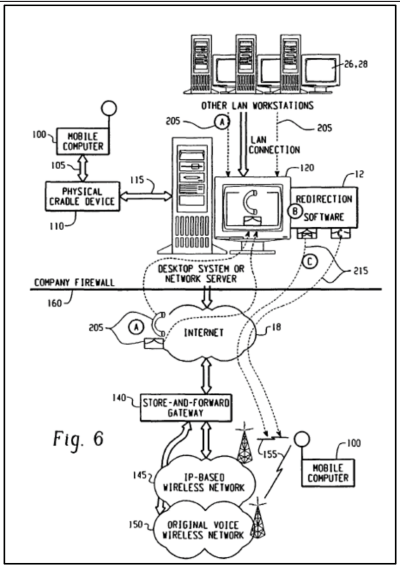
This disclosure is not an admission that Apple concedes any claim construction implied or suggested by SEVEN's apparent positions as to the scope of the patent's claims, nor is it an admission by Apple that any of its products are covered by or infringe the patent's claims, particularly when they are properly construed and applied. Apple is not taking any claim construction positions through this disclosure, including whether the preamble is a limitation.

Apple reserves the right to rely on additional citations or sources of evidence that also may be applicable, or that may become applicable in light of claim construction, changes in SEVEN's infringement contentions, and/or information obtained during discovery as the case progresses. Apple further reserves the right to amend or supplement this claim chart at a later date as more fully set forth in the Invalidity Contentions.

Hind qualifies as prior art under at least pre-AIA 35 U.S.C. §§ 102(a), (b) and/or (e). Hind is an International Patent Application that was filed on August 29, 2001 and published on March 28, 2002.

'619 Patent – Claim 22	Hind
[22pre] A device comprising:	To the extent the preamble is limiting, Hind discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:

’619 Patent – Claim 22	Hind
	 *Fig. 1* Hind, Fig. 1.

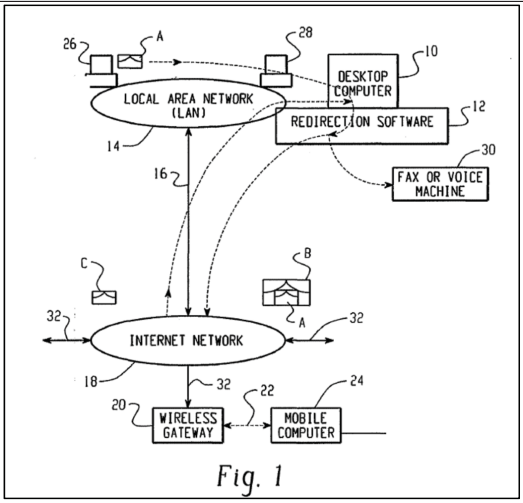
’619 Patent – Claim 22	Hind
	 Fig. 6 Hind, Fig. 2. “DETAILED DESCRIPTION OF THE DRAWINGS Referring now to the drawings, FIG. 1 is an example system diagram showing the redirection of user data items (such as message A or C) from a user's office PC (host system) 10 to the user's mobile data communication device 24, where the redirector software 12 is operating at the user's PC. Message A in FIG. 1 represents an internal message sent from desktop 26 to the user's host system 10 via LAN 14. Message C in FIG. 1 represents an external message from a sender that is not directly connected to LAN 14, such as the user's mobile data communication device 24, some other user's mobile device (not shown), or any user connected

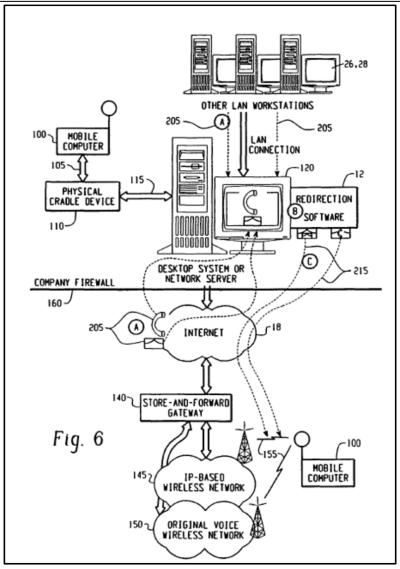
’619 Patent – Claim 22	Hind
	to the internet 18. Message C also represents a command message from the user's mobile data communication device 24 to the host system 10. As described in more detail in FIG. 3, the term "host system" 10 preferably includes, along with the typical hardware and software associated with a workstation or desktop computer, the redirector program 12, a TCP/IP subsystem 42, a primary message store 40, an E-mail subsystem 44, a screen saver subsystem 48, and a keyboard subsystem 46. The E-mail subsystem may be composed of one or more message servers (not necessarily the same type of message server) linked via communication means for the purposes of sending and receiving E-mail between workstations in the LAN, the Internet, and one or more Intranets or other proprietary private networks. In FIG. 1, the host system 10 is the user's desktop system, typically located in the user's office. The host system 10 is connected to a LAN 14, which also connects to other computers 26, 28 that may be in the user's office or elsewhere. The LAN 14, in turn, is connected to a wide area network ("WAN") 18, such as the Internet, which is defined by the use of the Transmission Control Protocol/Internet Protocol ("TCP/IP") to exchange information, but which, alternatively, could be any other type of WAN. The connection of the LAN 14 to the WAN 18 is via high bandwidth link 16, typically a TI or T3 connection. The WAN 18, in turn, is connected to a variety of gateways 20 via connections 32. A gateway forms a connection or bridge between the WAN 18 and some other type of network, such as an RF wireless network, cellular network, satellite network, or other synchronous or asynchronous land-line connection” Hind at 9:18-10:16. “FIG. 1 shows an E-mail message A being communicated over LAN 14 from computer 26 to the user's desktop system 10 (also shown in FIG. 1 is an external message C, which could be an E-mail message from an Internet user, or could be a command message from the user's mobile device 24). Once the message A (or C) reaches the primary message store of the host system 10, it can be detected and acted upon by the redirection software 12. The redirection software 12 can use many methods of detecting new messages. The preferred method of detecting new messages is using a message server like Microsoft's®

’619 Patent – Claim 22	Hind
	Messaging API (MAPI), IMAP4 server or Lotus Notes messaging API, in which programs, such as the redirector program 12, register for notifications or 'advise syncs' when changes to a mailbox take place.” Hind at 16:25-17:8. “Assuming that the redirector program 12 is activated, and has been configured by the user (either through the sensing of an internal, network or external event) to replicate certain user data items (including messages of type A or C) to the mobile device 24, when the message A is received at the host system 10, the redirector program 12 detects its presence and prepares the message for redirection to the mobile device 24. In preparing the message for redirection, the redirector program 12 could compress the original message A, could compress the message header, or could encrypt the entire message A to create a secure link to the mobile device 24.” Hind at 16:9-17. “Also exchanged between the mobile device and the redirector 12 is a personal identification number (PIN) of the user's mobile device 24 such that the redirector 12 associates the mailbox of the user with a PIN. The PIN value could be selected by the manfacturer of the mobile device 24 and programmed into the mobile device 24. Alternatively, this PIN could be a network identifier such as MSISDN, or another value associated with the Subscriber Identity Module (SIM) such as the LMSI. This PIN will be processed by the store-and-forward gateway as it maps the PIN of the mobile device 24 to the currently assigned IP address. Other values that could be saved by the redirector program 12 could include: the type of device, and whether the device 24 can accept certain types of attachments, such as word processing or voice attachments. If the. user's type of mobile device cannot accept these types of attachments, then the redirector 12 can be programmed to route the attachments to a fax or voice number where the user is located using an attached fax or voice machine 30.” Hind at 16:18-31. “FIG. 6 is a system diagram showing the basic components of an IP based wireless data network, such as the GPRS network, for use with the present

’619 Patent – Claim 22	Hind
	invention. In the case of FIG. 6, the mobile device 100 (also referenced as mobile device 24 in earlier figures) is shown as being in communication with the host system 120, via a short-range RF communication link, a serial link, or any other suitable connection 105. When the mobile device is communicating to the host via connection 115, it is said to be 'docked' with the host system 120 for the purposes of this description. Preferably the mobile device 100 communicates with a wireless packet data network 145 when not "docked," and may also be capable of communicating with a voice wireless network 150. The voice network 150 may be associated with the IP based wireless network 145, or it could be a completely separate network. A mobile device 100 that can communicate via networks 145 and 150 is referred to herein as a dual-mode device. The invention, however, is applicable to single-mode devices and other multi-mode devices, not just dual-mode devices. Although depicted as separate networks, the IP based wireless network 145 and the voice wireless network 150 are not necessarily mutually exclusive, and could be operating simultaneously with the same network hardware, i.e., they may be part of a single dual-mode network. In one embodiment, when a serial docking cradle 110 is used as a means of docking or undocking the mobile device 100, the serial docking cradle preferably has the ability to inform the redirector program 12 when the mobile device 100 is not in the cradle and therefore should be reached by the LP based wireless network 145. Preferably, only when the mobile device 100 is in the serial cradle 110, and behind the company's firewall 160, can it exchange shared secrets such as encryption keys, with the user's host system 120. Advantageously, these shared secrets can then be used by the redirection system to encrypt all data items being exchanged over the network 145. The redirector program 12 may also have the ability to compress information that is redirected to the mobile device 100, and thus increase data transfer rates through any delivery mechanism that is used. The redirector program 12 may also connect to a wide range of other devices, such as home or office alarm systems, personal monitoring equipment, such as a vital sign monitor, motion detectors, Internet web sites, e-mail message stores, PBX information storage, customer databases, proprietary software applications,

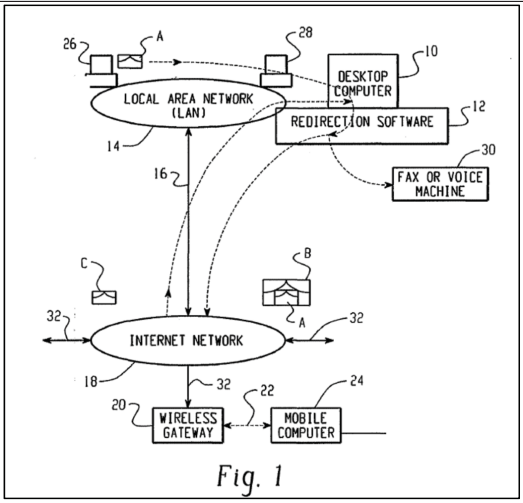
’619 Patent – Claim 22	Hind
	Intranet-based data stores and other information sources, for the purpose of collecting information to redirect to the mobile device 100.” Hind at 29:13-30:18. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[22a] a radio;	Hind discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:

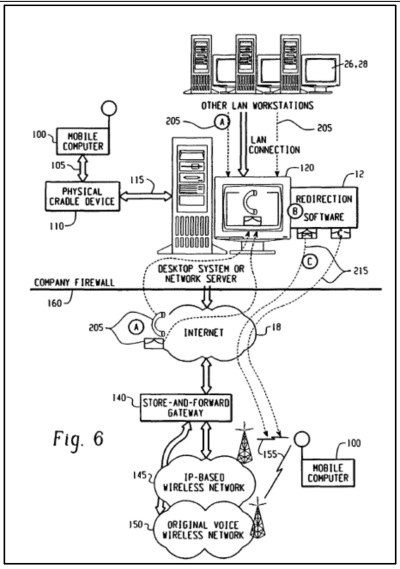
’619 Patent – Claim 22	Hind
	 *Fig. 1* Hind, Fig. 1.

’619 Patent – Claim 22	Hind
	 Fig. 6 Hind, Fig. 2. “For example, a device 24 destined for a North American market may include a communication subsystem 1911 designed to operate within the Mobitex™ mobile communication system or the DataTAC™ mobile communication system, whereas a device 24 intended for use in Europe may incorporate a General Packet Radio Service (GPRS) communication subsystem 1911.” Hind at 12:2-7. “The term IP based wireless network includes, but is not limited to (1) the Code Division Multiple Access (CDMA) network that has been developed and operated by Qualcomm, (2) the General Packet Radio Service (GPRS) for use

’619 Patent – Claim 22	Hind
	in conjunction with the Global System for Mobile Communications (GSM) network both developed by the standards committee of CEPT, and (3) future third- generation (3G) networks like EDGE and UMTS. GPRS is a data communications overlay on top of the GSM wireless network. It is to be understood that although an IP based wireless network is shown in FIG. 6, the present invention could be utilized with other types of wireless packet data network.” Hind at 32:3-12. “FIG. 6 is a system diagram showing the basic components of an IP based wireless data network, such as the GPRS network, for use with the present invention. In the case of FIG. 6, the mobile device 100 (also referenced as mobile device 24 in earlier figures) is shown as being in communication with the host system 120, via a short-range RF communication link, a serial link, or any other suitable connection 105. When the mobile device is communicating to the host via connection 115, it is said to be 'docked' with the host system 120 for the purposes of this description. Preferably the mobile device 100 communicates with a wireless packet data network 145 when not "docked," and may also be capable of communicating with a voice wireless network 150. The voice network 150 may be associated with the IP based wireless network 145, or it could be a completely separate network. A mobile device 100 that can communicate via networks 145 and 150 is referred to herein as a dual-mode device. The invention, however, is applicable to single-mode devices and other multi-mode devices, not just dual-mode devices. Although depicted as separate networks, the IP based wireless network 145 and the voice wireless network 150 are not necessarily mutually exclusive, and could be operating simultaneously with the same network hardware, i.e., they may be part of a single dual-mode network.” Hind at 29:13-31. “The mobile device cradle component 110 provides a communication node (or a physical serial link 105) for the mobile device 100 that allows the user to dock the mobile device 100 when the user is in their office. Alternatively, connection 105 could be a wireless connection, such as a short-range RF

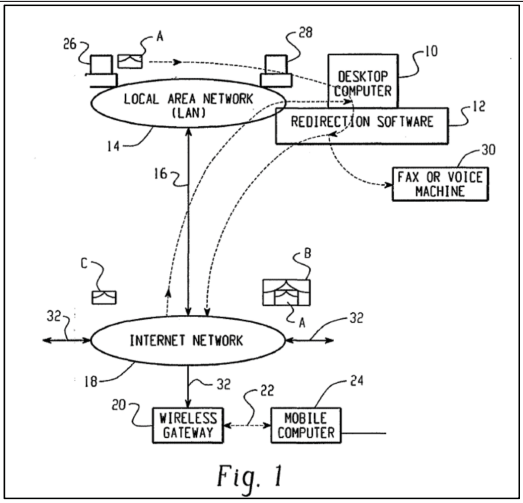
'619 Patent – Claim 22	Hind
	connection. This docking procedure is one method for exchanging bulk personal information locally (versus over a wireless communication network), such as, but not limited to, e-mail messages, calendar events, contacts, notes, and security information like encryption keys." Hind at 30:29-31:4. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[22b] a processor and memory containing instructions executable by the processor whereby the device is operable to:	Hind discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:

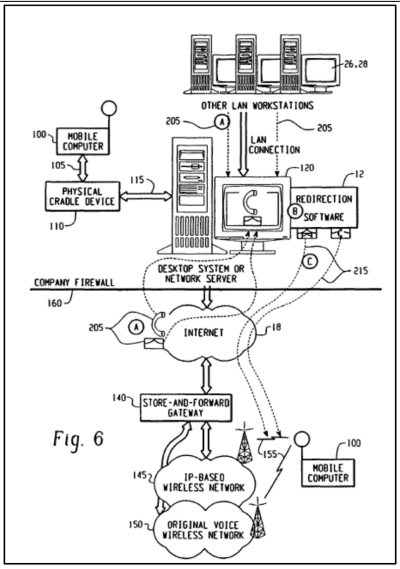
’619 Patent – Claim 22	Hind
	 *Fig. 1* Hind, Fig. 1.

’619 Patent – Claim 22	Hind
	 Fig. 6 Hind, Fig. 2. “Although it is preferable for the system to operate in a two-way communications mode, certain aspects of the invention could be beneficially used in a "one and one-half or acknowledgment paging environment, or even with a one-way paging system. The mobile data communication device 24 includes software program instructions that work in conjunction with the redirector program 12 to enable the seamless, transparent redirection of user-selected data items. FIG. 4 describes the basic method steps of the redirector program 12, and FIG. 5 describes the steps of the corresponding program operating at the mobile device 24.” Hind at 11:10-18.

’619 Patent – Claim 22	Hind
	“The desktop system 10 is connected to LAN 14, and can send and receive data, messages, signals, event triggers, etc., to and from other systems connected to the LAN 14 and to external networks 18, 22, such as the Internet or a wireless data network, which are also coupled to the LAN 14. hi addition to the standard hardware, operating system, and application programs associated with a typical microcomputer or workstation, the desktop system 10 includes the redirector program 12, a TCP/IP sub-system 42, an E-mail sub-system 44, a primary data storage device 40, a screen saver sub-system 48, and a keyboard sub-system 46. The TCP/IP and E-mail subsystems 42, 44 are examples of repackaging systems that can be used to achieve the transparency of the present invention, and the screen saver and keyboard sub-systems 46, 48 are examples of event generating systems that can be configured to generate event messages or signals that trigger redirection of the user selected data items. The method steps carried out by the redirector program 12 are described in more detail in FIG. 4. The basic functions of this program are: (1) configure and setup the user-defined event trigger points that will start redirection; (2) configure the types of user data items for redirection and optionally configure a preferred list of senders whose messages are to be redirected; (3) configure the type and capabilities of the user's mobile data communication device; (4) receive messages and signals from the repackaging systems and the event generating systems; and (5) command and control the redirection of the user-selected data items to the mobile data communication device via the repackaging systems. Other functions not specifically enumerated could also be integrated into this program.” Hind at 21:22-22:13. “Functionally, the redirector program 12 provides the user with the ability to configure the screen saver and keyboard systems so that under certain conditions a event trigger will be generated that can be detected by the redirector 12 to start the redirection process. For example, the screen saver system can be configured so that when the screen saver is activated, after, for example, 10 minutes of inactivity on the desktop system, an event trigger is transmitted to the redirector 12, which starts redirecting the previously selected

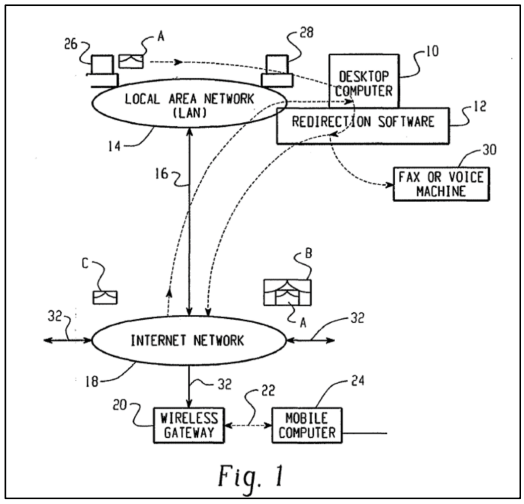
'619 Patent – Claim 22	Hind
	user data items. In a similar manner the keyboard sub-system can be configured to generate event triggers when no key has been depressed for a particular period of time, thus indicating that redirection should commence. These are just two examples of the numerous application programs and hardware systems internal to the host system 10 that can be used to generate internal event triggers. FIGs. 4 and 5, set forth, respectively, flow charts showing the steps carried out by the redirector software 12 operating at the host system 10, and the steps carried out by the mobile data communication device 24 in order to interface with the host system. Turning first to FIG. 4, at step 50, the redirector program 12 is started and initially configured." Hind at 23:17-24:2. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[22c] optically receive information including a displayed service activation code from a remote device;	Hind discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:

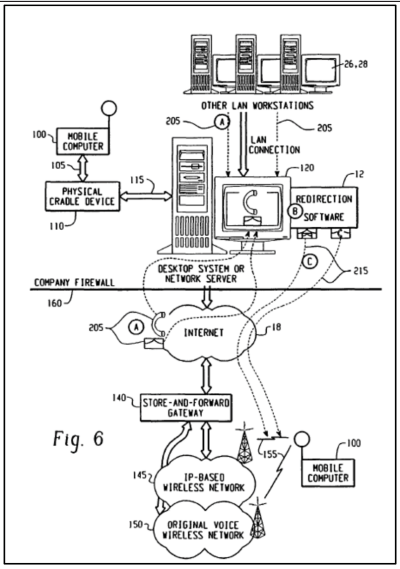
’619 Patent – Claim 22	Hind
	 *Fig. 1* Hind, Fig. 1.

’619 Patent – Claim 22	Hind
	 Fig. 6 Hind, Fig. 2. “FIG. 6 is a system diagram showing the basic components of an IP based wireless data network, such as the GPRS network, for use with the present invention. In the case of FIG. 6, the mobile device 100 (also referenced as mobile device 24 in earlier figures) is shown as being in communication with the host system 120, via a short-range RF communication link, a serial link, or any other suitable connection 105. When the mobile device is communicating to the host via connection 115, it is said to be 'docked' with the host system 120 for the purposes of this description. Preferably the mobile device 100 communicates with a wireless packet data network 145 when not "docked," and

’619 Patent – Claim 22	Hind
	may also be capable of communicating with a voice wireless network 150. The voice network 150 may be associated with the IP based wireless network 145, or it could be a completely separate network. A mobile device 100 that can communicate via networks 145 and 150 is referred to herein as a dual-mode device. The invention, however, is applicable to single-mode devices and other multi-mode devices, not just dual-mode devices. Although depicted as separate networks, the IP based wireless network 145 and the voice wireless network 150 are not necessarily mutually exclusive, and could be operating simultaneously with the same network hardware, i.e., they may be part of a single dual-mode network. In one embodiment, when a serial docking cradle 110 is used as a means of docking or undocking the mobile device 100, the serial docking cradle preferably has the ability to inform the redirector program 12 when the mobile device 100 is not in the cradle and therefore should be reached by the IP based wireless network 145.” Hind at 29:13-30:5. “Also exchanged between the mobile device and the redirector 12 is a personal identification number (PIN) of the user's mobile device 24 such that the redirector 12 associates the mailbox of the user with a PIN. The PIN value could be selected by the manfacturer of the mobile device 24 and programmed into the mobile device 24. Alternatively, this PIN could be a network identifier such as MSISDN, or another value associated with the Subscriber Identity Module (SIM) such as the LMSI. This PIN will be processed by the store-and-forward gateway as it maps the PIN of the mobile device 24 to the currently assigned IP address. Other values that could be saved by the redirector program 12 could include: the type of device, and whether the device 24 can accept certain types of attachments, such as word processing or voice attachments. If the. user's type of mobile device cannot accept these types of attachments, then the redirector 12 can be programmed to route the attachments to a fax or voice number where the user is located using an attached fax or voice machine 30.” Hind at 17:17-31. “Network access requirements will also vary depending upon the type of

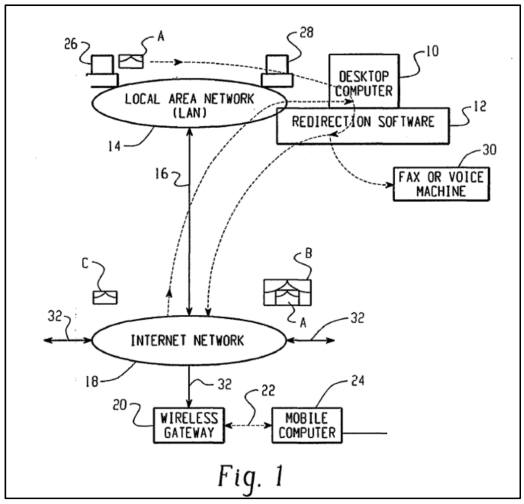
'619 Patent – Claim 22	Hind
	network 1919. For example, in the Mobitex and DataTAC networks, mobile devices 24 are registered on the network using a unique personal identification number or PIN associated with each device. In GPRS networks, however, network access is associated with a subscriber or user of a device 24." Hind at 12:8-12. "A short-range communications subsystem 1940 is a further optional component, which may provide for communication between the device 1924 and different systems or devices, which need not necessarily be similar devices. For example, the subsystem 1940 may include an infrared device and associated circuits and components or a Bluetooth™ communication module to provide for communication with similarly-enabled systems and devices." Hind at 15:14-19. "Alternatively, connection 105 could be a wireless connection, such as a short-range RF connection. This docking procedure is one method for exchanging bulk personal information locally (versus over a wireless communication network), such as, but not limited to, e-mail messages, calendar events, contacts, notes, and security information like encryption keys. The host system/redirector program 120/12 are also coupled to an external network 18, such as the Internet. The external network 18 could be the Internet, a company Intranet, and Extranet, a private network like an America On Line ("AOL™") network, a LAN, or some other network capable of exchanging information. The connection between the host system 120 and this external network 18 could use a range of existing technologies, such as Ethernet, Cable Modem, DSL, ISDN, or Frame Relay." Hind at 30:31-31:-11. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable

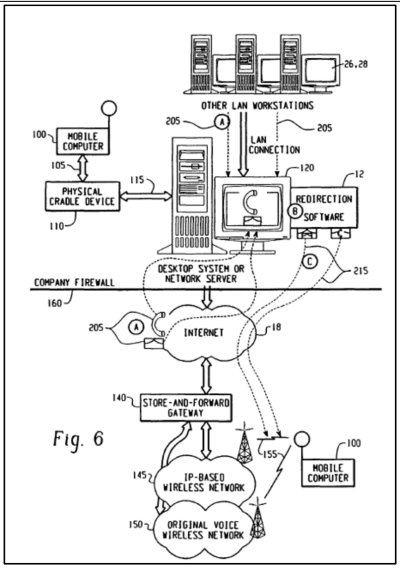
’619 Patent – Claim 22	Hind
	solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[22d] register the remote device for access to a messaging account using the service activation code;	Hind discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:  Fig. 1 Hind, Fig. 1.

’619 Patent – Claim 22	Hind
	 Fig. 6 Hind, Fig. 2. “Also exchanged between the mobile device and the redirector 12 is a personal identification number (PIN) of the user's mobile device 24 such that the redirector 12 associates the mailbox of the user with a PIN. The PIN value could be selected by the manfacturer of the mobile device 24 and programmed into the mobile device 24. Alternatively, this PIN could be a network identifier such as MSISDN, or another value associated with the Subscriber Identity Module (SIM) such as the LMSI. This PIN will be processed by the store-and-forward gateway as it maps the PIN of the mobile device 24 to the currently

’619 Patent – Claim 22	Hind
	assigned IP address. Other values that could be saved by the redirector program 12 could include: the type of device, and whether the device 24 can accept certain types of attachments, such as word processing or voice attachments. If the. user's type of mobile device cannot accept these types of attachments, then the redirector 12 can be programmed to route the attachments to a fax or voice number where the user is located using an attached fax or voice machine 30.” Hind at 17:17-31. “Network access requirements will also vary depending upon the type of network 1919. For example, in the Mobitex and DataTAC networks, mobile devices 24 are registered on the network using a unique personal identification number or PIN associated with each device. In GPRS networks, however, network access is associated with a subscriber or user of a device 24.” Hind at 12:8-12. “Assuming that the redirector program 12 is activated, and has been configured by the user (either through the sensing of an internal, network or external event) to replicate certain user data items (including messages of type A or C) to the mobile device 24, when the message A is received at the host system 10, the redirector program 12 detects its presence and prepares the message for redirection to the mobile device 24. In preparing the message for redirection, the redirector program 12 could compress the original message A, could compress the message header, or could encrypt the entire message A to create a secure link to the mobile device 24.” Hind at 17:9-17. “The redirection program could be configured to send the text of the E-mail to the mobile device, to send the word processing document to a networked printer located near the user, to send the video clip to a store accessible through a secure connection through the Internet, and to send the audio clip to the user's voice mail system.” Hind at 10:32-11:4. “Using the redirector program, the user can select certain data items for redirection, such as E-mail messages, calendar events, meeting notifications,

’619 Patent – Claim 22	Hind
	address entries, journal entries, personal reminders, etc. Having selected the data items for redirection, the user can then configure one or more event triggers, which are sensed by the redirector program to initiate redirection of the user's data items. These user-defined triggers (or event triggers) may include external events, internal events and networked events. Examples of external events include: receiving a message from the user's mobile data communication device to begin redirection; receiving a similar message from some external computer; sensing that the user is no longer in the vicmity of the host system; or any other event that is external to the host system. Internal events could be a calendar alarm, screen saver activation, keyboard timeout, programmable timer, or any other user-defined event that is internal to the host system. Networked events are user-defined messages that are transmitted to the host system from another computer coupled to the host system via a network to initiate redirection.” Hind at 5:21-6:3. “A user of the present invention can configure the redirector program 12 to push certain user-selected data items to the user's mobile device 24 when the redirector 12 detects that a particular user-defined event trigger (or trigger point) has taken place. User-selected data items preferably include E-mail messages, calendar events, meeting notifications, address entries, journal entries, personal alerts, alarms, warnings, stock quotes, news bulletins, corporate data (from an Intranet or from behind the corporate firewall), etc., but could, alternatively, include any other type of message that is transmitted to the host system 10, or that the host system 10 acquires through the use of intelligent agents, such as data that is received after the host system 10 initiates a search of a database or a website or a bulletin board.” Hind at 15:25-16:3. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable

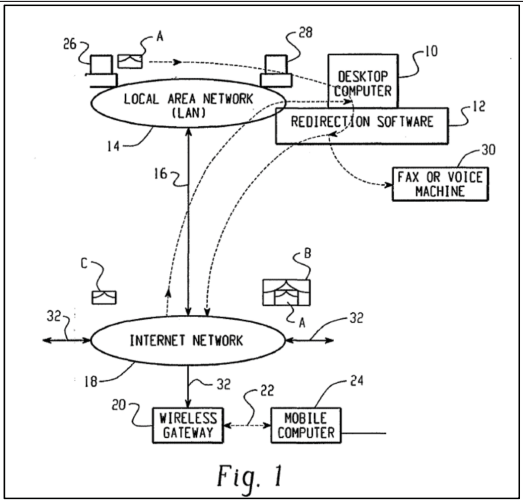
’619 Patent – Claim 22	Hind
	solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[22e] receive a message for the messaging account;	Hind discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:  Fig. 1 Hind, Fig. 1.

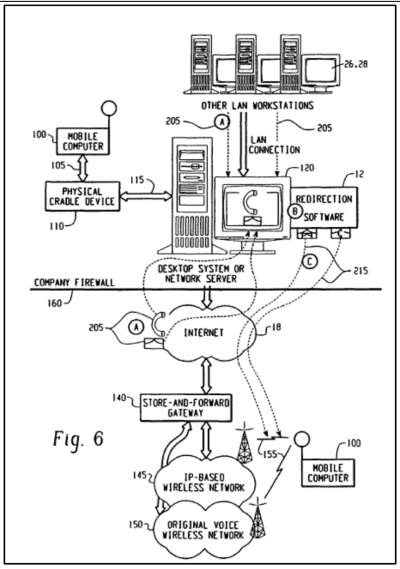
’619 Patent – Claim 22	Hind
	 Hind, Fig. 2. “FIG. 1 shows an E-mail message A being communicated over LAN 14 from computer 26 to the user's desktop system 10 (also shown in FIG. 1 is an external message C, which could be an E-mail message from an Internet user, or could be a command message from the user's mobile device 24). Once the message A (or C) reaches the primary message store of the host system 10, it can be detected and acted upon by the redirection software 12. The redirection software 12 can use many methods of detecting new messages. The preferred method of detecting new messages is using a message server like Microsoft's®

’619 Patent – Claim 22	Hind
	Messaging API (MAPI), IMAP4 server or Lotus Notes messaging API, in which programs, such as the redirector program 12, register for notifications or 'advise syncs' when changes to a mailbox take place. Other methods of detecting new messages could also be used with the present invention. This tight integration between the redirection program 12 and a messaging server effectively means the two programs are co-operating to provide a wireless extension to an existing messaging product. In another embodiment, the redirection program is an embedded component of the message server.” Hind at 16:25-17:8. “Assuming that the redirector program 12 is activated, and has been configured by the user (either through the sensing of an internal, network or external event) to replicate certain user data items (including messages of type A or C) to the mobile device 24, when the message A is received at the host system 10, the redirector program 12 detects its presence and prepares the message for redirection to the mobile device 24. In preparing the message for redirection, the redirector program 12 could compress the original message A, could compress the message header, or could encrypt the entire message A to create a secure link to the mobile device 24.” Hind at 17:9-17. “Using the redirector program, the user can select certain data items for redirection, such as E-mail messages, calendar events, meeting notifications, address entries, journal entries, personal reminders, etc. Having selected the data items for redirection, the user can then configure one or more event triggers, which are sensed by the redirector program to initiate redirection of the user's data items. These user-defined triggers (or event triggers) may include external events, internal events and networked events. Examples of external events include: receiving a message from the user's mobile data communication device to begin redirection; receiving a similar message from some external computer; sensing that the user is no longer in the vicmity of the host system; or any other event that is external to the host system. Internal events could be a calendar alarm, screen saver activation, keyboard timeout,

’619 Patent – Claim 22	Hind
	programmable timer, or any other user-defined event that is internal to the host system. Networked events are user-defined messages that are transmitted to the host system from another computer coupled to the host system via a network to initiate redirection.” Hind at 5:21-6:3. “After the redirector has determined that a particular message should be redirected, and it has prepared the message for redirection, the software 12 then sends the message A to a secondary memory store located in the mobile device 24, using whatever means are necessary. In the preferred embodiment this method is to send the message A back over the LAN 14, WAN 18, and through the store-and-forward gateway 20 to the mobile data commumcation device 24. In doing so, the redirector preferably repackages message A as an E-mail with an outer envelope B that contains the addressing information of the mobile device 24, although alternative repackaging techniques and protocols could be used, such as a TCP/IP repackaging and delivery method (most commonly used in the alternative server configuration shown in FIG. 2). The wireless gateway 20 requires this outer envelope information B in order to know where to send the redirected message A. Once the message (A in B) is received by the mobile device 24, the outer envelope B is removed and the original message A is placed in the secondary memory store within the mobile device 24. By repackaging and removing the outer envelope in this manner, the present invention causes the mobile computer 24 to appear to be at the same physical location as the host system 10, thus creating a transparent system.” Hind at 18:25-19:10. “A user of the present invention can configure the redirector program 12 to push certain user-selected data items to the user's mobile device 24 when the redirector 12 detects that a particular user-defined event trigger (or trigger point) has taken place. User-selected data items preferably include E-mail messages, calendar events, meeting notifications, address entries, journal entries, personal alerts, alarms, warnings, stock quotes, news bulletins, corporate data (from an Intranet or from behind the corporate firewall), etc., but

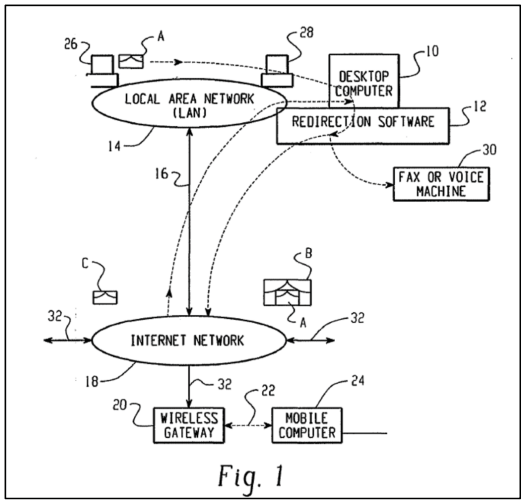
’619 Patent – Claim 22	Hind
	could, alternatively, include any other type of message that is transmitted to the host system 10, or that the host system 10 acquires through the use of intelligent agents, such as data that is received after the host system 10 initiates a search of a database or a website or a bulletin board.” Hind at 15:25-16:3. “As described above, the present invention preferably provides a redirection computer program ("redirector program") 12, operating within (or in conjunction with) the host system 120, behind a corporate firewall 160. Preferably in conjunction with a message server or some other hardware or software mechanism, the redirector 12 senses that a particular event has occurred, and redirects user-selected data items from the host system 120 to the user's mobile device 100. In one embodiment, the redirector program 12 also interfaces to a mobile device cradle component 110, over a serial connection 115, or some other suitable computer communication method, so that the redirector program 12 can detect the physical location, as well as other information, of the mobile device 100.” Hind at 30:19-31:4. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[22f] encrypt the message using an encryption key; and	Hind discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:

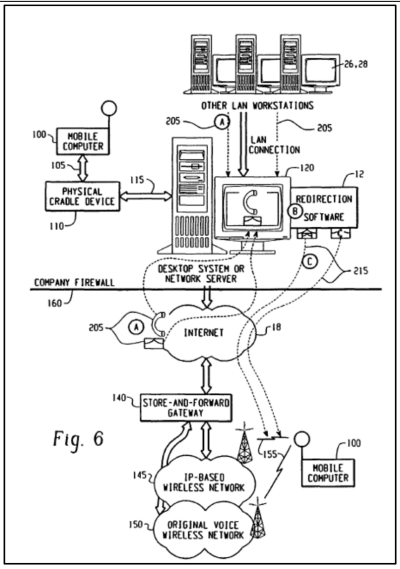
’619 Patent – Claim 22	Hind
	 *Fig. 1* Hind, Fig. 1.

’619 Patent – Claim 22	Hind
	 Fig. 6 Hind, Fig. 2. “Assuming that the redirector program 12 is activated, and has been configured by the user (either through the sensing of an internal, network or external event) to replicate certain user data items (including messages of type A or C) to the mobile device 24, when the message A is received at the host system 10, the redirector program 12 detects its presence and prepares the message for redirection to the mobile device 24. In preparing the message for redirection, the redirector program 12 could compress the original message A, could compress the message header, or could encrypt the entire message A to create a secure link to the mobile device 24.” Hind at 17:9-17.

’619 Patent – Claim 22	Hind
	“Once an event has triggered redirection of the user data items, the host system repackages these items in a manner that is transparent to the mobile data communication device, so that the data at the mobile device appears similar to the same data at the user's host system. The preferred repackaging method includes wrapping the user data items in an E-mail envelope that corresponds to the address of the mobile data communication device, although, alternatively, other repackaging methods could be used with the present invention, such as special- purpose TCP/IP wrapping techniques, or other methods of wrapping the user selected data items. The repackaging method preferably results in a shared E- mail address for the user's host system and the user's mobile device. To a recipient of an E-mail generated at either the host or the mobile device, it appears as though the E-mail was generated at the host system. The repackaging method also provides encryption/decryption and compression/decompression.” Hind at 6:28-7:8. “The alternate download path may, for example, be used to load an encryption key onto the device through a direct and thus reliable and trusted connection to thereby enable secure device communication.” Hind at 15:10-13. “If the system includes encryption keys, these too can be kept at one place for management and update purposes.” Hind at 20:12-13. “Preferably, only when the mobile device 100 is in the serial cradle 110, and behind the company's firewall 160, can it exchange shared secrets such as encryption keys, with the user's host system 120. Advantageously, these shared secrets can then be used by the redirection system to encrypt all data items being exchanged over the network 145. The redirector program 12 may also have the ability to compress information that is redirected to the mobile device 100, and thus increase data transfer rates through any delivery mechanism that is used.” Hind at 30:5-12.

’619 Patent – Claim 22	Hind
	“Alternatively, connection 105 could be a wireless connection, such as a short-range RF connection. This docking procedure is one method for exchanging bulk personal information locally (versus over a wireless communication network), such as, but not limited to, e-mail messages, calendar events, contacts, notes, and security information like encryption keys.” Hind at 30:31-31:4. “The network entry point 305 then uses an address assignment component, i.e. like DHCP 335 to allocate an IP address for the mobile device 100. Having allocated an IP address to the device 100 and communicated this information to the gateway 140, information, such as the stored data items, can then be sent from the store-and-forward gateway 140 to the mobile device 100 via the wireless network tunnel 325. In addition, as data items are received from the host system, these data items can be addressed with the IP address now associated with the mobile and immediately sent to the mobile without undue delay, thereby allowing a seamless and continuous pushing of the data items from the host to the mobile as they arrive temporarily at the store and forward gateway. The presence of the wireless tunnel provides the redirector program with a continuous, uninterrupted secure communication link between the host system, located behind the corporate firewall, and the mobile device 100. Through this secure communication link the redirector program delivers secure, encrypted messages that cannot be viewed by any intermediate component or node, only the mobile device user.” Hind at 36:13-28. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and

’619 Patent – Claim 22	Hind
	Exhibit 619-B.
[22g] send the message to the remote device,	Hind discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:  *Fig. 1* Hind, Fig. 1.

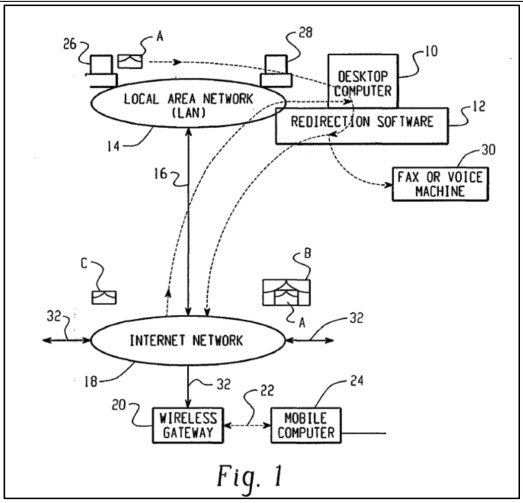
’619 Patent – Claim 22	Hind
	 Fig. 6 Hind, Fig. 2. “FIG. 1 shows an E-mail message A being communicated over LAN 14 from computer 26 to the user's desktop system 10 (also shown in FIG. 1 is an external message C, which could be an E-mail message from an Internet user, or could be a command message from the user's mobile device 24). Once the message A (or C) reaches the primary message store of the host system 10, it can be detected and acted upon by the redirection software 12. The redirection software 12 can use many methods of detecting new messages. The preferred method of detecting new messages is using a message server like Microsoft's® Messaging API (MAPI), IMAP4 server or Lotus Notes messaging API, in

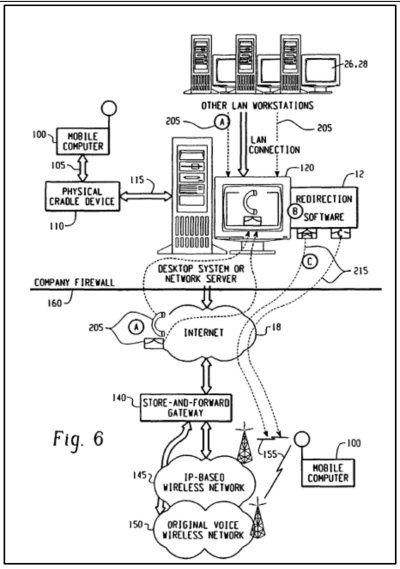
’619 Patent – Claim 22	Hind
	which programs, such as the redirector program 12, register for notifications or 'advise syncs' when changes to a mailbox take place. Other methods of detecting new messages could also be used with the present invention. This tight integration between the redirection program 12 and a messaging server effectively means the two programs are co-operating to provide a wireless extension to an existing messaging product. In another embodiment, the redirection program is an embedded component of the message server.” Hind at 16:25-17:8. “Assuming that the redirector program 12 is activated, and has been configured by the user (either through the sensing of an internal, network or external event) to replicate certain user data items (including messages of type A or C) to the mobile device 24, when the message A is received at the host system 10, the redirector program 12 detects its presence and prepares the message for redirection to the mobile device 24. In preparing the message for redirection, the redirector program 12 could compress the original message A, could compress the message header, or could encrypt the entire message A to create a secure link to the mobile device 24.” Hind at 17:9-17. “Using the redirector program, the user can select certain data items for redirection, such as E-mail messages, calendar events, meeting notifications, address entries, journal entries, personal reminders, etc. Having selected the data items for redirection, the user can then configure one or more event triggers, which are sensed by the redirector program to initiate redirection of the user's data items. These user-defined triggers (or event triggers) may include external events, internal events and networked events. Examples of external events include: receiving a message from the user's mobile data communication device to begin redirection; receiving a similar message from some external computer; sensing that the user is no longer in the vicmity of the host system; or any other event that is external to the host system. Internal events could be a calendar alarm, screen saver activation, keyboard timeout, programmable timer, or any other user-defined event that is internal to the host

’619 Patent – Claim 22	Hind
	system. Networked events are user-defined messages that are transmitted to the host system from another computer coupled to the host system via a network to initiate redirection.” Hind at 5:21-6:3. “After the redirector has determined that a particular message should be redirected, and it has prepared the message for redirection, the software 12 then sends the message A to a secondary memory store located in the mobile device 24, using whatever means are necessary. In the preferred embodiment this method is to send the message A back over the LAN 14, WAN 18, and through the store-and-forward gateway 20 to the mobile data commumcation device 24. In doing so, the redirector preferably repackages message A as an E-mail with an outer envelope B that contains the addressing information of the mobile device 24, although alternative repackaging techniques and protocols could be used, such as a TCP/IP repackaging and delivery method (most commonly used in the alternative server configuration shown in FIG. 2). The wireless gateway 20 requires this outer envelope information B in order to know where to send the redirected message A. Once the message (A in B) is received by the mobile device 24, the outer envelope B is removed and the original message A is placed in the secondary memory store within the mobile device 24. By repackaging and removing the outer envelope in this manner, the present invention causes the mobile computer 24 to appear to be at the same physical location as the host system 10, thus creating a transparent system.” Hind at 18:25-19:10. “A user of the present invention can configure the redirector program 12 to push certain user-selected data items to the user's mobile device 24 when the redirector 12 detects that a particular user-defined event trigger (or trigger point) has taken place. User-selected data items preferably include E-mail messages, calendar events, meeting notifications, address entries, journal entries, personal alerts, alarms, warnings, stock quotes, news bulletins, corporate data (from an Intranet or from behind the corporate firewall), etc., but could, alternatively, include any other type of message that is transmitted to the

'619 Patent – Claim 22	Hind
	host system 10, or that the host system 10 acquires through the use of intelligent agents, such as data that is received after the host system 10 initiates a search of a database or a website or a bulletin board." Hind at 15:25-16:3. "Once an event has triggered redirection of the user data items, the host system repackages these items in a manner that is transparent to the mobile data communication device, so that the data at the mobile device appears similar to the same data at the user's host system. The preferred repackaging method includes wrapping the user data items in an E-mail envelope that corresponds to the address of the mobile data communication device, although, alternatively, other repackaging methods could be used with the present invention, such as special- purpose TCP/IP wrapping techniques, or other methods of wrapping the user selected data items. The repackaging method preferably results in a shared E- mail address for the user's host system and the user's mobile device. To a recipient of an E-mail generated at either the host or the mobile device, it appears as though the E-mail was generated at the host system. The repackaging method also provides encryption/decryption and compression/decompression." Hind at 6:28-7:8. "The network entry point 305 then uses an address assignment component, i.e. like DHCP 335 to allocate an IP address for the mobile device 100. Having allocated an IP address to the device 100 and communicated this information to the gateway 140, information, such as the stored data items, can then be sent from the store-and-forward gateway 140 to the mobile device 100 via the wireless network tunnel 325. In addition, as data items are received from the host system, these data items can be addressed with the IP address now associated with the mobile and immediately sent to the mobile without undue delay, thereby allowing a seamless and continuous pushing of the data items from the host to the mobile as they arrive temporarily at the store and forward gateway. The presence of the wireless tunnel provides the redirector program with a continuous, uninterrupted secure communication link between the host

'619 Patent – Claim 22	Hind
	system, located behind the corporate firewall, and the mobile device 100. Through this secure communication link the redirector program delivers secure, encrypted messages that cannot be viewed by any intermediate component or node, only the mobile device user." Hind at 36:13-28. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[22h] wherein the device is authenticated to access the messaging account.	Hind discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:

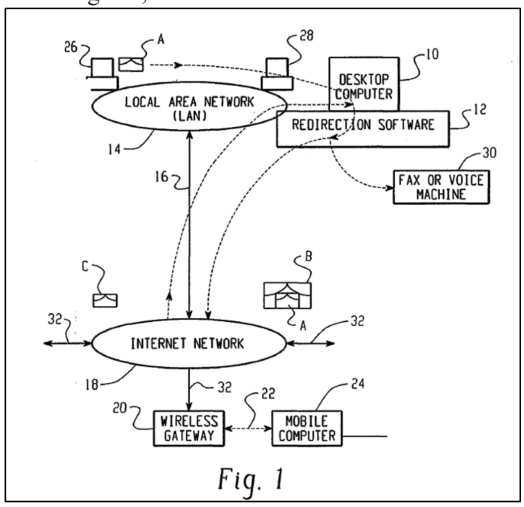
’619 Patent – Claim 22	Hind
	 *Fig. 1* Hind, Fig. 1.

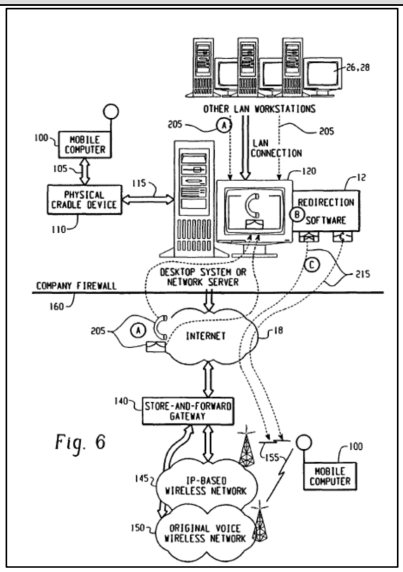
’619 Patent – Claim 22	Hind
	 Hind, Fig. 2. “DETAILED DESCRIPTION OF THE DRAWINGS Referring now to the drawings, FIG. 1 is an example system diagram showing the redirection of user data items (such as message A or C) from a user's office PC (host system) 10 to the user's mobile data communication device 24, where the redirector software 12 is operating at the user's PC. Message A in FIG. 1 represents an internal message sent from desktop 26 to the user's host system 10 via LAN 14. Message C in FIG. 1 represents an external message from a sender that is not directly connected to LAN 14, such as the user's mobile data communication device 24, some other user's mobile device (not shown), or any user connected

’619 Patent – Claim 22	Hind
	to the internet 18. Message C also represents a command message from the user's mobile data communication device 24 to the host system 10. As described in more detail in FIG. 3, the term "host system" 10 preferably includes, along with the typical hardware and software associated with a workstation or desktop computer, the redirector program 12, a TCP/IP subsystem 42, a primary message store 40, an E-mail subsystem 44, a screen saver subsystem 48, and a keyboard subsystem 46. The E-mail subsystem may be composed of one or more message servers (not necessarily the same type of message server) linked via communication means for the purposes of sending and receiving E-mail between workstations in the LAN, the Internet, and one or more Intranets or other proprietary private networks. In FIG. 1, the host system 10 is the user's desktop system, typically located in the user's office. The host system 10 is connected to a LAN 14, which also connects to other computers 26, 28 that may be in the user's office or elsewhere. The LAN 14, in turn, is connected to a wide area network ("WAN") 18, such as the Internet, which is defined by the use of the Transmission Control Protocol/Internet Protocol ("TCP/IP") to exchange information, but which, alternatively, could be any other type of WAN. The connection of the LAN 14 to the WAN 18 is via high bandwidth link 16, typically a TI or T3 connection. The WAN 18, in turn, is connected to a variety of gateways 20 via connections 32. A gateway forms a connection or bridge between the WAN 18 and some other type of network, such as an RF wireless network, cellular network, satellite network, or other synchronous or asynchronous land-line connection” Hind at 9:18-10:16. “FIG. 1 shows an E-mail message A being communicated over LAN 14 from computer 26 to the user's desktop system 10 (also shown in FIG. 1 is an external message C, which could be an E-mail message from an Internet user, or could be a command message from the user's mobile device 24). Once the message A (or C) reaches the primary message store of the host system 10, it can be detected and acted upon by the redirection software 12. The redirection software 12 can use many methods of detecting new messages. The preferred method of detecting new messages is using a message server like Microsoft's®

’619 Patent – Claim 22	Hind
	Messaging API (MAPI), IMAP4 server or Lotus Notes messaging API, in which programs, such as the redirector program 12, register for notifications or 'advise syncs' when changes to a mailbox take place.” Hind at 16:25-17:8. “Assuming that the redirector program 12 is activated, and has been configured by the user (either through the sensing of an internal, network or external event) to replicate certain user data items (including messages of type A or C) to the mobile device 24, when the message A is received at the host system 10, the redirector program 12 detects its presence and prepares the message for redirection to the mobile device 24. In preparing the message for redirection, the redirector program 12 could compress the original message A, could compress the message header, or could encrypt the entire message A to create a secure link to the mobile device 24.” Hind at 16:9-17. “As described above, the redirector program 12 executing at the host system then strips the outer envelope and routes the reply message to the appropriate destination address using the address of the user's e-mail account associated with the host system as the "from" field, so that to the recipient of the redirected message, it appears as though it originated from the user's host system rather than the mobile device. In an alternative embodiment a tag or signature line is added to the message (at either the device or the host system) to indicate that it has been sent from a mobile device 24 whilst the mobile device and host system continue to share a common single email address. This integrated common email address provides the host system (desktop or server system) with seamless wireless connectivity to the mobile device.” Hind at 27:24-28:3. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable

’619 Patent – Claim 22	Hind
	solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

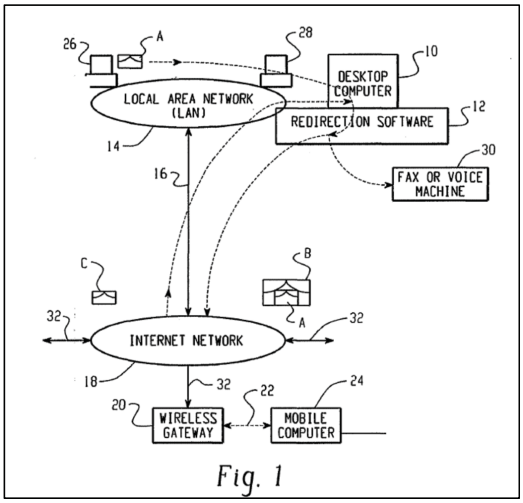
’619 Patent – Claim 23	Hind
[23] The device of claim 22, wherein the information including the service activation code is received by the device in response to user input at the remote device.	Hind discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:  *Fig. 1* Hind, Fig. 1.

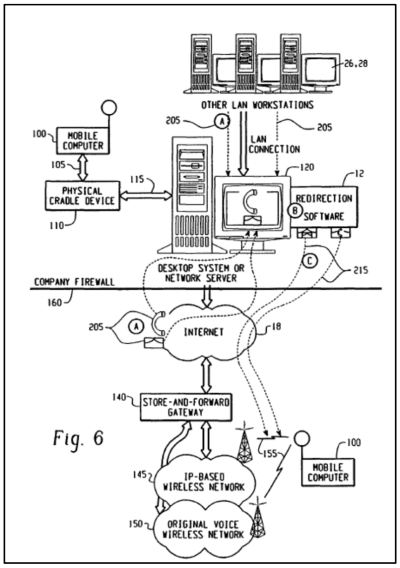
’619 Patent – Claim 23	Hind
	 Hind, Fig. 2. “Also exchanged between the mobile device and the redirector 12 is a personal identification number (PIN) of the user's mobile device 24 such that the redirector 12 associates the mailbox of the user with a PIN. The PIN value could be selected by the manfacturer of the mobile device 24 and programmed into the mobile device 24. Alternatively, this PIN could be a network identifier such as MSISDN, or another value associated with the Subscriber Identity Module (SIM) such as the LMSI. This PIN will be processed by the store-and-forward gateway as it maps the PIN of the mobile device 24 to the currently assigned IP address. Other values that could be saved by the redirector program

’619 Patent – Claim 23	Hind
	12 could include: the type of device, and whether the device 24 can accept certain types of attachments, such as word processing or voice attachments. If the. user's type of mobile device cannot accept these types of attachments, then the redirector 12 can be programmed to route the attachments to a fax or voice number where the user is located using an attached fax or voice machine 30.” Hind at 16:18-31. “Network access requirements will also vary depending upon the type of network 1919. For example, in the Mobitex and DataTAC networks, mobile devices 24 are registered on the network using a unique personal identification number or PIN associated with each device. In GPRS networks, however, network access is associated with a subscriber or user of a device 24.” Hind at 12:8-12. “Alternatively, connection 105 could be a wireless connection, such as a short-range RF connection. This docking procedure is one method for exchanging bulk personal information locally (versus over a wireless communication network), such as, but not limited to, e-mail messages, calendar events, contacts, notes, and security information like encryption keys.” Hind at 30:31-31:4. “FIG. 6 is a system diagram showing the basic components of an IP based wireless data network, such as the GPRS network, for use with the present invention. In the case of FIG. 6, the mobile device 100 (also referenced as mobile device 24 in earlier figures) is shown as being in communication with the host system 120, via a short-range RF communication link, a serial link, or any other suitable connection 105. When the mobile device is communicating to the host via connection 115, it is said to be 'docked' with the host system 120 for the purposes of this description. Preferably the mobile device 100 communicates with a wireless packet data network 145 when not "docked," and may also be capable of communicating with a voice wireless network 150. The

’619 Patent – Claim 23	Hind
	voice network 150 may be associated with the IP based wireless network 145, or it could be a completely separate network. A mobile device 100 that can communicate via networks 145 and 150 is referred to herein as a dual-mode device. The invention, however, is applicable to single-mode devices and other multi-mode devices, not just dual-mode devices. Although depicted as separate networks, the IP based wireless network 145 and the voice wireless network 150 are not necessarily mutually exclusive, and could be operating simultaneously with the same network hardware, i.e., they may be part of a single dual-mode network. In one embodiment, when a serial docking cradle 110 is used as a means of docking or undocking the mobile device 100, the serial docking cradle preferably has the ability to inform the redirector program 12 when the mobile device 100 is not in the cradle and therefore should be reached by the LP based wireless network 145. Preferably, only when the mobile device 100 is in the serial cradle 110, and behind the company's firewall 160, can it exchange shared secrets such as encryption keys, with the user's host system 120. Advantageously, these shared secrets can then be used by the redirection system to encrypt all data items being exchanged over the network 145. The redirector program 12 may also have the ability to compress information that is redirected to the mobile device 100, and thus increase data transfer rates through any delivery mechanism that is used. The redirector program 12 may also connect to a wide range of other devices, such as home or office alarm systems, personal monitoring equipment, such as a vital sign monitor, motion detectors, Internet web sites, e-mail message stores, PBX information storage, customer databases, proprietary software applications, Intranet-based data stores and other information sources, for the purpose of collecting information to redirect to the mobile device 100.” Hind at 29:13-30:18. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in

’619 Patent – Claim 23	Hind
	Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

’619 Patent – Claim 24	Hind
[24] The device of claim 22, wherein the information including the service activation code is received by the device in an off-line communication.	Hind discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:  Fig. 1

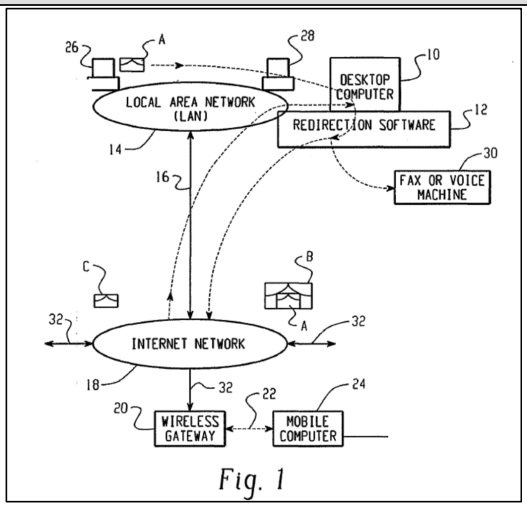
’619 Patent – Claim 24	Hind
	Hind, Fig. 1.  Fig. 6 Hind, Fig. 2. “Also exchanged between the mobile device and the redirector 12 is a personal identification number (PIN) of the user's mobile device 24 such that the redirector 12 associates the mailbox of the user with a PIN. The PIN value could be selected by the manfacturer of the mobile device 24 and programmed into the mobile device 24. Alternatively, this PIN could be a network identifier such as MSISDN, or another value associated with the Subscriber Identity Module (SIM) such as the LMSI. This PIN will be processed by the store-and-

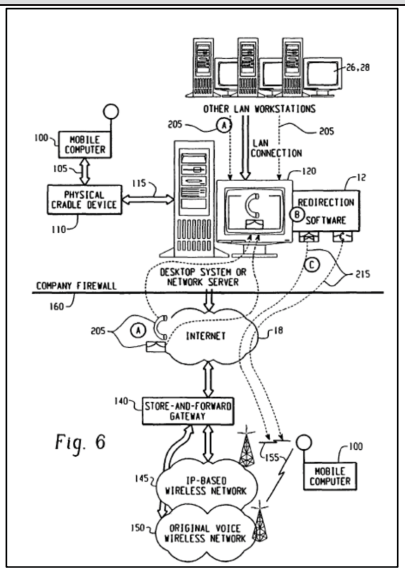
’619 Patent – Claim 24	Hind
	forward gateway as it maps the PIN of the mobile device 24 to the currently assigned IP address. Other values that could be saved by the redirector program 12 could include: the type of device, and whether the device 24 can accept certain types of attachments, such as word processing or voice attachments. If the. user's type of mobile device cannot accept these types of attachments, then the redirector 12 can be programmed to route the attachments to a fax or voice number where the user is located using an attached fax or voice machine 30.” Hind at 16:18-31. “Network access requirements will also vary depending upon the type of network 1919. For example, in the Mobitex and DataTAC networks, mobile devices 24 are registered on the network using a unique personal identification number or PIN associated with each device. In GPRS networks, however, network access is associated with a subscriber or user of a device 24.” Hind at 12:8-12. “Alternatively, connection 105 could be a wireless connection, such as a short-range RF connection. This docking procedure is one method for exchanging bulk personal information locally (versus over a wireless communication network), such as, but not limited to, e-mail messages, calendar events, contacts, notes, and security information like encryption keys.” Hind at 30:31-31:4. “FIG. 6 is a system diagram showing the basic components of an IP based wireless data network, such as the GPRS network, for use with the present invention. In the case of FIG. 6, the mobile device 100 (also referenced as mobile device 24 in earlier figures) is shown as being in communication with the host system 120, via a short-range RF communication link, a serial link, or any other suitable connection 105. When the mobile device is communicating to the host via connection 115, it is said to be 'docked' with the host system 120 for the purposes of this description. Preferably the mobile device 100

’619 Patent – Claim 24	Hind
	communicates with a wireless packet data network 145 when not "docked," and may also be capable of communicating with a voice wireless network 150. The voice network 150 may be associated with the IP based wireless network 145, or it could be a completely separate network. A mobile device 100 that can communicate via networks 145 and 150 is referred to herein as a dual-mode device. The invention, however, is applicable to single-mode devices and other multi-mode devices, not just dual-mode devices. Although depicted as separate networks, the IP based wireless network 145 and the voice wireless network 150 are not necessarily mutually exclusive, and could be operating simultaneously with the same network hardware, i.e., they may be part of a single dual-mode network. In one embodiment, when a serial docking cradle 110 is used as a means of docking or undocking the mobile device 100, the serial docking cradle preferably has the ability to inform the redirector program 12 when the mobile device 100 is not in the cradle and therefore should be reached by the LP based wireless network 145. Preferably, only when the mobile device 100 is in the serial cradle 110, and behind the company's firewall 160, can it exchange shared secrets such as encryption keys, with the user's host system 120. Advantageously, these shared secrets can then be used by the redirection system to encrypt all data items being exchanged over the network 145. The redirector program 12 may also have the ability to compress information that is redirected to the mobile device 100, and thus increase data transfer rates through any delivery mechanism that is used. The redirector program 12 may also connect to a wide range of other devices, such as home or office alarm systems, personal monitoring equipment, such as a vital sign monitor, motion detectors, Internet web sites, e-mail message stores, PBX information storage, customer databases, proprietary software applications, Intranet-based data stores and other information sources, for the purpose of collecting information to redirect to the mobile device 100.” Hind at 29:13-30:18.

’619 Patent – Claim 24	Hind
	Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

’619 Patent – Claim 25	Hind
[25] The device of claim 24, wherein the off-line communication involves a local connection.	Hind discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:

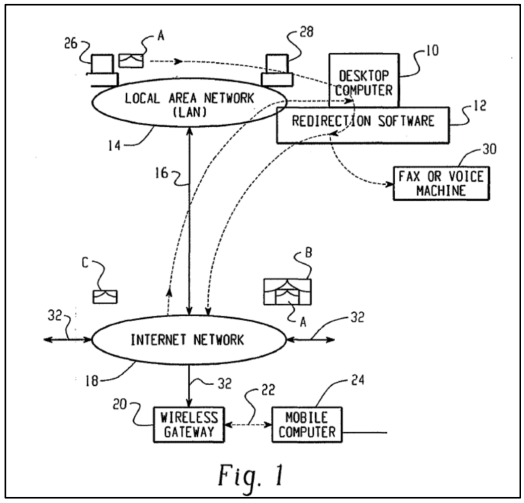
’619 Patent – Claim 25	Hind
	 *Fig. 1* Hind, Fig. 1.

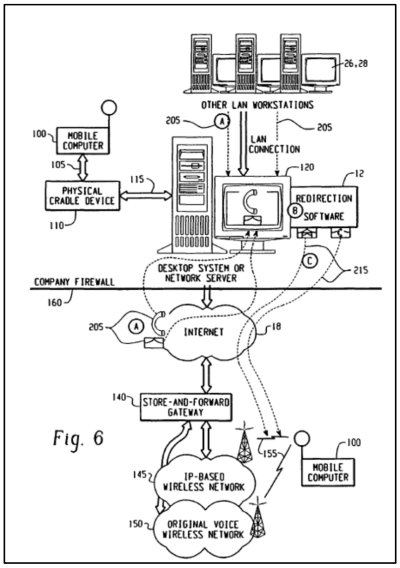
’619 Patent – Claim 25	Hind
	 Fig. 6 Hind, Fig. 2. “Also exchanged between the mobile device and the redirector 12 is a personal identification number (PIN) of the user's mobile device 24 such that the redirector 12 associates the mailbox of the user with a PIN. The PIN value could be selected by the manfacturer of the mobile device 24 and programmed into the mobile device 24. Alternatively, this PIN could be a network identifier such as MSISDN, or another value associated with the Subscriber Identity Module (SIM) such as the LMSI. This PIN will be processed by the store-and-forward gateway as it maps the PIN of the mobile device 24 to the currently assigned IP address. Other values that could be saved by the redirector program

’619 Patent – Claim 25	Hind
	12 could include: the type of device, and whether the device 24 can accept certain types of attachments, such as word processing or voice attachments. If the. user's type of mobile device cannot accept these types of attachments, then the redirector 12 can be programmed to route the attachments to a fax or voice number where the user is located using an attached fax or voice machine 30.” Hind at 16:18-31. “Network access requirements will also vary depending upon the type of network 1919. For example, in the Mobitex and DataTAC networks, mobile devices 24 are registered on the network using a unique personal identification number or PIN associated with each device. In GPRS networks, however, network access is associated with a subscriber or user of a device 24.” Hind at 12:8-12. “Alternatively, connection 105 could be a wireless connection, such as a short-range RF connection. This docking procedure is one method for exchanging bulk personal information locally (versus over a wireless communication network), such as, but not limited to, e-mail messages, calendar events, contacts, notes, and security information like encryption keys.” Hind at 30:31-31:4. “FIG. 6 is a system diagram showing the basic components of an IP based wireless data network, such as the GPRS network, for use with the present invention. In the case of FIG. 6, the mobile device 100 (also referenced as mobile device 24 in earlier figures) is shown as being in communication with the host system 120, via a short-range RF communication link, a serial link, or any other suitable connection 105. When the mobile device is communicating to the host via connection 115, it is said to be 'docked' with the host system 120 for the purposes of this description. Preferably the mobile device 100 communicates with a wireless packet data network 145 when not "docked," and may also be capable of communicating with a voice wireless network 150. The

’619 Patent – Claim 25	Hind
	voice network 150 may be associated with the IP based wireless network 145, or it could be a completely separate network. A mobile device 100 that can communicate via networks 145 and 150 is referred to herein as a dual-mode device. The invention, however, is applicable to single-mode devices and other multi-mode devices, not just dual-mode devices. Although depicted as separate networks, the IP based wireless network 145 and the voice wireless network 150 are not necessarily mutually exclusive, and could be operating simultaneously with the same network hardware, i.e., they may be part of a single dual-mode network. In one embodiment, when a serial docking cradle 110 is used as a means of docking or undocking the mobile device 100, the serial docking cradle preferably has the ability to inform the redirector program 12 when the mobile device 100 is not in the cradle and therefore should be reached by the LP based wireless network 145. Preferably, only when the mobile device 100 is in the serial cradle 110, and behind the company's firewall 160, can it exchange shared secrets such as encryption keys, with the user's host system 120. Advantageously, these shared secrets can then be used by the redirection system to encrypt all data items being exchanged over the network 145. The redirector program 12 may also have the ability to compress information that is redirected to the mobile device 100, and thus increase data transfer rates through any delivery mechanism that is used. The redirector program 12 may also connect to a wide range of other devices, such as home or office alarm systems, personal monitoring equipment, such as a vital sign monitor, motion detectors, Internet web sites, e-mail message stores, PBX information storage, customer databases, proprietary software applications, Intranet-based data stores and other information sources, for the purpose of collecting information to redirect to the mobile device 100.” Hind at 29:13-30:18. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in

’619 Patent – Claim 25	Hind
	Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

’619 Patent – Claim 26	Hind
[26] The device of claim 24, wherein the off-line communication prevents eavesdropping of the service activation code.	Hind discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:  Fig. 1

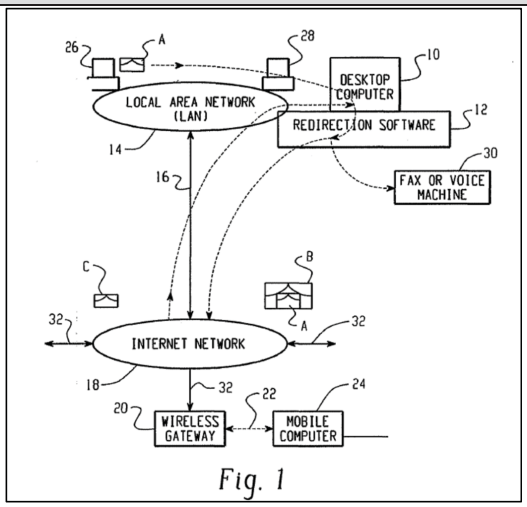
’619 Patent – Claim 26	Hind
	Hind, Fig. 1.  Fig. 6 Hind, Fig. 2. “Also exchanged between the mobile device and the redirector 12 is a personal identification number (PIN) of the user's mobile device 24 such that the redirector 12 associates the mailbox of the user with a PIN. The PIN value could be selected by the manfacturer of the mobile device 24 and programmed into the mobile device 24. Alternatively, this PIN could be a network identifier such as MSISDN, or another value associated with the Subscriber Identity Module (SIM) such as the LMSI. This PIN will be processed by the store-and-

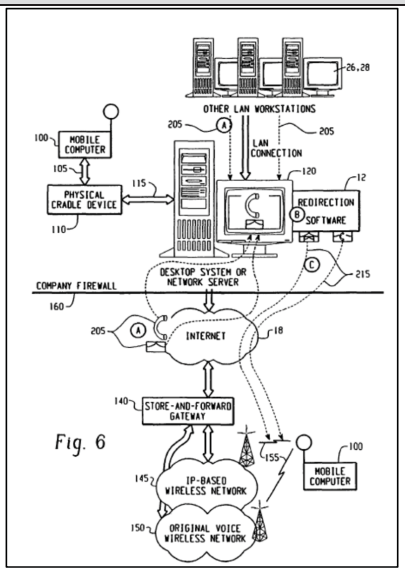
’619 Patent – Claim 26	Hind
	forward gateway as it maps the PIN of the mobile device 24 to the currently assigned IP address. Other values that could be saved by the redirector program 12 could include: the type of device, and whether the device 24 can accept certain types of attachments, such as word processing or voice attachments. If the. user's type of mobile device cannot accept these types of attachments, then the redirector 12 can be programmed to route the attachments to a fax or voice number where the user is located using an attached fax or voice machine 30.” Hind at 16:18-31. “Network access requirements will also vary depending upon the type of network 1919. For example, in the Mobitex and DataTAC networks, mobile devices 24 are registered on the network using a unique personal identification number or PIN associated with each device. In GPRS networks, however, network access is associated with a subscriber or user of a device 24.” Hind at 12:8-12. “Alternatively, connection 105 could be a wireless connection, such as a short-range RF connection. This docking procedure is one method for exchanging bulk personal information locally (versus over a wireless communication network), such as, but not limited to, e-mail messages, calendar events, contacts, notes, and security information like encryption keys.” Hind at 30:31-31:4. “FIG. 6 is a system diagram showing the basic components of an IP based wireless data network, such as the GPRS network, for use with the present invention. In the case of FIG. 6, the mobile device 100 (also referenced as mobile device 24 in earlier figures) is shown as being in communication with the host system 120, via a short-range RF communication link, a serial link, or any other suitable connection 105. When the mobile device is communicating to the host via connection 115, it is said to be 'docked' with the host system 120 for the purposes of this description. Preferably the mobile device 100

’619 Patent – Claim 26	Hind
	communicates with a wireless packet data network 145 when not "docked," and may also be capable of communicating with a voice wireless network 150. The voice network 150 may be associated with the IP based wireless network 145, or it could be a completely separate network. A mobile device 100 that can communicate via networks 145 and 150 is referred to herein as a dual-mode device. The invention, however, is applicable to single-mode devices and other multi-mode devices, not just dual-mode devices. Although depicted as separate networks, the IP based wireless network 145 and the voice wireless network 150 are not necessarily mutually exclusive, and could be operating simultaneously with the same network hardware, i.e., they may be part of a single dual-mode network. In one embodiment, when a serial docking cradle 110 is used as a means of docking or undocking the mobile device 100, the serial docking cradle preferably has the ability to inform the redirector program 12 when the mobile device 100 is not in the cradle and therefore should be reached by the LP based wireless network 145. Preferably, only when the mobile device 100 is in the serial cradle 110, and behind the company's firewall 160, can it exchange shared secrets such as encryption keys, with the user's host system 120. Advantageously, these shared secrets can then be used by the redirection system to encrypt all data items being exchanged over the network 145. The redirector program 12 may also have the ability to compress information that is redirected to the mobile device 100, and thus increase data transfer rates through any delivery mechanism that is used. The redirector program 12 may also connect to a wide range of other devices, such as home or office alarm systems, personal monitoring equipment, such as a vital sign monitor, motion detectors, Internet web sites, e-mail message stores, PBX information storage, customer databases, proprietary software applications, Intranet-based data stores and other information sources, for the purpose of collecting information to redirect to the mobile device 100.” Hind at 29:13-30:18.

’619 Patent – Claim 26	Hind
	Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

’619 Patent – Claim 27	Hind
[27] The device of claim 22, wherein the authentication of the device relies on the authentication of the messaging account.	Hind discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:

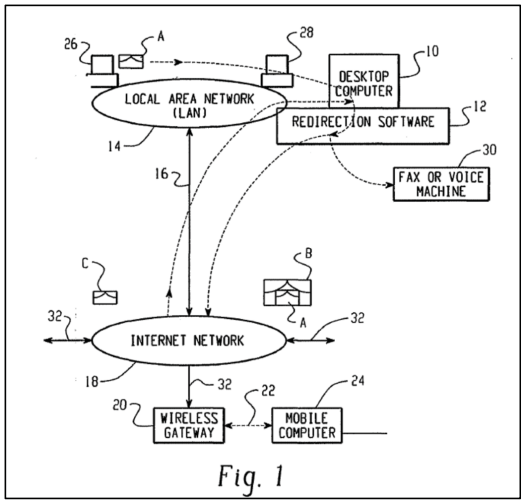
’619 Patent – Claim 27	Hind
	 *Fig. 1* Hind, Fig. 1.

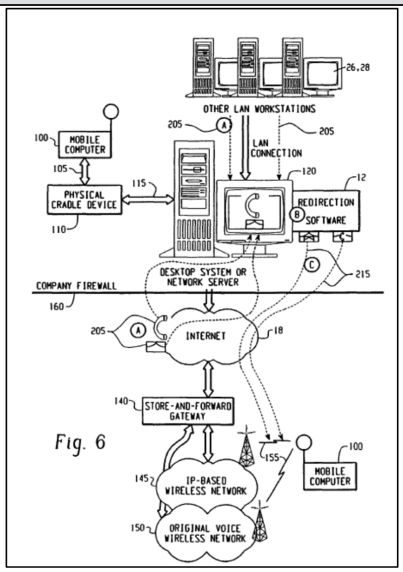
’619 Patent – Claim 27	Hind
	 Fig. 6 Hind, Fig. 2. “Also exchanged between the mobile device and the redirector 12 is a personal identification number (PIN) of the user's mobile device 24 such that the redirector 12 associates the mailbox of the user with a PIN. The PIN value could be selected by the manfacturer of the mobile device 24 and programmed into the mobile device 24. Alternatively, this PIN could be a network identifier such as MSISDN, or another value associated with the Subscriber Identity Module (SIM) such as the LMSI. This PIN will be processed by the store-and-forward gateway as it maps the PIN of the mobile device 24 to the currently assigned IP address. Other values that could be saved by the redirector program

'619 Patent – Claim 27	Hind
	12 could include: the type of device, and whether the device 24 can accept certain types of attachments, such as word processing or voice attachments. If the. user's type of mobile device cannot accept these types of attachments, then the redirector 12 can be programmed to route the attachments to a fax or voice number where the user is located using an attached fax or voice machine 30." Hind at 17:17-31. "Network access requirements will also vary depending upon the type of network 1919. For example, in the Mobitex and DataTAC networks, mobile devices 24 are registered on the network using a unique personal identification number or PIN associated with each device. In GPRS networks, however, network access is associated with a subscriber or user of a device 24." Hind at 12:8-12. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

'619 Patent – Claim 28	Hind
[28] The device of claim 27, wherein the authentication of the messaging account includes a username and password.	This claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable

’619 Patent – Claim 28	Hind
	solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

’619 Patent – Claim 32	Hind
[32] The device of claim 22, wherein the encryption key is closely related to the service activation code.	Hind discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:  Fig. 1 Hind, Fig. 1.

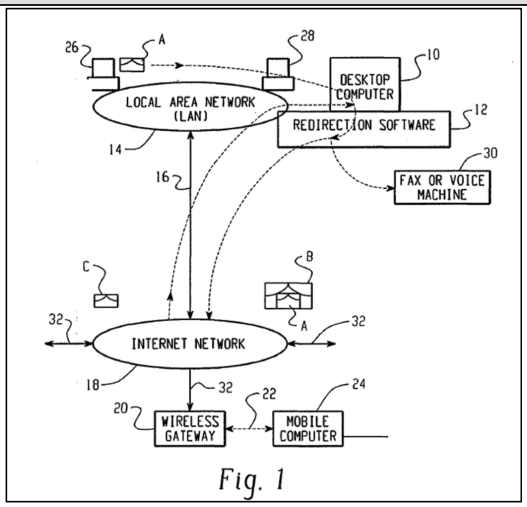
’619 Patent – Claim 32	Hind
	 Fig. 6 Hind, Fig. 2. “Assuming that the redirector program 12 is activated, and has been configured by the user (either through the sensing of an internal, network or external event) to replicate certain user data items (including messages of type A or C) to the mobile device 24, when the message A is received at the host system 10, the redirector program 12 detects its presence and prepares the message for redirection to the mobile device 24. In preparing the message for redirection, the redirector program 12 could compress the original message A, could compress the message header, or could encrypt the entire message A to create a

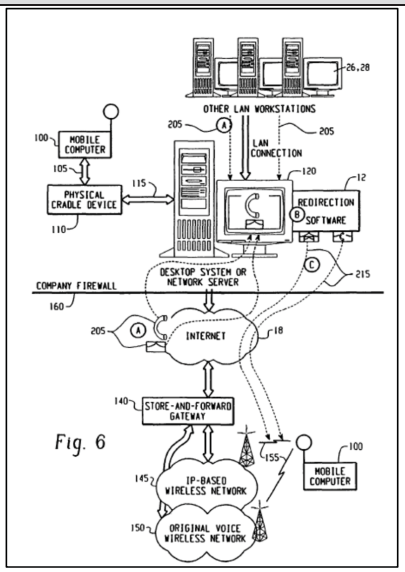
’619 Patent – Claim 32	Hind
	secure link to the mobile device 24.” Hind at 17:9-17. “Once an event has triggered redirection of the user data items, the host system repackages these items in a manner that is transparent to the mobile data communication device, so that the data at the mobile device appears similar to the same data at the user's host system. The preferred repackaging method includes wrapping the user data items in an E-mail envelope that corresponds to the address of the mobile data communication device, although, alternatively, other repackaging methods could be used with the present invention, such as special- purpose TCP/IP wrapping techniques, or other methods of wrapping the user selected data items. The repackaging method preferably results in a shared E- mail address for the user's host system and the user's mobile device. To a recipient of an E-mail generated at either the host or the mobile device, it appears as though the E-mail was generated at the host system. The repackaging method also provides encryption/decryption and compression/decompression.” Hind at 6:28-7:8. “The alternate download path may, for example, be used to load an encryption key onto the device through a direct and thus reliable and trusted connection to thereby enable secure device communication.” Hind at 15:10-13. “If the system includes encryption keys, these too can be kept at one place for management and update purposes.” Hind at 20:12-13. “Preferably, only when the mobile device 100 is in the serial cradle 110, and behind the company's firewall 160, can it exchange shared secrets such as encryption keys, with the user's host system 120. Advantageously, these shared secrets can then be used by the redirection system to encrypt all data items being exchanged over the network 145. The redirector program 12 may also have the ability to compress information that is redirected to the mobile device

’619 Patent – Claim 32	Hind
	100, and thus increase data transfer rates through any delivery mechanism that is used.” Hind at 30:5-12. “Alternatively, connection 105 could be a wireless connection, such as a short-range RF connection. This docking procedure is one method for exchanging bulk personal information locally (versus over a wireless communication network), such as, but not limited to, e-mail messages, calendar events, contacts, notes, and security information like encryption keys.” Hind at 30:31-31:4. “The network entry point 305 then uses an address assignment component, i.e. like DHCP 335 to allocate an IP address for the mobile device 100. Having allocated an IP address to the device 100 and communicated this information to the gateway 140, information, such as the stored data items, can then be sent from the store-and-forward gateway 140 to the mobile device 100 via the wireless network tunnel 325. In addition, as data items are received from the host system, these data items can be addressed with the IP address now associated with the mobile and immediately sent to the mobile without undue delay, thereby allowing a seamless and continuous pushing of the data items from the host to the mobile as they arrive temporarily at the store and forward gateway. The presence of the wireless tunnel provides the redirector program with a continuous, uninterrupted secure communication link between the host system, located behind the corporate firewall, and the mobile device 100. Through this secure communication link the redirector program delivers secure, encrypted messages that cannot be viewed by any intermediate component or node, only the mobile device user.” Hind at 36:13-28. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person

’619 Patent – Claim 32	Hind
	of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

’619 Patent – Claim 33	Hind
[33a] The device of claim 22, wherein the device is further operable to:	Hind discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22pre]-[22h], *above*. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[33b] store an association between at least two of the encryption key, the messaging account, an identifier of the remote device, and the service activation code.	Hind discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:

’619 Patent – Claim 33	Hind
	 *Fig. 1* Hind, Fig. 1.

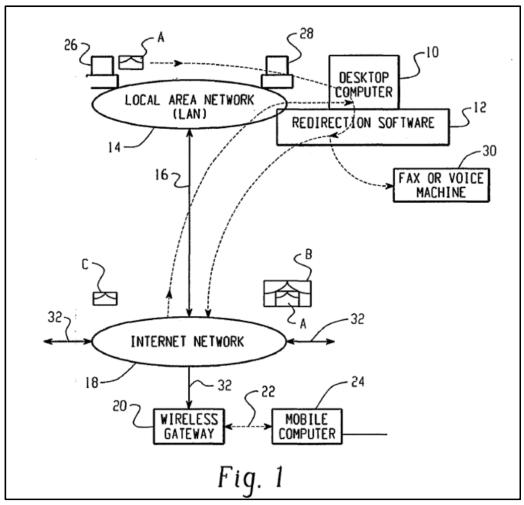
’619 Patent – Claim 33	Hind
	 Fig. 6 Hind, Fig. 2. “Also exchanged between the mobile device and the redirector 12 is a personal identification number (PIN) of the user's mobile device 24 such that the redirector 12 associates the mailbox of the user with a PIN. The PIN value could be selected by the manfacturer of the mobile device 24 and programmed into the mobile device 24. Alternatively, this PIN could be a network identifier such as MSISDN, or another value associated with the Subscriber Identity Module (SIM) such as the LMSI. This PIN will be processed by the store-and-forward gateway as it maps the PIN of the mobile device 24 to the currently assigned IP address. Other values that could be saved by the redirector program

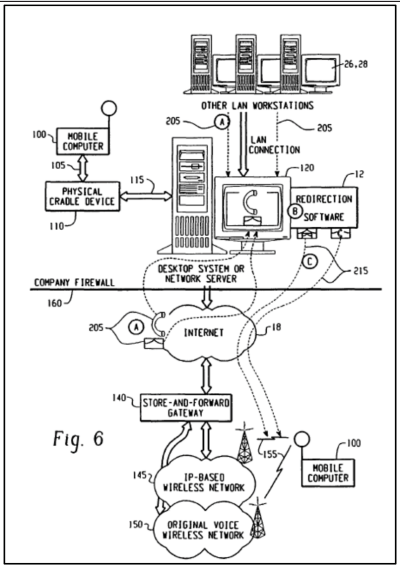
’619 Patent – Claim 33	Hind
	12 could include: the type of device, and whether the device 24 can accept certain types of attachments, such as word processing or voice attachments. If the. user's type of mobile device cannot accept these types of attachments, then the redirector 12 can be programmed to route the attachments to a fax or voice number where the user is located using an attached fax or voice machine 30.” Hind at 16:18-31. “The redirector program preferably adds a permanent identifier on the outer envelop during the repackaging step. Advantageously this permits association of the data items upon arrival at the store-and-forward gateway with the mobile devices newly assigned network address. Since the IP address associated to the mobile device could change, the permanent identifier used by the redirector program could be a manufacturing number assigned when the unit is built, a value from the SIM card, or a network specific identifier.” Hind at 24:12-18. “The alternate download path may, for example, be used to load an encryption key onto the device through a direct and thus reliable and trusted connection to thereby enable secure device communication.” Hind at 15:10-13. “If the system includes encryption keys, these too can be kept at one place for management and update purposes.” Hind at 20:12-13. “Preferably, only when the mobile device 100 is in the serial cradle 110, and behind the company's firewall 160, can it exchange shared secrets such as encryption keys, with the user's host system 120. Advantageously, these shared secrets can then be used by the redirection system to encrypt all data items being exchanged over the network 145. The redirector program 12 may also have the ability to compress information that is redirected to the mobile device 100, and thus increase data transfer rates through any delivery mechanism that is used.” Hind at 30:5-12.

’619 Patent – Claim 33	Hind
	“Alternatively, connection 105 could be a wireless connection, such as a short-range RF connection. This docking procedure is one method for exchanging bulk personal information locally (versus over a wireless communication network), such as, but not limited to, e-mail messages, calendar events, contacts, notes, and security information like encryption keys.” Hind at 30:31-31:4. “The network entry point 305 then uses an address assignment component, i.e. like DHCP 335 to allocate an IP address for the mobile device 100. Having allocated an IP address to the device 100 and communicated this information to the gateway 140, information, such as the stored data items, can then be sent from the store-and-forward gateway 140 to the mobile device 100 via the wireless network tunnel 325. In addition, as data items are received from the host system, these data items can be addressed with the IP address now associated with the mobile and immediately sent to the mobile without undue delay, thereby allowing a seamless and continuous pushing of the data items from the host to the mobile as they arrive temporarily at the store and forward gateway. The presence of the wireless tunnel provides the redirector program with a continuous, uninterrupted secure communication link between the host system, located behind the corporate firewall, and the mobile device 100. Through this secure communication link the redirector program delivers secure, encrypted messages that cannot be viewed by any intermediate component or node, only the mobile device user.” Hind at 36:13-28. “Therefore, wireless network operators have allocated only a small number of 'real IP addresses' and use a dynamic address assignment as a preferred strategy. Mobile devices 100 must therefore have an alternate permanent identifier, and servers must maintain a dynamic link between that permanent identifier of the mobile device and the temporary IP address of the mobile device.” Hind at 41:7-12.

’619 Patent – Claim 33	Hind
	Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

’619 Patent – Claim 36	Hind
[36] The device of claim 22, wherein a control message is received from the remote device upon user interaction with the message.	Hind discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22pre]-[22h], *above*. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

’619 Patent – Claim 37	Hind
[37pre] 37. A method for sharing a messaging account, the method comprising:	To the extent the preamble is limiting, Hind discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:  *Fig. 1* Hind, Fig. 1.

’619 Patent – Claim 37	Hind
	 Fig. 6 Hind, Fig. 2. “Once an event has triggered redirection of the user data items, the host system repackages these items in a manner that is transparent to the mobile data communication device, so that the data at the mobile device appears similar to the same data at the user's host system. The preferred repackaging method includes wrapping the user data items in an E-mail envelope that corresponds to the address of the mobile data communication device, although, alternatively, other repackaging methods could be used with the present invention, such as special- purpose TCP/IP wrapping techniques, or other methods of wrapping the user selected data items. The repackaging method

’619 Patent – Claim 37	Hind
	preferably results in a shared E- mail address for the user's host system and the user's mobile device. To a recipient of an E-mail generated at either the host or the mobile device, it appears as though the E-mail was generated at the host system. The repackaging method also provides encryption/decryption and compression/decompression.” Hind at 6:28-7:8. “As described above, the redirector program 12 executing at the host system then strips the outer envelope and routes the reply message to the appropriate destination address using the address of the user's e-mail account associated with the host system as the "from" field, so that to the recipient of the redirected message, it appears as though it originated from the user's host system rather than the mobile device. In an alternative embodiment a tag or signature line is added to the message (at either the device or the host system) to indicate that it has been sent from a mobile device 24 whilst the mobile device and host system continue to share a common single email address. This integrated common email address provides the host system (desktop or server system) with seamless wireless connectivity to the mobile device.” Hind at 27:24-28:3. “FIG. 1 shows an E-mail message A being communicated over LAN 14 from computer 26 to the user's desktop system 10 (also shown in FIG. 1 is an external message C, which could be an E-mail message from an Internet user, or could be a command message from the user's mobile device 24). Once the message A (or C) reaches the primary message store of the host system 10, it can be detected and acted upon by the redirection software 12. The redirection software 12 can use many methods of detecting new messages. The preferred method of detecting new messages is using a message server like Microsoft's® Messaging API (MAPI), IMAP4 server or Lotus Notes messaging API, in which programs, such as the redirector program 12, register for notifications or 'advise syncs' when changes to a mailbox take place. Other methods of detecting new messages could also be used with the present invention. This tight integration between the redirection program 12 and a messaging server

’619 Patent – Claim 37	Hind
	effectively means the two programs are co-operating to provide a wireless extension to an existing messaging product. In another embodiment, the redirection program is an embedded component of the message server.” Hind at 16:25-17:8. “Assuming that the redirector program 12 is activated, and has been configured by the user (either through the sensing of an internal, network or external event) to replicate certain user data items (including messages of type A or C) to the mobile device 24, when the message A is received at the host system 10, the redirector program 12 detects its presence and prepares the message for redirection to the mobile device 24. In preparing the message for redirection, the redirector program 12 could compress the original message A, could compress the message header, or could encrypt the entire message A to create a secure link to the mobile device 24.” Hind at 17:9-17. “Using the redirector program, the user can select certain data items for redirection, such as E-mail messages, calendar events, meeting notifications, address entries, journal entries, personal reminders, etc. Having selected the data items for redirection, the user can then configure one or more event triggers, which are sensed by the redirector program to initiate redirection of the user's data items. These user-defined triggers (or event triggers) may include external events, internal events and networked events. Examples of external events include: receiving a message from the user's mobile data communication device to begin redirection; receiving a similar message from some external computer; sensing that the user is no longer in the vicmity of the host system; or any other event that is external to the host system. Internal events could be a calendar alarm, screen saver activation, keyboard timeout, programmable timer, or any other user-defined event that is internal to the host system. Networked events are user-defined messages that are transmitted to the host system from another computer coupled to the host system via a network to initiate redirection.” Hind at 5:21-6:3.

’619 Patent – Claim 37	Hind
	“After the redirector has determined that a particular message should be redirected, and it has prepared the message for redirection, the software 12 then sends the message A to a secondary memory store located in the mobile device 24, using whatever means are necessary. In the preferred embodiment this method is to send the message A back over the LAN 14, WAN 18, and through the store-and-forward gateway 20 to the mobile data commumcation device 24. In doing so, the redirector preferably repackages message A as an E-mail with an outer envelope B that contains the addressing information of the mobile device 24, although alternative repackaging techniques and protocols could be used, such as a TCP/IP repackaging and delivery method (most commonly used in the alternative server configuration shown in FIG. 2). The wireless gateway 20 requires this outer envelope information B in order to know where to send the redirected message A. Once the message (A in B) is received by the mobile device 24, the outer envelope B is removed and the original message A is placed in the secondary memory store within the mobile device 24. By repackaging and removing the outer envelope in this manner, the present invention causes the mobile computer 24 to appear to be at the same physical location as the host system 10, thus creating a transparent system.” Hind at 18:25-19:10. “A user of the present invention can configure the redirector program 12 to push certain user-selected data items to the user's mobile device 24 when the redirector 12 detects that a particular user-defined event trigger (or trigger point) has taken place. User-selected data items preferably include E-mail messages, calendar events, meeting notifications, address entries, journal entries, personal alerts, alarms, warnings, stock quotes, news bulletins, corporate data (from an Intranet or from behind the corporate firewall), etc., but could, alternatively, include any other type of message that is transmitted to the host system 10, or that the host system 10 acquires through the use of intelligent agents, such as data that is received after the host system 10 initiates a search of a database or a website or a bulletin board.” Hind at 15:25-16:3.

'619 Patent – Claim 37	Hind
	"As described above, the present invention preferably provides a redirection computer program ("redirector program") 12, operating within (or in conjunction with) the host system 120, behind a corporate firewall 160. Preferably in conjunction with a message server or some other hardware or software mechanism, the redirector 12 senses that a particular event has occurred, and redirects user-selected data items from the host system 120 to the user's mobile device 100. In one embodiment, the redirector program 12 also interfaces to a mobile device cradle component 110, over a serial connection 115, or some other suitable computer communication method, so that the redirector program 12 can detect the physical location, as well as other information, of the mobile device 100." Hind at 30:19-31:4. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[37a] authenticating a device for access to the messaging account;	Hind discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22h], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and

’619 Patent – Claim 37	Hind
	Exhibit 619-B.
[37b] optically receiving information including a displayed service activation code from a remote device;	Hind discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22c], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[37c] registering the remote device for access to the messaging account using the service activation code;	Hind discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22d], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[37d] receiving a message for the messaging account;	Hind discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:

’619 Patent – Claim 37	Hind
	See [22e], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[37e] encrypting the message using an encryption key; and	Hind discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22f], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[37f] sending the message to the remote device.	Hind discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22g], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill

'619 Patent – Claim 37	Hind
	in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

'619 Patent – Claim 38	Hind
[38] The method of claim 37, wherein the information including the service activation code is received by the device in response to user input at the remote device.	Hind discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [23], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

'619 Patent – Claim 39	Hind
[39] The method of claim 38, wherein the information including the service activation code is received by the device in an off-line communication.	Hind discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [24], above.

’619 Patent – Claim 39	Hind
	Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

’619 Patent – Claim 40	Hind
[40] The method of claim 39, wherein the off-line communication prevents eavesdropping of the service activation code.	Hind discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [26], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

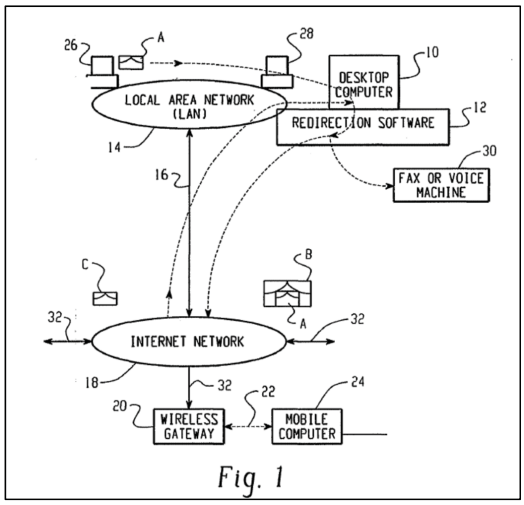
’619 Patent – Claim 41	Hind
[41] The method of claim 37, wherein the authentication of the device relies on the authentication of the messaging system.	Hind discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:

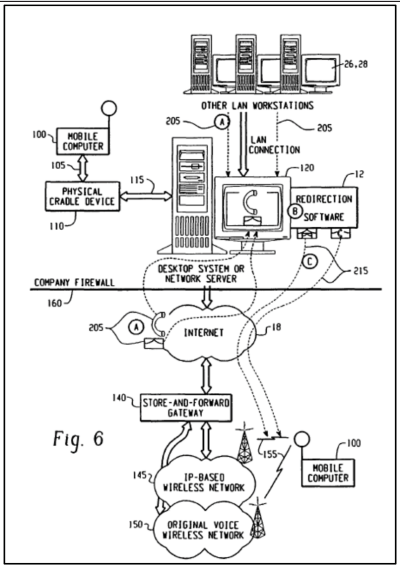
’619 Patent – Claim 41	Hind
	See [27], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

’619 Patent – Claim 42	Hind
[42] The method of claim 41, wherein the authentication of the messaging system includes a username and password.	Hind discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [28], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

’619 Patent – Claim 46	Hind
[46] The method of claim 37, wherein the encryption key is closely related to the service activation code.	Hind discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [32], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

’619 Patent – Claim 50	Hind
[50] The method of claim 37, wherein a control message is received from the remote device upon user interaction with the message.	Hind discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [36], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

’619 Patent – Claim 51	Hind
[51pre] 51. A non-transient computer-readable medium containing program instructions for causing a device to perform a method, the method comprising:	To the extent the preamble is limiting, Hind discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:  *Fig. 1* Hind, Fig. 1.

’619 Patent – Claim 51	Hind
	 Fig. 6 Hind, Fig. 2. “Although it is preferable for the system to operate in a two-way communications mode, certain aspects of the invention could be beneficially used in a "one and one-half or acknowledgment paging environment, or even with a one-way paging system. The mobile data communication device 24 includes software program instructions that work in conjunction with the redirector program 12 to enable the seamless, transparent redirection of user-selected data items. FIG. 4 describes the basic method steps of the redirector program 12, and FIG. 5 describes the steps of the corresponding program operating at the mobile device 24.” Hind at 11:10-18.

’619 Patent – Claim 51	Hind
	“The desktop system 10 is connected to LAN 14, and can send and receive data, messages, signals, event triggers, etc., to and from other systems connected to the LAN 14 and to external networks 18, 22, such as the Internet or a wireless data network, which are also coupled to the LAN 14. hi addition to the standard hardware, operating system, and application programs associated with a typical microcomputer or workstation, the desktop system 10 includes the redirector program 12, a TCP/IP sub-system 42, an E-mail sub-system 44, a primary data storage device 40, a screen saver sub-system 48, and a keyboard sub-system 46. The TCP/IP and E-mail subsystems 42, 44 are examples of repackaging systems that can be used to achieve the transparency of the present invention, and the screen saver and keyboard sub-systems 46, 48 are examples of event generating systems that can be configured to generate event messages or signals that trigger redirection of the user selected data items. The method steps carried out by the redirector program 12 are described in more detail in FIG. 4. The basic functions of this program are: (1) configure and setup the user-defined event trigger points that will start redirection; (2) configure the types of user data items for redirection and optionally configure a preferred list of senders whose messages are to be redirected; (3) configure the type and capabilities of the user's mobile data communication device; (4) receive messages and signals from the repackaging systems and the event generating systems; and (5) command and control the redirection of the user-selected data items to the mobile data communication device via the repackaging systems. Other functions not specifically enumerated could also be integrated into this program.” Hind at 21:22-22:13. “Functionally, the redirector program 12 provides the user with the ability to configure the screen saver and keyboard systems so that under certain conditions a event trigger will be generated that can be detected by the redirector 12 to start the redirection process. For example, the screen saver system can be configured so that when the screen saver is activated, after, for example, 10 minutes of inactivity on the desktop system, an event trigger is transmitted to the redirector 12, which starts redirecting the previously selected

’619 Patent – Claim 51	Hind
	user data items. In a similar manner the keyboard sub-system can be configured to generate event triggers when no key has been depressed for a particular period of time, thus indicating that redirection should commence. These are just two examples of the numerous application programs and hardware systems internal to the host system 10 that can be used to generate internal event triggers. FIGs. 4 and 5, set forth, respectively, flow charts showing the steps carried out by the redirector software 12 operating at the host system 10, and the steps carried out by the mobile data communication device 24 in order to interface with the host system. Turning first to FIG. 4, at step 50, the redirector program 12 is started and initially configured.” Hind at 23:17-24:2. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[51a] optically receiving information including a displayed service activation code from a remote device;	Hind discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22c], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and

’619 Patent – Claim 51	Hind
	Exhibit 619-B.
[51b] registering the remote device for access to a messaging account using the service activation code;	Hind discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22d], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[51c] receiving a message for the messaging account;	Hind discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22e], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[51d] encrypting the message using an encryption key; and	Hind discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures:

'619 Patent – Claim 51	Hind
	See [22f], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[51e] sending the message to the remote device,	Hind discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22g], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.
[51f] wherein the device is authenticated to access the messaging account.	Hind discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [22h], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill

’619 Patent – Claim 51	Hind
	in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

’619 Patent – Claim 52	Hind
[52] The method of claim 51, wherein a control message is received from the remote device upon user interaction with the message.	Hind discloses this claim limitation. For example, see the following passages and/or figures, as well as all related disclosures: *See* [36], above. Furthermore, this claim element is obvious in light of this reference itself, when combined with any of the other references as charted for this claim element in Exhibit A, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Exhibit 619-B.

EXHIBIT 619-B

EXHIBIT 619-B

TABLE OF CONTENTS

Page

Motivation to Combine References

Where obviousness is asserted, an explanation of why the prior art renders the asserted claim obvious, including examples of combinations of prior art showing obviousness, is set forth in the claim charts included in Exhibit 619-A, which identify specific examples of where each limitation of the asserted claims is found in the prior art references, or herein.

Apple notes that in *KSR Int'l Co. v. Teleflex Inc.*, the Supreme Court held that "[i]n determining whether the subject matter of a patent claim is obvious, neither the particular motivation nor the avowed purpose of the patentee controls. What matters is the objective reach of the claim. If the claim extends to what is obvious, it is invalid under § 103." 550 U.S. 398, 127 S.Ct. 1727, 1742 (2007).

KSR further illustrated several ways in which the subject matter of a patent claim may be shown to be obvious. For instance, "[o]ne of the ways in which a patent's subject matter can be proved obvious is by noting that there existed at the time of invention a known problem for which there was an obvious solution encompassed by the patent's claims." *KSR*, 127 S.Ct. 1727, 1742. The Supreme Court held that it was error to "look only to the problem the patentee was trying to solve." *Id.* Rather, "[t]he question is not whether the combination was obvious to the patentee but whether the combination was obvious to a person with ordinary skill in the art. Under the correct analysis, any need or problem known in the field of endeavor at the time of invention and addressed by the patent can provide a reason for combining the elements in the manner claimed." *Id.* Further, "[c]ommon sense teaches … that familiar items may have obvious uses beyond their primary purposes, and in many cases a person of ordinary skill will be able to fit the teachings of multiple patents together like pieces of a puzzle." *Id.* Further, a showing that a combination of elements was "obvious to try" may show that it was obvious

under § 103. *Id.* For instance, the Supreme Court held that "predictable solutions" using a combination of "known options" may render the subject matter of a patent claim obvious:

> When there is a design need or market pressure to solve a problem and there are a finite number of identified, predictable solutions, a person of ordinary skill has good reason to pursue the known options within his or her technical grasp. If this leads to the anticipated success, it is likely the product not of innovation but of ordinary skill and common sense.

Id.

The ways in which the subject matter of a patent claim may be shown to be obvious, identified by *KSR*, are merely illustrative. The main thrust of *KSR* was that "[r]igid preventative rules that deny factfinders recourse to common sense"—such as the overturned "teaching, suggestion, or motivation" test—are neither necessary under our case law nor consistent with it." *KSR*, 127 S.Ct. 1727, 1742-43; citing with approval, e.g., *DyStar Textilfarben GmbH & Co. Deutschland KG v. C.H. Patrick Co.*, 464 F. 3d 1356, 1367 (2006) ("Our suggestion test is in actuality quite flexible and not only permits, but requires, consideration of common knowledge and common sense"); *Alza Corp. v. Mylan Labs., Inc.*, 464 F. 3d 1286, 1291 (2006) ("There is flexibility in our obviousness jurisprudence because a motivation may be found implicitly in the prior art. We do not have a rigid test that requires an actual teaching to combine . . . .").

Although Apple notes that there is no longer a rigid requirement regarding motivation to combine under *KSR*, Apple provides the following statements regarding motivation to combine to comply with Patent L.R. 3-3(b). Multiple teachings, suggestions, and/or reasons to modify any of the references and/or to combine any two or more of the references in Exhibit A come from many sources, including the prior art (specific and as a whole), common knowledge, common sense, predictability, expectations, industry trends, design incentives or need, market demand or pressure, market forces, obvious to try, the nature of the problem faced, and/or knowledge possessed by one of ordinary skill. In addition, it would have been obvious to try

combining the prior art references identified above because there were only a finite number of predictable solutions and/or because known work in one field or endeavor prompted variations based on predictable design incentives and/or market forces either in the same field or a different one. The combination of prior art references identified in these contentions would have been obvious because the combination represents the known potential options with a reasonable expectation of success. Additionally, one of ordinary skill in the art would have been motivated to create combinations identified in these contentions using: known methods to yield predictable results; known techniques in the same way; a simple substitution of one known, equivalent element for another to obtain predictable results; and/or teaching, suggestion, or motivation in the prior art generally. Also, market forces in the industry, and the desire to improve features and performance, would motivate the addition of features to systems as they become available, become less expensive, become more commonly used, provide better performance, reduce costs, size or weight, or predictably achieve other clearly desirable results.

Because discovery is ongoing and Apple has not yet completed their investigation, discovery, or analysis of the issues raised by SEVEN's claims, Apple reserves the right to supplement and amend their explanation of why the prior art renders the asserted claims obvious, including an identification of any combinations of prior art showing obviousness, as they receive additional information either through their own investigations or from SEVEN or third parties. In particular, Apple's investigation and analysis is significantly impeded by the insufficiency and incompleteness of SEVEN's infringement contentions.

Table 1: "a radio"

Independent claim 22 of the '619 patent recites "a radio." To the extent SEVEN alleges this limitation is missing in any of the references charted in Exhibit 619-A, such a limitation would have been obvious to a person of ordinary skill in the art at the time of the alleged invention. Market forces and other consumer trends to smaller devices and wireless devices would have motivated a person of ordinary skill in the art to provide a radio to a device the availability of wireless communication and messaging to increase user convenience, and enhance user experiences. *See, e.g.*, Thompson at 1:17-20 ("Personal Digital Assistant (PDA) devices, like the 3 Com PalmPilot®, provide a user with an easy, compact device that can hold all of a user's daily essentials in one place."); 1:23-27 ("Other desirable features found on a PDA device include instant information access, intuitive construction for easy use, conservative energy cell consumption, extensive personal calendaring features, a customized address book, a digital memo pad, an expense calculator, desktop e-mail connectivity, Internet compatibility, and local or remote database synchronization."); Cross at 11:14-25; Brown at 5:26-36; Klassen at 8:41-53; Munje at 3:17-37; Little at [0076]; Hind at 12:2-7. Because little or no complexity was involved in including a feature such as a radio to a device, one of ordinary skill in the art would have found the addition of a radio to a computing device obvious as shown below.

As of the alleged '619 patent priority date, the presence of a radio in a computer or similar device was well known and commonplace in the art. *See, e.g.*, Thompson at 1:17-20; 1:23-27; Cross at 11:14-25; Brown at 5:26-36; Klassen at 8:41-53; Munje at 3:17-37; Little at [0076]; Hind at 12:2-7. Numerous systems and publications, including those described in Exhibit 619-A, disclosed a radio.

For these reasons, the "a radio" limitation is anticipated by the references listed in Exhibit 619-A or, to the extent not anticipated, obvious to one of ordinary skill in the art at the time the

invention described in the '619 patent was made. To the extent a primary or obviousness reference does not disclose this limitation, one of ordinary skill in the art would be motivated to combine the primary or obviousness references with any one or more of the Table 1 references listed below because: all the references relate to computing devices used for communication; using the techniques of the Table 1 references would have improved the primary or obviousness references in the same way (for example, by adding a radio to a computing device); and applying the techniques of the Table 1 references to improve primary or obviousness references would have yielded predictable results.

Reference	**Disclosure**
International Patent Application No. WO 01/29731 to Thompson et al. ("Thompson")	*See, e.g.*, Thompson at Figs. 1-5; 3:34-4:17; 8:7-17; 15:1-20
U.S. Patent No. 7,984,488 to Cross et al. ("Cross")	*See, e.g.*, Cross at Figs. 1, 7; 10:47-61; 11:14-25
U.S. Patent No. 7,603,556 to Brown et al. ("Brown")	*See, e.g.*, Brown at Figs. 1-2, 4; 5:26-36; 9:49-64; 5:57-6:14; 13:43-54
U.S. Patent No. 7,849,313 to Klassen et al. ("Klassen")	*See, e.g.*, Klassen at Figs. 1, 5-6; 5:46-6:15; 8:41-53
U.S. Patent No. 8,831,576 to Munje et al. ("Munje")	*See, e.g.*, Munje at Figs. 1, 3, 6; 3:17-37
U.S. Patent App. No. 2004/0205248 to Little et al. ("Little")	*See, e.g.*, Little at [0025], [0027], [0067], [0068], [0072], [0079], Fig. 2, Fig. 3, Fig. 8
U.S. Patent No. 7,012,503 to	*See, e.g.*, Nielsen at Figs. 2a-b, 3, 5a-b, 6a-c, 7b; 10:25-44; 12:3-14

Reference	Disclosure
Nielsen et al. ("Nielsen")	
U.S. Patent App. No. 2004/0255034 ("Choi")	*See, e.g.*, Choi at [0024]; [0026]; [0065]; [0069]; [0071]; [0078];
U.S. Patent App. No. 2003/0014267 ("Culp")	*See, e.g.*, Culp at [0016]
U.S. Patent App. No. 2006/0028924 ("Atkinson")	*See, e.g.*, Atkinson at [0021]; [0022]
Int. Patent App. WO 2005/002174 ("Braley")	*See, e.g.*, Braley at Abstract; [001]; [006]; [008]; [016]
U.S. Patent App. No. 2006/0135064 ("Cho")	*See, e.g.*, Cho at [0005]; [0021]; [0041]
European Patent EP 1 578 093 ("Ekdahl")	*See, e.g.*, Ekdahl at [0012]; [0020]; [0023]; [0026]
U.S. Patent No. 7,921,209 ("Hammell")	*See, e.g.*, Hammell at 3:12-40; 3:41-59
U.S. Patent No. 7,562,218 ("Kirkup")	*See, e.g.*, Kirkup at 7:1-27
Int. Patent App. WO 02/25890 ("Hind")	*See, e.g.*, Hind at 12:2-7; 32:3-12; 29:13-31; 30:29-31:4

Table 2: "optically receive information including a displayed service activation code from a remote device;"

Each asserted independent claim of the '619 patent recites "optically receive [receiving] information including a displayed service activation code from a remote device." To the extent SEVEN alleges this limitation is missing in any of the references charted in Exhibit 619-A, such a limitation would have been obvious to a person of ordinary skill in the art at the time of the alleged invention. Market forces and other consumer trends to more secure transmission of data would have motivated a person of ordinary skill to use a finite number of options to transmit data from one device to another: a direct-wired connection or a direct non-wired connection to increase the security of the passing of data. *See, e.g.*, Thompson at 4:7-15 ("Just as there are many different types of access control codes, there are multiple methods of delivering the codes to a service controller or security outlet. One method is through the I/O cradle attached to the PDA device and the digital device. I/O cradles are usually attached to either the serial RS-232 port or the parallel port. Another interface method is between a PDA Infra-Red (IR) port and an I/O module attached to the digital device with a IR interface. A preferred embodiment of the present invention utilizes wireless transceiver, built into the PDA device to communicate with a receiver. Finally traditional interface parts, coils, or transmissions may be effectively used."); Cross at 3:13-37; Brown at 13:43-54; Hind at 15:14-19; Antilla at Figs. 1-3; [0014]; [0016]; [0021]-[0023]; [0028]-[0030]; Osthoff at [0011]; Turunen at 8:26-49. As the security between the transfer of data between two devices became more important with the advent of the internet and networks, one of ordinary skill in the art would have been motivated to use near-field wireless communications between two devices such as infrared, Bluetooth, lasers, or barcodes to transfer secure data because wired connections can be cumbersome. *See, e.g.*, Thompson at 4:7-15; Cross at 3:13-37; Brown at 13:43-54; Hind at 15:14-19. Because little or no complexity was

involved in including these features and functionalities on computing devices, one of ordinary skill in the art would have found the migration of near-field wireless communications obvious as shown below.

As of the alleged ’619 patent priority date, the near-field wireless transfer of secure data was well known and commonplace in the art. *See, e.g.*, Thompson at 4:7-15; Cross at 3:13-37; Brown at 13:43-54; Hind at 15:14-19. Numerous systems and publications, including those described in Exhibit 619-A, disclosed “optically receive information including a displayed service activation code from a remote device”.

For these reasons, the “optically receive information including a displayed service activation code from a remote device” limitation is anticipated by the references listed in Exhibit 619-A or, to the extent not anticipated, obvious to one of ordinary skill in the art at the time the invention described in the ’619 patent was made. To the extent a primary or obviousness reference does not disclose this limitation, one of ordinary skill in the art would be motivated to combine the primary or obviousness references with any one or more of the Table 2 references listed below because: all the references relate to the secure transfer and access to data; using the techniques of the Table 2 references would have improved the primary or obviousness references in the same way (for example, by adding an IR port to a device); and applying the techniques of the Table 2 references to improve primary or obviousness references would have yielded predictable results.

Reference	**Disclosure**
International Patent Application No. WO 01/29731 to Thompson et al. (“Thompson”)	*See, e.g.*, Thompson at Figs. 1-5; Abstract; 2:11-29; 2:30-3:8; 3:34-4:17; 4:18-36; 7:6-19; 8:7-17; 15:1-20

Reference	Disclosure
U.S. Patent No. 7,984,488 to Cross et al. ("Cross")	*See, e.g.*, Cross at Figs. 1, 7; Abstract; 3:13-37; 3:40-57; 4:4-19; 10:63-11:13
U.S. Patent No. 7,603,556 to Brown et al. ("Brown")	*See, e.g.*, Brown at Figs. 1-2, 4, Abstract; Summary; 8:16-9:18; 12:46-61
U.S. Patent No. 7,849,313 to Klassen et al. ("Klassen")	*See, e.g.*, Klassen at Figs. 1, 5-6; Abstract; 2:46-59; 2:60-3:22; 6:16-35; 7:27-46; 7:60-8:6; 8:7-27; 10:47-62; 11:57-12:11
U.S. Patent No. 8,831,576 to Munje et al. ("Munje")	*See, e.g.*, Munje at Figs. 1, 3, 6; 3:17-37; 4:60-5:16; 5:65-6:11; 6:44-7:61
U.S. Patent No. 7,012,503 to Nielsen et al. ("Nielsen")	*See, e.g.*, Nielsen at Figs. 2a-b, 3, 5a-b, 6a-c, 7b; 16:54-17:6
U.S. Patent App. No. 2006/0031913 ("Pulitzer")	*See, e.g.,* Pulitzer at [0004]; [0038]; Fig. 4
U.S. Patent App. No. 2004/0255034 ("Choi")	*See, e.g.,* Choi at [0069-]-[0071]; [0095]; [0111]-[0117]; [0128]; [0141]
U.S. Patent App. No. 2003/0014267 ("Culp")	*See, e.g.*, Culp at [0016]; [0018]
U.S. Patent App. No. 2006/0028924 ("Atkinson")	*See, e.g.*, Atkinson at [0010]; [0021]; [0022]; [0031]
Int. Patent App. WO 2005/002174 ("Braley")	*See, e.g.*, Braley at Abstract; [001]; [006]-[008]; [017]-028]
U.S. Patent App. No. 2006/0135064 ("Cho")	*See, e.g.*, Cho at Fig. 2; Abstract; [0026]; [0028]; [0038]; [0040]; [0043]; [0045]; [0059]; Claim 1, 9

Reference	Disclosure
European Patent EP 1 578 093 ("Ekdahl")	*See, e.g.*, Ekdahl at Abstract; [0003]; [0007]; [0018]; [0023]-[0026]; [0029]-[0030]; [0033]-[0036]; Figs. 1, 2
U.S. patent No. 7,289,792 ("Turunen")	*See, e.g.*, Turunen at 8:26-49
U.S. Patent App. No. 2002/0147918 ("Osthoff")	*See, e.g.*, Osthoff at [0011]
U.S. Patent No. 7,124,953 ("Antilla")	*See, e.g.*, Antilla at Figs. 1-3; [0014]; [0016]; [0021]-[0023]; [0028]-[0030]
U.S. Patent No. 7,921,209 ("Hammell")	*See, e.g.*, Hammell at Abstract; 4:13-40; 8:5-14; 9:57-10:18
U.S. Patent No. 7,562,218 ("Kirkup")	*See, e.g.*, Kirkup at Abstract; 3:14-20; 3:28-44; 4:21-44; 4:51-59
Int. Patent App. WO 02/25890 ("Hind")	*See, e.g.*, Hind at 29:13-30:5; 17:17-31; 12:8-12; 15:14-19; 30:31-31:11

Table 3: "register the remote device for access to a messaging account using the service activation code;"

Each asserted independent claim of the '619 patent recites "register[ing] the remote device for access to a messaging account using the service activation code." To the extent SEVEN alleges this limitation is missing in any of the references charted in Exhibit 619-A, such a limitation would have been obvious to a person of ordinary skill in the art at the time of the alleged invention. Maintaining secure access to a messaging account would have motivated a person of skill in the art to require the registration of a device to access a messaging account. *See, e.g.*, Thompson at ABSTRACT ("An access control system combining PDA functionality with user authentication so that only the authorized user or users may obtain access control codes from a PDA device for an access control point."); Cross at 2:46-67; Brown at 12:46-61; Klassen at ABSTRACT; Munje at 4:26-5:4; Little at [0105]. A person of ordinary skill in the art would know that it is not secure to allow a device access to a messaging account without a way to verify that the device has the rights to access the messaging account. *See, e.g.*, Thompson at ABSTRACT; Cross at 2:46-67; Brown at 12:46-61; Klassen at ABSTRACT; Munje at 4:26-5:4; Little at [0105]; Hind at 17:17-31. Because little or no complexity was involved in including the feature of requiring that a device be registered before accessing a messaging account, one of ordinary skill in the art would have found the feature obvious as shown below.

As of the alleged '619 patent priority date, requiring that a device be registered before accessing a messaging account was well known and commonplace in the art. *See, e.g.*, Thompson at ABSTRACT; Cross at 2:46-67; Brown at 12:46-61; Klassen at ABSTRACT; Munje at 4:26-5:4; Little at [0105]; Hind at 17:17-31. Numerous systems and publications, including those described in Exhibit 619-A, disclosed "register[ing] the remote device for access to a messaging account using the service activation code".

For these reasons, the "register[ing] the remote device for access to a messaging account using the service activation code" limitation is anticipated by the references listed in Exhibit 619-A or, to the extent not anticipated, obvious to one of ordinary skill in the art at the time the invention described in the '619 patent was made. To the extent a primary or obviousness reference does not disclose this limitation, one of ordinary skill in the art would be motivated to combine the primary or obviousness references with any one or more of the Table 3 references listed below because: all the references relate to computing devices used for communication; using the techniques of the Table 3 references would have improved the primary or obviousness references in the same way; and applying the techniques of the Table 3 references to improve primary or obviousness references would have yielded predictable results.

Reference	**Disclosure**
International Patent Application No. WO 01/29731 to Thompson et al. ("Thompson")	*See, e.g.*, Thompson at Figs. 1-5; Abstract; 8:18-35; 9:30-10:15; 15:1-20
U.S. Patent No. 7,984,488 to Cross et al. ("Cross")	*See, e.g.*, Cross at Figs. 1, 7; 1:18-26; 2:46-67; Abstract; 3:13-37; 3:40-57; 4:4-19; 10:63-11:13
U.S. Patent No. 7,603,556 to Brown et al. ("Brown")	*See, e.g.*, Brown at Figs. 1-2, 4, 5:8-25; 5:37-56; 7:24-43; 10:55-11:4; 12:19-29; 12:46-61
U.S. Patent No. 7,849,313 to Klassen et al. ("Klassen")	*See, e.g.*, Klassen at Figs. 1, 5-6; Abstract; 2:46-59; 2:60-3:22; 6:16-35; 7:27-46; 7:60-8:6; 8:7-27; 10:47-62; 11:57-12:11
U.S. Patent No. 8,831,576 to Munje et al. ("Munje")	*See, e.g.*, Munje at Figs. 1, 3, 6; 4:26-5:4; 7:62-8:23
U.S. Patent App. No.	*See, e.g.*, Little at [0105], Fig. 2, Fig. 3, Fig. 8.

Reference	Disclosure
2004/0205248 to Little et al. ("Little")	
U.S. Patent No. 7,012,503 to Nielsen et al. ("Nielsen")	*See, e.g.*, Nielsen at Figs. 2a-b, 3, 5a-b, 6a-c, 7b; 2:48-3:3; 3:38-56; 4:29-51; 7:1-9; 13:1-13; 16:54-17:6; 17:56-18:20; 18:39-51
U.S. Patent No. 7,921,209 ("Hammell")	*See, e.g.*, Hammell at Abstract; 4:13-40; 8:5-14; 9:57-10:18
U.S. Patent No. 7,562,218 ("Kirkup")	*See, e.g.*, Kirkup at Abstract; 3:14-20; 3:28-44; 4:21-44; 4:51-59
Int. Patent App. WO 02/25890 ("Hind")	*See, e.g.*, Hind at 17:17-31; 12:8-12; 17:9-17; 10:32-11:4; 5:21-6:3; 15:25-16:3

Table 4: "receive a message for the messaging account"

Each asserted independent claim of the '619 patent recites "receive [receiving] a message for the messaging account." To the extent SEVEN alleges this limitation is missing in any of the references charted in Exhibit 619-A, such a limitation would have been obvious to a person of ordinary skill in the art at the time of the alleged invention. The proliferation of personal messaging and e-mail messaging accounts would have motivated a person of skill to create an application that allowed the receipt of messaging on a device, such as a computer. *See, e.g.*, Thompson at 9:30-10:15 ("This access control protocol allows users to access their files on a common computer shared with multiple users. E-mail files are optionally loaded directly down to the PDA once the identification authorization has been made. Additionally, a user could use a traveling work station in which he was only required to carry his PDA containing the appropriate identification information to request from the network server the user's standard desktop and access to the user's e-mail files. As a result, a traveler could go to a foreign office or another work site location, plug his PDA into the control port and be granted access to the computer with the same restrictions and limitations that he may have had at his workstation at home."); Cross at 2:46-67; Brown 5:8-37; Klassen at ABSTRACT; Munje at 2:49-3:1; Little at [0078]; Hind at 16:25-17:8. Because little or no complexity was involved in including the feature of adding an application to a device with the ability to receive messages for a messaging account, such as e-mail, one of ordinary skill in the art would have found adding the limitation obvious as shown below.

As of the alleged '619 patent priority date, receiving a message for a messaging account on a computer was well known and commonplace in the art. *See, e.g.*, Thompson at 9:30-10:15; Cross at 2:46-67; Brown 5:8-37; Klassen at ABSTRACT; Munje at 2:49-3:1; Little at [0078];

Hind at 16:25-17:8. Numerous systems and publications, including those described in Exhibit 619-A, disclosed "receive a message for the messaging account."

For these reasons, the "receive a message for the messaging account" limitation is anticipated by the references listed in Exhibit 619-A or, to the extent not anticipated, obvious to one of ordinary skill in the art at the time the invention described in the '619 patent was made. To the extent a primary or obviousness reference does not disclose this limitation, one of ordinary skill in the art would be motivated to combine the primary or obviousness references with any one or more of the Table 4 references listed below because: all the references relate to computing devices used for communication; using the techniques of the Table 4 references would have improved the primary or obviousness references in the same way (for example, by adding an e-mail application such as Microsoft Outlook or Lotus Notes); and applying the techniques of the Table 4 references to improve primary or obviousness references would have yielded predictable results.

Reference	**Disclosure**
International Patent Application No. WO 01/29731 to Thompson et al. ("Thompson")	*See, e.g.*, Thompson at Figs. 1-5; Abstract; 8:18-35; 9:30-10:15; 15:1-20
U.S. Patent No. 7,984,488 to Cross et al. ("Cross")	*See, e.g.*, Cross at Figs. 1, 7; 1:18-26; 2:46-67
U.S. Patent No. 7,603,556 to Brown et al. ("Brown")	*See, e.g.*, Brown at Figs. 1-2, 4, 5:8-37; 5:37-56; 7:24-43; 13:8-26
U.S. Patent No. 8,831,576 to Munje et al. ("Munje")	*See, e.g.*, Munje at Figs. 1, 3, 6; 2:49-3:1; 3:1-17; 4:26-5:4

Reference	Disclosure
U.S. Patent App. No. 2004/0205248 to Little et al. ("Little")	*See, e.g.*, Little at [0031], [0078], Fig. 2, Fig. 3, Fig. 8.
Int. Patent App. WO 02/25890 ("Hind")	*See, e.g.*, Hind at Fig. 1; 16:25-17:8; 17:9-17; 5:21-6:3; 18:25-19:10; 15:25-16:3; 30:19-31:4

Table 5: "encrypt the message using an encryption key"

Each independent claim of the '619 patent recites "encrypt the message using an encryption key." To the extent SEVEN alleges this limitation is missing in any of the references charted in Exhibit 619-A, such a limitation would have been obvious to a person of ordinary skill in the art at the time of the alleged invention. Maintaining the secure transfer of the messages of a messaging account would have motivated a person of skill in the art to require the encryption of any message that is transmitted from one device to another. *See, e.g.*, Thompson at 2:11-29 ("Examples of computer data felt to require access control include secure files, personalized e-mail accounts, specific user profiles, specific network profiles, and access to licensed programs. A secure file may be created by a user encrypting the file with a password. E-mail accounts obtain limited security by archiving data into personalized data structures or by password protecting e-mail access."); Cross at 1:18-26 ("Various types of encryption schemes are widely used to secure data (e.g., an email message or file) for communication over a network. For example, in symmetric encryption, both the user that is encrypting data and the user that is decrypting the data need copies of the same encryption key. Asymmetric encryption, also known as public key encryption, uses key pairs (e.g., a public key and a private key). In asymmetric encryption the public keys may be shared but the private keys are not."); Brown at Abstract; Klassen at ABSTRACT; Munje at 3:1-17; Little at [0081]; Hind at 15:10-13. Because little or no complexity was involved in including a feature to encrypt a message to be sent from one device to another, one of ordinary skill in the art would have found the feature obvious as shown below.

As of the alleged '619 patent priority date, encrypting a message was well known and commonplace in the art. *See, e.g.*, Thompson at 2:11-29; Cross at 1:18-26; Brown at Abstract; Klassen at ABSTRACT; Munje at 3:1-17; Little at [0081]; Hind at 15:10-13. Numerous systems

and publications, including those described in Exhibit 619-A, disclosed "encrypt the message using an encryption key".

For these reasons, the "encrypt the message using an encryption key" limitation is anticipated by the references listed in Exhibit 619-A or, to the extent not anticipated, obvious to one of ordinary skill in the art at the time the invention described in the '619 patent was made. To the extent a primary or obviousness reference does not disclose this limitation, one of ordinary skill in the art would be motivated to combine the primary or obviousness references with any one or more of the Table 5 references listed below because: all the references relate to computing devices used for communication; using the techniques of the Table 5 references would have improved the primary or obviousness references in the same way; and applying the techniques of the Table 5 references to improve primary or obviousness references would have yielded predictable results.

Reference	**Disclosure**
International Patent Application No. WO 01/29731 to Thompson et al. ("Thompson")	*See, e.g.*, Thompson at Figs. 1-5; 2:11-29
U.S. Patent No. 7,984,488 to Cross et al. ("Cross")	*See, e.g.*, Cross at Figs. 1, 7; 1:18-26; 2:46-67; 3:13-37; 3:40-57; 4:4-19
U.S. Patent No. 7,603,556 to Brown et al. ("Brown")	*See, e.g.*, Brown at Figs. 1-2, 4, Abstract; 6:29-59; 7:24-63
U.S. Patent No. 7,849,313 to Klassen et al. ("Klassen")	*See, e.g.*, Klassen at Figs. 1, 5-6; Abstract; 2:46-59; 2:60-3:22; 6:16-35; 7:27-46; 7:60-8:6; 8:7-27; 10:47-62; 11:57-12:11; 10:48-62; 12:46-13:3
U.S. Patent No. 8,831,576 to	*See, e.g.*, Munje at Figs. 1, 3, 6; 2:49-3:1; 3:1-17; 4:26-5:4

Reference	Disclosure
Munje et al. ("Munje")	
U.S. Patent App. No. 2004/0205248 to Little et al. ("Little")	*See, e.g.*, Little at [0031], [0081], Fig. 2, Fig. 3, Fig. 8.
U.S. Patent No. 7,012,503 to Nielsen et al. ("Nielsen")	*See, e.g.*, Nielsen at Figs. 2a-b, 3, 5a-b, 6a-c, 7b; 17:17-27; 20:55-63
Int. Patent App. WO 02/25890 ("Hind")	*See, e.g.*, Hind at 17:9-17; 6:28-7:8; 15:10-13; 20:12-13; 30:5-12; 30:31-31:4; 36:13-28

Table 6: "send the message to the remote device"

Each independent claim of the '619 patent recites "send the message to the remote device." To the extent SEVEN alleges this limitation is missing in any of the references charted in Exhibit 619-A, such a limitation would have been obvious to a person of ordinary skill in the art at the time of the alleged invention. The proliferation of personal messaging and e-mail messaging accounts would have motivated a person of skill to create an application that allowed sending of a message from one device to another, such as a computer to a PDA. *See, e.g.*, Thompson at 9:30-10:15 ("This access control protocol allows users to access their files on a common computer shared with multiple users. E-mail files are optionally loaded directly down to the PDA once the identification authorization has been made. Additionally, a user could use a traveling work station in which he was only required to carry his PDA containing the appropriate identification information to request from the network server the user's standard desktop and access to the user's e-mail files. As a result, a traveler could go to a foreign office or another work site location, plug his PDA into the control port and be granted access to the computer with the same restrictions and limitations that he may have had at his workstation at home."); Cross at 2:46-67; Brown 5:8-37; Klassen at ABSTRACT; Munje at 2:49-3:1; Little at [0031]; Hind at 16:25-17:8. Because little or no complexity was involved in including the feature of adding an application to a device with the ability to send a message to another device, such as e-mail, one of ordinary skill in the art would have found adding the limitation obvious as shown below.

As of the alleged '619 patent priority date, sending a message from one device to another was well known and commonplace in the art. *See, e.g.*, Thompson at 9:30-10:15; Cross at 2:46-67; Brown 5:8-37; Klassen at ABSTRACT; Munje at 2:49-3:1; Little at [0031]; Hind at 16:25-17:8. Numerous systems and publications, including those described in Exhibit 619-A, disclosed "send the message to the remote device".

For these reasons, the "send the message to the remote device" limitation is anticipated by the references listed in Exhibit 619-A or, to the extent not anticipated, obvious to one of ordinary skill in the art at the time the invention described in the '619 patent was made. To the extent a primary or obviousness reference does not disclose this limitation, one of ordinary skill in the art would be motivated to combine the primary or obviousness references with any one or more of the Table 6 references listed below because: all the references relate to computing devices used for communication; using the techniques of the Table 6 references would have improved the primary or obviousness references in the same way (for example, by adding an e-mail application such as Microsoft Outlook or Lotus Notes); and applying the techniques of the Table 6 references to improve primary or obviousness references would have yielded predictable results.

Reference	**Disclosure**
International Patent Application No. WO 01/29731 to Thompson et al. ("Thompson")	*See, e.g.*, Thompson at Figs. 1-5; Abstract; 8:18-35; 9:30-10:15; 15:1-20
U.S. Patent No. 7,984,488 to Cross et al. ("Cross")	*See, e.g.*, Cross at Figs. 1, 7; 1:18-26; 2:46-67; 3:13-37; 3:40-57; 4:4-19
U.S. Patent No. 7,603,556 to Brown et al. ("Brown")	*See, e.g.*, Brown at Figs. 1-2, 4, 5:8-37; 5:37-56; 7:24-43; 13:8-26
U.S. Patent No. 7,849,313 to Klassen et al. ("Klassen")	*See, e.g.*, Klassen at Figs. 1, 5-6; Abstract; 2:46-59; 2:60-3:22; 6:16-35; 7:27-46; 7:60-8:6; 8:7-27; 10:47-62; 11:57-12:11
U.S. Patent No. 8,831,576 to Munje et al. ("Munje")	*See, e.g.*, Munje at Figs. 1, 3, 6; 2:49-3:1; 3:1-17; 4:26-5:4

Reference	Disclosure
U.S. Patent App. No. 2004/0205248 to Little et al. ("Little")	*See, e.g.*, Little at [0031], [0081], Fig. 2, Fig. 3, Fig. 8.
U.S. Patent No. 7,012,503 to Nielsen et al. ("Nielsen")	*See, e.g.*, Nielsen at Figs. 2a-b, 3, 5a-b, 6a-c, 7b; 11:21-39; 12:21-40; 17:18-28
Int. Patent App. WO 02/25890 ("Hind")	*See, e.g.*, Hind at Fig. 1; 16:25-17:8; 17:9-17; 5:21-6:3; 18:25-19:10; 15:25-16:3; 6:28-7:8; 36:13-28

Table 7: "wherein the device is authenticated to access the messaging account"

Each asserted independent claim of the '619 patent recites either "wherein the device is authenticated to access the messaging account" or "authenticating a device for access to the messaging account", which are sufficiently similar and are treated as such here. To the extent SEVEN alleges this limitation is missing in any of the references charted in Exhibit 619-A, such a limitation would have been obvious to a person of ordinary skill in the art at the time of the alleged invention. Maintaining secure access to a messaging account would have motivated a person of skill in the art to require the authentication of a device to access a messaging account. A person of ordinary skill in the art would know that it is not secure to allow a device access to a messaging account without a way to verify that the device has the rights to access the messaging account. *See, e.g.*, Thompson at 9:30-10:15 ("This access control protocol allows users to access their files on a common computer shared with multiple users. E-mail files are optionally loaded directly down to the PDA once the identification authorization has been made. Additionally, a user could use a traveling work station in which he was only required to carry his PDA containing the appropriate identification information to request from the network server the user's standard desktop and access to the user's e-mail files. As a result, a traveler could go to a

foreign office or another work site location, plug his PDA into the control port and be granted access to the computer with the same restrictions and limitations that he may have had at his workstation at home."); Cross at 2:46-67; Brown 10:55-11:4; Klassen at ABSTRACT; Munje at 4:26-5:4; Little at [0078]. Because little or no complexity was involved in including the feature of requiring that a device be authenticated before accessing a messaging account, one of ordinary skill in the art would have found the feature obvious as shown below.

As of the alleged '619 patent priority date, authenticating a device before allowing access to a messaging account was well known and commonplace in the art. *See, e.g.*, Thompson at 9:30-10:15; Cross at 2:46-67; Brown 10:55-11:4; Munje at 4:26-5:4; Little at [0078]. Numerous systems and publications, including those described in Exhibit 619-A, disclosed "wherein the device is authenticated to access the messaging account".

For these reasons, the "wherein the device is authenticated to access the messaging account" limitation is anticipated by the references listed in Exhibit 619-A or, to the extent not anticipated, obvious to one of ordinary skill in the art at the time the invention described in the '619 patent was made. To the extent a primary or obviousness reference does not disclose this limitation, one of ordinary skill in the art would be motivated to combine the primary or obviousness references with any one or more of the Table 7 references listed below because: all the references relate to computing devices used for communication; using the techniques of the Table 7 references would have improved the primary or obviousness references in the same way; and applying the techniques of the Table 7 references to improve primary or obviousness references would have yielded predictable results.

Reference	**Disclosure**
International Patent Application No.	*See, e.g.*, Thompson at Figs. 1-5; Abstract; 8:18-35; 9:30-10:15; 15:1-20

Reference	Disclosure
WO 01/29731 to Thompson et al. ("Thompson")	
U.S. Patent No. 7,984,488 to Cross et al. ("Cross")	*See, e.g.*, Cross at Figs. 1, 7; 1:18-26; 2:46-67; 3:13-37; 3:40-57; 4:4-19
U.S. Patent No. 7,603,556 to Brown et al. ("Brown")	*See, e.g.*, Brown at Figs. 1-2, 4, 5:8-25; 5:37-56; 7:24-43; 10:55-11:4; 12:19-29; 12:46-61
U.S. Patent No. 7,849,313 to Klassen et al. ("Klassen")	*See, e.g.*, Klassen at Figs. 1, 5-6; Abstract; 2:46-59; 2:60-3:22; 6:16-35; 7:27-46; 7:60-8:6; 8:7-27; 10:47-62; 11:57-12:11
U.S. Patent No. 8,831,576 to Munje et al. ("Munje")	*See, e.g.*, Munje at Figs. 1, 3, 6; 4:26-5:4; 3:1-17; 4:60-5:16; 5:65-6:11; 6:44-7:61
U.S. Patent App. No. 2004/0205248 to Little et al. ("Little")	*See, e.g.*, Little at [0031], [0078], [0105], Fig. 2, Fig. 3, Fig. 8.
U.S. Patent No. 7,012,503 to Nielsen et al. ("Nielsen")	*See, e.g.*, Nielsen at Figs. 2a-b, 3, 5a-b, 6a-c, 7b; 11:21-39; 12:21-40; 17:18-28
U.S. Patent No. 7,921,209 ("Hammell")	*See, e.g.*, Hammell at Abstract; 4:13-40; 8:5-14; 9:57-10:18
U.S. Patent No. 7,562,218 ("Kirkup")	*See, e.g.*, Kirkup at Abstract; 3:14-20; 3:28-44; 4:21-44; 4:51-59
Int. Patent App. WO 02/25890 ("Hind")	*See, e.g.*, Hind at Fig. 1; 9:18-10:16; 16:25-17:8; 16:9-17; 27:24-28:3

Table 8: "wherein the information including the service activation code is received by the device in response to user input at the remote device"

Dependent claims 23 and 38 of the '619 patent recite "wherein the information including the service activation code is received by the device in response to user input at the remote device" To the extent SEVEN alleges this limitation is missing in any of the references charted in Exhibit 619-A, such a limitation would have been obvious to a person of ordinary skill in the art at the time of the alleged invention. Market forces and other consumer trends to more secure transmission of data would have motivated a person of ordinary skill to use a finite number of options to transmit data from one device to another: a direct-wired connection or a direct non-wired connection to increase the security of the passing of data. *See, e.g.*, Thompson at 4:7-15 ("Just as there are many different types of access control codes, there are multiple methods of delivering the codes to a service controller or security outlet. One method is through the I/O cradle attached to the PDA device and the digital device. I/O cradles are usually attached to either the serial RS-232 port or the parallel port. Another interface method is between a PDA Infra-Red (IR) port and an I/O module attached to the digital device with a IR interface. A preferred embodiment of the present invention utilizes wireless transceiver, built into the PDA device to communicate with a receiver. Finally traditional interface parts, coils, or transmissions may be effectively used."); Cross at 2:46-67; Brown at 8:16-37; Klassen at 4:25-31; Munje at 4:65-5:16; Little at [0044]; Hind at 16:18-31; Hammell at Abstract; 4:13-40; 8:5-14; 9:57-10:18. As the security between the transfer of data between two devices became more important with the advent of the internet and networks, one of ordinary skill in the art would have been motivated to use near-field wireless communications between two devices such as infrared, Bluetooth, lasers, or barcodes to transfer secure data because wired connections can be cumbersome. *See, e.g.*, Thompson at 4:7-15; Cross at 2:46-67; Brown at 8:16-37; Klassen at

4:25-31; Munje at 4:65-5:16; Little at [0044]; Hind at 16:18-31; Hammell at Abstract; 4:13-40; 8:5-14; 9:57-10:18; Kirkup at Abstract; 3:14-20; 3:28-44; 4:21-44; 4:51-59. Further, it would have been obvious to one of skill in the art that before sending a service activation code securely from one device to another, that a requirement that user input at the remote device before sending would be required. *See, e.g.*, Thompson at 2:30-3:8 ("A variety of access control systems and devices presently exist, however; these access control systems do not interface or coordinate with PDA devices. Specifically, a user attempting to gain access to various resources within a company is often required to carry an access card, an access key, or an I.D. access badge. The user may be required to know an access number, a PIN number, a combination, a password, or to provide a computer authorization number."); Cross at 2:46-67; Brown at 8:16-37; Klassen at 4:25-31; Munje at 4:65-5:16; Little at [0044]; Hind at 16:18-31; Hammell at Abstract; 4:13-40; 8:5-14; 9:57-10:18; Kirkup at Abstract; 3:14-20; 3:28-44; 4:21-44; 4:51-59. Because little or no complexity was involved in including these features and functionalities on computing devices, one of ordinary skill in the art would have found the requirement to have user input prior to sending a secure code from one device to another obvious as shown below.

As of the alleged '619 patent priority date, the requirement of user input prior to the near-field wireless transfer of secure data between two devices was well known and commonplace in the art. *See, e.g.*, Thompson at 4:7-15; Cross at 2:46-67; Brown at 8:16-37; Klassen at 4:25-31; Munje at 4:65-5:16; Little at [0044]; Hind at 16:18-31; Hammell at Abstract; 4:13-40; 8:5-14; 9:57-10:18; Kirkup at Abstract; 3:14-20; 3:28-44; 4:21-44; 4:51-59. Numerous systems and publications, including those described in Exhibit 619-A, disclosed "wherein the information including the service activation code is received by the device in response to user input at the remote device".

For these reasons, the "wherein the information including the service activation code is received by the device in response to user input at the remote device" limitation is anticipated by the references listed in Exhibit 619-A or, to the extent not anticipated, obvious to one of ordinary skill in the art at the time the invention described in the '619 patent was made. To the extent a primary or obviousness reference does not disclose this limitation, one of ordinary skill in the art would be motivated to combine the primary or obviousness references with any one or more of the Table 8 references listed below because: all the references relate to the secure transfer and access to data; using the techniques of the Table 8 references would have improved the primary or obviousness references in the same way (for example, by adding an IR port to a device or a "send" button on a remote device); and applying the techniques of the Table 8 references to improve primary or obviousness references would have yielded predictable results.

Reference	**Disclosure**
International Patent Application No. WO 01/29731 to Thompson et al. ("Thompson")	*See, e.g.*, Thompson at Figs. 1-5; Abstract; 2:11-29; 2:30-3:8; 3:34-4:17; 4:18-36; 7:6-19; 8:7-17; 15:1-20
U.S. Patent No. 7,984,488 to Cross et al. ("Cross")	*See, e.g.*, Cross at Figs. 1, 7; 1:18-26; 2:46-67; 3:13-37; 3:40-57; 4:4-19
U.S. Patent No. 7,603,556 to Brown et al. ("Brown")	*See, e.g.*, Brown at Figs. 1-2, 4, 7:67-8:15; 8:16-37; 8:46-58
7,849,313 to Klassen et al. ("Klassen")	*See, e.g.*, Klassen at Figs. 1, 5-6; 4:25-31; 4:48-58; 5:8-16; 5:27-41; 7:39-46; 7:60-8:6; 10:22-29; 13:25-46
U.S Patent No. 8,831,576 to Munje et al. ("Munje").	*See, e.g.*, Munje at Figs. 1, 3, 6; 4:65-5:16; 7:19-34; 7:62-8:23

Reference	Disclosure
U.S. Patent App. No. 2004/0205248 to Little et al. ("Little")	*See, e.g.*, Little at [0044], [0031], [0078], [0105], Fig. 2, Fig. 3, Fig. 8.
U.S. Patent No. 7,012,503 to Nielsen et al. ("Nielsen")	*See, e.g.*, Nielsen at Figs. 2a-b, 3, 5a-b, 6a-c, 7b; 5:13-32; 5:38-54; 13:1-13; 17:56-18:20
U.S. Patent App. No. 2004/0255034 ("Choi")	*See, e.g.* Choi at [0069-]-[0071]; [0095]; [0111]-[0117]; [0128]; [0141]
U.S. Patent App. No. 2006/0135064 ("Cho")	*See, e.g.*, Cho at Fig. 2; Abstract; [0026]; [0028]; [0038]; [0040]; [0043]; [0045]; [0059]; Claim 1, 9
Int. Patent App. WO 2005/002174 ("Braley")	*See, e.g.*, Braley at Abstract; [001]; [006]-[008]; [017]-028]
European Patent EP 1 578 093 ("Ekdahl")	*See, e.g.*, Ekdahl at Abstract; [0003]; [0007]; [0018]; [0023]-[0026]; [0029]-[0030]; [0033]-[0036]; Figs. 1, 2
U.S. Patent App. No. 2006/0031913 ("Pulitzer")	*See, e.g.*, Pulitzer at [0004]; [0038]; Fig. 4
U.S. patent No. 7,289,792 ("Turunen")	*See, e.g.*, Turunen at 7:55-65; 8:26-49
U.S. Patent App. No. 2002/0147918 ("Osthoff")	*See, e.g.*, Osthoff at [0011]
U.S. Patent No. 7,921,209 ("Hammell")	*See, e.g.*, Hammell at Abstract; 4:13-40; 8:5-14; 9:57-10:18
U.S. Patent No. 7,562,218 ("Kirkup")	*See, e.g.*, Kirkup at Abstract; 3:14-20; 3:28-44; 4:21-44; 4:51-59
Int. Patent App. WO 02/25890 ("Hind")	*See, e.g.*, Hind at 16:18-31; 12:8-12; 30:31-31:4; 29:13-30:18; 16:18-31

Table 9: "wherein the information including the service activation code is received by the device in an off-line communication"

Dependent claims 24 and 38 of the '619 patent recite "wherein the information including the service activation code is received by the device in an off-line communication." To the extent SEVEN alleges this limitation is missing in any of the references charted in Exhibit 619-A, such a limitation would have been obvious to a person of ordinary skill in the art at the time of the alleged invention. Maintaining the secure transfer of a service activation code to pair two devices would have motivated a person of skill in the art to require the off-line communication between two devices, such as a local connection. *See, e.g.*, Thompson at 4:7-15 ("Just as there are many different types of access control codes, there are multiple methods of delivering the codes to a service controller or security outlet. One method is through the I/O cradle attached to the PDA device and the digital device. I/O cradles are usually attached to either the serial RS-232 port or the parallel port. Another interface method is between a PDA Infra-Red (IR) port and an I/O module attached to the digital device with a IR interface. A preferred embodiment of the present invention utilizes wireless transceiver, built into the PDA device to communicate with a receiver. Finally traditional interface parts, coils, or transmissions may be effectively used."); Cross at 2:46-67; Brown at 12:46-61; Klassen at 9:63-10:4; Hind at 30:31-31:4. Because little or no complexity was involved in including a feature to transfer a service activation code in an off-line communication, one of ordinary skill in the art would have found the feature obvious as shown below.

As of the alleged '619 patent priority date, off-line communications were well known and commonplace in the art. *See, e.g.*, Thompson at 4:7-15; Cross at 2:46-67; Brown at 12:46-61; Klassen at 9:63-10:4; Hind at 30:31-31:4. Numerous systems and publications, including those

described in Exhibit 619-A, disclosed "wherein the information including the service activation code is received by the device in an off-line communication".

For these reasons, the "wherein the information including the service activation code is received by the device in an off-line communication" limitation is anticipated by the references listed in Exhibit 619-A or, to the extent not anticipated, obvious to one of ordinary skill in the art at the time the invention described in the '619 patent was made. To the extent a primary or obviousness reference does not disclose this limitation, one of ordinary skill in the art would be motivated to combine the primary or obviousness references with any one or more of the Table 9 references listed below because: all the references relate to computing devices used for communication; using the techniques of the Table 9 references would have improved the primary or obviousness references in the same way (for example, by adding a Bluetooth connection between devices); and applying the techniques of the Table 9 references to improve primary or obviousness references would have yielded predictable results.

Reference	**Disclosure**
International Patent Application No. WO 01/29731 to Thompson et al. ("Thompson")	*See, e.g.*, Thompson at Figs. 1-5; Abstract; 2:11-29; 2:30-3:8; 3:34-4:17; 4:18-36; 7:6-19; 8:7-17; 15:1-20
U.S. Patent No. 7,984,488 to Cross et al. ("Cross")	*See, e.g.*, Cross at Figs. 1, 7; 1:18-26; 2:46-67; 3:13-37; 3:40-57; 4:4-19
U.S. Patent No. 7,603,556 to Brown et al. ("Brown")	*See, e.g.*, Brown at Figs. 1-2, 4, 7:67-8:15; 12:46-61; 13:43-54
U.S. Patent No. 7,849,313 to Klassen et al. ("Klassen")	*See, e.g.*, Klassen at Figs. 1, 5-6; 8:7-27; 9:63-10:4

Reference	Disclosure
U.S. Patent No. 8,831,576 to Munje et al. ("Munje")	*See, e.g.*, Munje at Figs. 1, 3, 6; 2:3-8; 6:44-53; 7:19-34
U.S. Patent No. 7,012,503 to Nielsen et al. ("Nielsen")	*See, e.g.*, Nielsen at Figs. 2a-b, 3, 5a-b, 6a-c, 7b; 4:1-23; 6:8-16; 10:25-44; 11:63-12:2
U.S. Patent App. No. 2006/0031913 ("Pulitzer")	*See, e.g.*, Pulitzer at [0004]; [0038]; Fig. 4
U.S. Patent App. No. 2004/0255034 ("Choi")	*See, e.g.*, Choi at [0069-]-[0071]; [0095]; [0111]-[0117]; [0128]; [0141]
U.S. Patent No. 7,562,218 ("Kirkup")	*See, e.g.*, Kirkup at 7:1-27
Int. Patent App. WO 02/25890 ("Hind")	*See, e.g.*, Hind at 16:18-31; 12:8-12; 30:31-31:4; 29:13-30:18

Table 10: "wherein the off-line communication involves a local connection"

Dependent claim 25 of the '619 patent recites "wherein the off-line communication involves a local connection." To the extent SEVEN alleges this limitation is missing in any of the references charted in Exhibit 619-A, such a limitation would have been obvious to a person of ordinary skill in the art at the time of the alleged invention. Maintaining the secure transfer of a service activation code to pair two devices would have motivated a person of skill in the art to require the off-line communication between two devices, such as a local connection. *See, e.g.*, Thompson at 4:7-15; Cross at 2:46-67; Brown at 12:46-61; Klassen at 9:63-10:4; Hind at 30:31-31:4. Because little or no complexity was involved in including a feature to transfer a service activation code in an off-line communication, one of ordinary skill in the art would have found the feature obvious as shown below.

As of the alleged '619 patent priority date, off-line communications by local connection were well known and commonplace in the art. *See, e.g.*, Thompson at 4:7-15; Cross at 2:46-67; Brown at 12:46-61; Klassen at 9:63-10:4; Hind at 30:31-31:4. Numerous systems and publications, including those described in Exhibit 619-A, disclosed "wherein the off-line communication involves a local connection".

For these reasons, the "wherein the off-line communication involves a local connection" limitation is anticipated by the references listed in Exhibit 619-A or, to the extent not anticipated, obvious to one of ordinary skill in the art at the time the invention described in the '619 patent was made. To the extent a primary or obviousness reference does not disclose this limitation, one of ordinary skill in the art would be motivated to combine the primary or obviousness references with any one or more of the Table 10 references listed below because: all the references relate to computing devices used for communication; using the techniques of the Table 10 references would have improved the primary or obviousness references in the same

way (for example, by adding a Bluetooth connection between devices); and applying the techniques of the Table 10 references to improve primary or obviousness references would have yielded predictable results.

Reference	Disclosure
International Patent Application No. WO 01/29731 to Thompson et al. ("Thompson")	*See, e.g.*, Thompson at Figs. 1-5; Abstract; 2:11-29; 2:30-3:8; 3:34-4:17; 4:18-36; 7:6-19; 8:7-17; 15:1-20
U.S. Patent No. 7,984,488 to Cross et al. ("Cross")	*See, e.g.*, Cross at Figs. 1, 7; 1:18-26; 2:46-67; 3:13-37; 3:40-57; 4:4-19
U.S. Patent No. 7,603,556 to Brown et al. ("Brown")	*See, e.g.*, Brown at Figs. 1-2, 4, 7:67-8:15; 12:46-61; 13:43-54
U.S. Patent No. 7,849,313 to Klassen et al. ("Klassen")	*See, e.g.*, Klassen at Figs. 1, 5-6; 8:7-27; 9:63-10:4
U.S. Patent No. 8,831,576 to Munje et al. ("Munje")	*See, e.g.*, Munje at Figs. 1, 3, 6; 6:44-53; 7:19-34
U.S. Patent No. 7,012,503 to Nielsen et al. ("Nielsen")	*See, e.g.*, Nielsen at Figs. 2a-b, 3, 5a-b, 6a-c, 7b; 4:1-23; 6:8-16; 10:25-44; 11:63-12:2
U.S. Patent App. No. 2006/0031913 ("Pulitzer")	*See, e.g.*, Pulitzer at [0004]; [0038]; Fig. 4
U.S. Patent App. No. 2004/0255034 ("Choi")	*See, e.g.*, Choi at [0069-]-[0071]; [0095]; [0111]-[0117]; [0128]; [0141]
U.S. Patent No. 7,562,218 ("Kirkup")	*See, e.g.*, Kirkup at 7:1-27

Reference	Disclosure
Int. Patent App. WO 02/25890 ("Hind")	*See, e.g.*, Hind at 16:18-31; 12:8-12; 30:31-31:4; 29:13-30:18

Table 11: "wherein the off-line communication prevents eavesdropping of the service activation code"

Dependent claims 27 and 40 of the '619 patent recite "wherein the off-line communication prevents eavesdropping of the service activation code." To the extent SEVEN alleges this limitation is missing in any of the references charted in Exhibit 619-A, such a limitation would have been obvious to a person of ordinary skill in the art at the time of the alleged invention. Maintaining the secure transfer of a service activation code to pair two devices would have motivated a person of skill in the art to require the off-line communication between two devices, such as a local connection. *See, e.g.*, Thompson at 4:7-15; Cross at 2:46-67; Brown at 12:46-61; Klassen at 9:63-10:4; Hind at 30:31-31:4. Off-line communications necessarily prevents eavesdropping by not being on an open network. Because little or no complexity was involved in including a feature to transfer a service activation code in an off-line communication, one of ordinary skill in the art would have found the feature obvious as shown below.

As of the alleged '619 patent priority date, off-line communications were well known and commonplace in the art. Numerous systems and publications, including those described in Exhibit 619-A, disclosed "wherein the off-line communication prevents eavesdropping of the service activation code". *See, e.g.*, Thompson at 4:7-15; Cross at 2:46-67; Brown at 12:46-61; Klassen at 9:63-10:4; Hind at 30:31-31:4.

For these reasons, the "wherein the off-line communication prevents eavesdropping of the service activation code" limitation is anticipated by the references listed in Exhibit 619-A or, to the extent not anticipated, obvious to one of ordinary skill in the art at the time the invention described in the '619 patent was made. To the extent a primary or obviousness reference does not disclose this limitation, one of ordinary skill in the art would be motivated to combine the

primary or obviousness references with any one or more of the Table 11 references listed below because: all the references relate to computing devices used for communication; using the techniques of the Table 11 references would have improved the primary or obviousness references in the same way (for example, by adding a Bluetooth connection between devices); and applying the techniques of the Table 11 references to improve primary or obviousness references would have yielded predictable results.

Reference	**Disclosure**
International Patent Application No. WO 01/29731 to Thompson et al. ("Thompson")	*See, e.g.*, Thompson at Figs. 1-5; Abstract; 2:11-29; 2:30-3:8; 3:34-4:17; 4:18-36; 7:6-19; 8:7-17; 15:1-20
U.S. Patent No. 7,984,488 to Cross et al. ("Cross")	*See, e.g.*, Cross at Figs. 1, 7; 1:18-26; 2:46-67; 3:13-37; 3:40-57; 4:4-19
U.S. Patent No. 7,603,556 to Brown et al. ("Brown")	*See, e.g.*, Brown at Figs. 1-2, 4, 7:67-8:15; 12:46-61; 13:43-54
U.S. Patent No. 7,849,313 to Klassen et al. ("Klassen")	*See, e.g.*, Klassen at Figs. 1, 5-6; 7:39-59
U.S. Patent No. 8,831,576 to Munje et al. ("Munje")	*See, e.g.*, Munje at Figs. 1, 3, 6; 2:3-8; 6:44-53; 7:19-34
U.S. Patent No. 7,012,503 to Nielsen et al. ("Nielsen")	*See, e.g.*, Nielsen at Figs. 2a-b, 3, 5a-b, 6a-c, 7b; 4:1-23; 6:8-16; 10:25-44; 11:63-12:2
U.S. Patent App. No. 2006/0031913 ("Pulitzer")	*See, e.g.*, Pulitzer at [0004]; [0038]; Fig. 4
U.S. Patent App. No.	*See, e.g.*, Choi at [0069-]-[0071]; [0095]; [0111]-[0117]; [0128]; [0141]

Reference	Disclosure
2004/0255034 ("Choi")	
U.S. Patent No. 7,562,218 ("Kirkup")	*See, e.g.*, Kirkup at 7:1-27
Int. Patent App. WO 02/25890 ("Hind")	*See, e.g.*, Hind at 16:18-31; 12:8-12; 30:31-31:4; 29:13-30:18

Table 12: "wherein the authentication of the device relies on the authentication of the messaging account"

Asserted dependent claims 27 and 41 of the '619 patent recite "wherein the authentication of the device relies on the authentication of the messaging account." To the extent SEVEN alleges this limitation is missing in any of the references charted in Exhibit 619-A, such a limitation would have been obvious to a person of ordinary skill in the art at the time of the alleged invention. Maintaining secure access to a messaging account would have motivated a person of skill in the art to require the registration of a device to access a messaging account. *See, e.g.*, Thompson at 9:30-10:15 ("This access control protocol allows users to access their files on a common computer shared with multiple users. E-mail files are optionally loaded directly down to the PDA once the identification authorization has been made. Additionally, a user could use a traveling work station in which he was only required to carry his PDA containing the appropriate identification information to request from the network server the user's standard desktop and access to the user's e-mail files. As a result, a traveler could go to a foreign office or another work site location, plug his PDA into the control port and be granted access to the computer with the same restrictions and limitations that he may have had at his workstation at home."); Cross at 2:46-67; Munje at 4:26-5:4; Little at [0044]; Hind at 17:17-31. A person of ordinary skill in the art would know that it is not secure to allow a device access to a messaging account without a way to verify that the device has the rights to access the messaging account. *See, e.g.*, Thompson at 9:30-10:15; Cross at 2:46-67; Munje at 4:26-5:4; Little at [0044]; Hind at 17:17-31. Because little or no complexity was involved in including the feature of requiring that a device be registered before accessing a messaging account, one of ordinary skill in the art would have found the feature obvious as shown below.

As of the alleged ’619 patent priority date, requiring that a device be registered before accessing a messaging account was well known and commonplace in the art. *See, e.g.*, Thompson at 9:30-10:15; Cross at 2:46-67; Munje at 4:26-5:4; Little at [0044]; Hind at 17:17-31. Numerous systems and publications, including those described in Exhibit 619-A, disclosed “wherein the authentication of the device relies on the authentication of the messaging account”.

For these reasons, the “wherein the authentication of the device relies on the authentication of the messaging account” limitation is anticipated by the references listed in Exhibit 619-A or, to the extent not anticipated, obvious to one of ordinary skill in the art at the time the invention described in the ’619 patent was made. To the extent a primary or obviousness reference does not disclose this limitation, one of ordinary skill in the art would be motivated to combine the primary or obviousness references with any one or more of the Table 12 references listed below because: all the references relate to computing devices used for communication; using the techniques of the Table 12 references would have improved the primary or obviousness references in the same way; and applying the techniques of the Table 12 references to improve primary or obviousness references would have yielded predictable results.

Reference	**Disclosure**
International Patent Application No. WO 01/29731 to Thompson et al. (“Thompson”)	*See, e.g.*, Thompson at Figs. 1-5; Abstract; 8:18-35; 9:30-10:15; 15:1-20
U.S. Patent No. 7,984,488 to Cross et al. (“Cross”)	*See, e.g.*, Cross at Figs. 1, 7; 1:18-26; 2:46-67; 3:13-37; 3:40-57; 4:4-19
U.S. Patent No. 7,603,556 to Brown et al. (“Brown”)	*See, e.g.*, Brown at Figs. 1-2, 4, 4:63-5:2; 7:64-9:17; 10:40-11:4

Reference	Disclosure
U.S. Patent No. 8,831,576 to Munje et al. ("Munje")	*See, e.g.*, Munje at Figs. 1, 3, 6; 4:26-5:4; 3:1-17; 4:60-5:16; 5:65-6:11; 6:44-7:61
U.S. Patent App. No. 2004/0205248 to Little et al. ("Little")	*See, e.g.*, Little at [0044], [0031], [0078], [0105], Fig. 2, Fig. 3, Fig. 8.
U.S. Patent No. 7,921,209 ("Hammell")	*See, e.g.*, Hammell at Abstract; 4:13-40; 8:5-14; 9:57-10:18
U.S. Patent Pub. No. 2005/0060551 ("Barchi")	*See, e.g.*, Barchi at [0008]; [0044]-[0045]; [0059]
JP Patent Pub. No. JP2002288059A ("Kazuo")	*See, e.g.*, Machine Translation of Kazuo at pages 8-9. Kazuo at p. 8 ("This computer 15 determines a PIN code etc. for every (every [in this case,] employee) user, and sets usage rights, especially when shared by the unspecified number in the plant|facility which may exclude the use of those other than the its use person, and has public responsibility, such as a hotel, like a present Example, it is good also as a setting which does not define the usage rights of computer itself. When these usage rights are set, it is necessary to perform authentication which confirms the presence or absence of these usage rights at the time of computer starting, etc. It is easily controllable by how many authentication information, such as a PIN code, is issued whether several usage rights of whether to set one usage rights to the one computer 15 are set.") Kazuo at pp. 8-9 ("As required account information, it is account (mail) and a password, and when usage rights are set to the computer which is due to be borrowed from others, the PIN code for user individual authentications is needed beforehand. A PIN code is set for every employee, Comprising: It is used for the corresponding compatible confirmation about the usage rights of the computer 15 and the USB key 10 which the said employee uses.")
U.S. Patent Pub. No. 2003/0101343 ("Eaton")	*See, e.g.*, Eaton at [0008]; [0028]; [0094]; Fig. 2
Int. Patent App. WO 02/25890 ("Hind")	*See, e.g.*, Hind at 17:17-31; 12:8-12

Table 13: "wherein the authentication of the messaging account includes a username and password"

Asserted dependent claims 28 and 42 of the '619 patent recite "wherein the authentication of the messaging account includes a username and password." To the extent SEVEN alleges this limitation is missing in any of the references charted in Exhibit 619-A, such a limitation would have been obvious to a person of ordinary skill in the art at the time of the alleged invention. Maintaining secure access to a messaging account would have motivated a person of skill in the art to include a username and password requirement to access a messaging account. *See, e.g.*, Little at [0078] ("E-mail messages such as 833 normally use traditional SMTP, RFC822 headers and MIME body parts to define the format of the e-mail message. These techniques are all well known to one in the art. The e-mail message 833 arrives at the message server 820, which determines into which mailboxes 819 the e-mail message 833 should be stored. As described above, a message such as the e-mail message 833 may include a user name, a user account, a mailbox identifier, or other type of identifier that may be mapped to a particular account or associated mailbox 819 by the message server 820. For an e-mail message 833, recipients are typically identified using e-mail addresses corresponding to a user account and thus a mailbox 819."); Hammell at Abstract; 4:13-40; 8:5-14; 9:57-10:18; Nielsen at Figs. 2a-b, 3, 5a-b, 6a-c, 7b; 3:48-63; 6:23-28; 15:14-22. A person of ordinary skill in the art would know that a username and password is an additional level of security when allowing a device access to a messaging account. *See, e.g.*, Little at [0078]; Hammell at Abstract; 4:13-40; 8:5-14; 9:57-10:18; Nielsen at Figs. 2a-b, 3, 5a-b, 6a-c, 7b; 3:48-63; 6:23-28; 15:14-22. Because little or no complexity was involved in requiring a username and password to authenticate a messaging account, one of ordinary skill in the art would have found the feature obvious as shown below.

As of the alleged ’619 patent priority date, requiring that a device be registered before accessing a messaging account was well known and commonplace in the art. *See, e.g.*, Little at [0078]; Hammell at Abstract; 4:13-40; 8:5-14; 9:57-10:18; Nielsen at Figs. 2a-b, 3, 5a-b, 6a-c, 7b; 3:48-63; 6:23-28; 15:14-22. Numerous systems and publications, including those described in Exhibit 619-A, disclosed “wherein the authentication of the messaging account includes a username and password”.

For these reasons, the “wherein the authentication of the messaging account includes a username and password” limitation is anticipated by the references listed in Exhibit 619-A or, to the extent not anticipated, obvious to one of ordinary skill in the art at the time the invention described in the ’619 patent was made. To the extent a primary or obviousness reference does not disclose this limitation, one of ordinary skill in the art would be motivated to combine the primary or obviousness references with any one or more of the Table 13 references listed below because: all the references relate to computing devices used for communication; using the techniques of the Table 13 references would have improved the primary or obviousness references in the same way (for example, by requiring a username and password); and applying the techniques of the Table 13 references to improve primary or obviousness references would have yielded predictable results.

Reference	**Disclosure**
International Patent Application No. WO 01/29731 to Thompson et al. (“Thompson”)	*See, e.g.*, Thompson at Figs. 1-5; Abstract; 2:11-29; 2:30-3:7; 4:18-37; 8:18-35; 9:30-10:15; 15:1-20
U.S. Patent No. 7,603,556 to Brown et al. (“Brown”)	*See, e.g.*, Brown at Figs. 1-2, 4, 4:63-5:2; 7:64-9:17; 10:40-11:4

Reference	Disclosure
U.S. Patent No. 7,849,313 to Klassen et al. ("Klassen")	*See, e.g.*, Klassen at Figs. 1, 5-6; 12:19-28
U.S. Patent App. No. 2004/0205248 to Little et al. ("Little")	*See, e.g.*, Little at [0044], [0031], [0078], [0105], Fig. 2, Fig. 3, Fig. 8.
U.S. Patent No. 7,012,503 to Nielsen et al. ("Nielsen")	*See, e.g.*, Nielsen at Figs. 2a-b, 3, 5a-b, 6a-c, 7b; 3:48-63; 6:23-28; 15:14-22
U.S. Patent No. 7,921,209 ("Hammell")	*See, e.g.*, Hammell at Abstract; 4:13-40; 8:5-14; 9:57-10:18
U.S. Patent Pub. No. 2005/0060551 ("Barchi")	*See, e.g.*, Barchi at [0008]; [0044]-[0045]; [0059]
JP Patent Pub. No. JP2002288059A ("Kazuo")	*See, e.g.*, Machine Translation of Kazuo at pages 8-9. Kazuo at p. 8 ("This computer 15 determines a PIN code etc. for every (every [in this case,] employee) user, and sets usage rights, especially when shared by the unspecified number in the plant|facility which may exclude the use of those other than the its use person, and has public responsibility, such as a hotel, like a present Example, it is good also as a setting which does not define the usage rights of computer itself. When these usage rights are set, it is necessary to perform authentication which confirms the presence or absence of these usage rights at the time of computer starting, etc. It is easily controllable by how many authentication information, such as a PIN code, is issued whether several usage rights of whether to set one usage rights to the one computer 15 are set.") Kazuo at pp. 8-9 ("As required account information, it is account (mail) and a password, and when usage rights are set to the computer which is due to be borrowed from others, the PIN code for user individual authentications is needed beforehand. A PIN code is set for every employee, Comprising: It is used for the corresponding compatible confirmation about the usage rights of the computer 15 and the USB key 10 which the said employee uses.")
U.S. Patent Pub. No. 2003/0101343 ("Eaton")	*See, e.g.*, Eaton at [0008]; [0028]; [0094]; Fig. 2

Table 14: "wherein the encryption key is closely related to the service activation code"

Asserted dependent claims 32 and 46 of the '619 patent recite "wherein the encryption key is closely related to the service activation code." To the extent SEVEN alleges this limitation is missing in any of the references charted in Exhibit 619-A, such a limitation would have been obvious to a person of ordinary skill in the art at the time of the alleged invention. Maintaining the secure transfer of the messages of a messaging account would have motivated a person of skill in the art to require the encryption of any message that is transmitted from one device to another, and further to have an activation code and encryption key be closely related such that the same device is doing the encryption for added security. *See, e.g.*, Thompson at 2:11-29 ("Examples of computer data felt to require access control include secure files, personalized e-mail accounts, specific user profiles, specific network profiles, and access to licensed programs. A secure file may be created by a user encrypting the file with a password. E-mail accounts obtain limited security by archiving data into personalized data structures or by password protecting e-mail access."); Cross at 1:18-26 ("Various types of encryption schemes are widely used to secure data (e.g., an email message or file) for communication over a network. For example, in symmetric encryption, both the user that is encrypting data and the user that is decrypting the data need copies of the same encryption key. Asymmetric encryption, also known as public key encryption, uses key pairs (e.g., a public key and a private key). In asymmetric encryption the public keys may be shared but the private keys are not."); Brown at Abstract; Klassen at ABSTRACT; Little at [0037]; Hind at 17:9-17. Because little or no complexity was involved in requiring that an encryption key and service activation code be closely related or issued by the same device, one of ordinary skill in the art would have found the feature obvious as shown below.

As of the alleged ’619 patent priority date, encrypting a message was well known and commonplace in the art. *See, e.g.*, Thompson at 2:11-29; Cross at 1:18-26; Brown at Abstract; Klassen at ABSTRACT; Little at [0037]; Hind at 17:9-17. Numerous systems and publications, including those described in Exhibit 619-A, disclosed “wherein the encryption key is closely related to the service activation code”.

For these reasons, the “wherein the encryption key is closely related to the service activation code” limitation is anticipated by the references listed in Exhibit 619-A or, to the extent not anticipated, obvious to one of ordinary skill in the art at the time the invention described in the ’619 patent was made. To the extent a primary or obviousness reference does not disclose this limitation, one of ordinary skill in the art would be motivated to combine the primary or obviousness references with any one or more of the Table 14 references listed below because: all the references relate to computing devices used for communication; using the techniques of the Table 14 references would have improved the primary or obviousness references in the same way; and applying the techniques of the Table 14 references to improve primary or obviousness references would have yielded predictable results.

Reference	**Disclosure**
International Patent Application No. WO 01/29731 to Thompson et al. (“Thompson”)	*See, e.g.*, Thompson at Figs. 1-5; 2:11-29
U.S. Patent No. 7,984,488 to Cross et al. (“Cross”)	*See, e.g.*, Cross at Figs. 1, 7; 1:18-26; 2:46-67; 3:13-37; 3:40-57; 3:51-58; 4:4-19
U.S. Patent No. 7,603,556 to Brown et al. (“Brown”)	*See, e.g.*, Brown at Figs. 1; -2, 4, 8:16-23; 8:46-58; 8:65-9:17; Abstract; Summary; 12:46-61

Reference	Disclosure
U.S. Patent No. 7,849,313 to Klassen et al. ("Klassen")	*See, e.g.*, Klassen at Figs. 1, 5-6; Abstract; 2:46-59; 2:60-3:22; 6:16-35; 7:27-46; 7:60-8:6; 8:7-27; 10:47-62; 11:57-12:11; 10:45-54; 12:1-9
U.S. Patent No. 8,831,576 to Munje et al. ("Munje")	*See, e.g.*, Munje at Figs. 1, 3, 6; 3:1-17; 4:60-5:16; 5:65-6:11; 6:44-7:61
U.S. Patent App. No. 2004/0205248 to Little et al. ("Little")	*See, e.g.*, Little at [0037], [0031], [0078], [0105], Fig. 2, Fig. 3, Fig. 8.
U.S. Patent No. 7,012,503 to Nielsen et al. ("Nielsen")	*See, e.g.*, Nielsen at Figs. 2a-b, 3, 5a-b, 6a-c, 7b; 20:55-63
U.S. Patent No. 7,921,209 ("Hammell")	*See, e.g.*, Hammell at Abstract; 4:13-40; 8:5-14; 9:57-10:18
U.S. Patent No. 9,020,854 ("Giobbi")	*See, e.g.*, Giobbi at 7:16-33
Int. Patent App. WO 02/25890 ("Hind")	*See, e.g.*, Hind at 17:9-17; 6:28-7:8; 15:10-13; 20:12-13; 30:5-12; 30:31-31:4; 36:13-28

Table 15: "store an association between at least two of the encryption key, the messaging account, an identifier of the remote device, and the service activation code"

Asserted dependent claim 33 of the '619 patent recites "store an association between at least two of the encryption key, the messaging account, an identifier of the remote device, and the service activation code." To the extent SEVEN alleges this limitation is missing in any of the references charted in Exhibit 619-A, such a limitation would have been obvious to a person of ordinary skill in the art at the time of the alleged invention. Maintaining secure access to a messaging account would have motivated a person of skill in the art to require the storage and association of various identifiers and encryption data. *See, e.g.,* Cross at 2:46-67 ("Briefly, credential roaming may be implemented to synchronize local credentials (encryption keys, certificates, tokens, etc.) at any number (n) of computing devices. For purposes of illustration, a user may change, modify, add and/or remove credentials at his or her laptop or desktop computer. When the user logs out of the laptop or desktop computer, a management service synchronizes the local credentials with a remote cache."); Brown at Abstract; Klassen at ABSTRACT; Munje at 3:1-17; Little at [0037]; Hind at 16:18-31. A person of ordinary skill in the art would know that multiple steps and pieces to encryption and identifications when creating a secure messaging account would be advantageous in maintaining the security of the messaging account. *See, e.g.,* Cross at 2:46-67; Brown at Abstract; Klassen at ABSTRACT; Munje at 3:1-17; Little at [0037]; Hind at 16:18-31. Because little or no complexity was involved in including the feature of requiring that various identifiers and encryption data be associated when maintaining the security of a messaging account, one of ordinary skill in the art would have found the feature obvious as shown below.

As of the alleged '619 patent priority date, requiring the association of various identifiers and encryption data to maintain the security of a communication between two devices was well

known and commonplace in the art. *See, e.g.,* Cross at 2:46-67; Brown at Abstract; Munje at 3:1-17; Little at [0037]; Hind at 16:18-31. Numerous systems and publications, including those described in Exhibit 619-A, disclosed "store an association between at least two of the encryption key, the messaging account, an identifier of the remote device, and the service activation code".

For these reasons, the "store an association between at least two of the encryption key, the messaging account, an identifier of the remote device, and the service activation code" limitation is anticipated by the references listed in Exhibit 619-A or, to the extent not anticipated, obvious to one of ordinary skill in the art at the time the invention described in the '619 patent was made. To the extent a primary or obviousness reference does not disclose this limitation, one of ordinary skill in the art would be motivated to combine the primary or obviousness references with any one or more of the Table 15 references listed below because: all the references relate to computing devices used for communication; using the techniques of the Table 15 references would have improved the primary or obviousness references in the same way; and applying the techniques of the Table 15 references to improve primary or obviousness references would have yielded predictable results.

Reference	**Disclosure**
International Patent Application No. WO 01/29731 to Thompson et al. ("Thompson")	*See, e.g.*, Thompson at Figs. 1-5; Abstract; 2:11-29; 2:30-3:7; 4:18-37; 8:18-35; 9:30-10:15; 15:1-20
U.S. Patent No. 7,984,488 to Cross et al. ("Cross")	*See, e.g.*, Cross at Figs. 1, 7; 1:18-26; 2:46-67; 3:13-37; 3:40-57; 3:51-58; 4:4-19

Reference	Disclosure
U.S. Patent No. 7,603,556 to Brown et al. ("Brown")	*See, e.g.*, Brown at Figs. 1; -2, 4, Abstract; Summary; 8:16-9:18; 12:46-61
U.S. Patent No. 7,849,313 to Klassen et al. ("Klassen")	*See, e.g.*, Klassen at Figs. 1, 5-6; Abstract; 2:46-59; 2:60-3:22; 6:16-35; 7:27-46; 7:60-8:6; 8:7-27; 10:47-62; 11:57-12:11; 10:48-62.; 14:15-19; 14:60-67
U.S. Patent No. 8,831,576 to Munje et al. ("Munje")	*See, e.g.*, Munje at Figs. 1, 3, 6; 3:1-17; 4:60-5:16; 5:65-6:11; 6:44-7:61
U.S. Patent App. No. 2004/0205248 to Little et al. ("Little")	*See, e.g.*, Little at [0037], [0031], [0078], [0105], Fig. 2, Fig. 3, Fig. 8.
U.S. Patent No. 7,012,503 to Nielsen et al. ("Nielsen")	*See, e.g.*, Nielsen at Figs. 2a-b, 3, 5a-b, 6a-c, 7b; 17:56-18:20; 18:39-51
U.S. Patent No. 7,921,209 ("Hammell")	*See, e.g.*, Hammell Abstract; 4:13-40; 8:5-14; 9:57-10:18
U.S. Patent No. 7,562,218 ("Kirkup")	*See, e.g.*, Kirkup at 4:51-59
U.S. Patent Pub. No. 2003/0101343 ("Eaton")	*See, e.g.*, Eaton at [0008]; [0027]-[0028]; [0094]; Fig. 2
Int. Patent App. WO 02/25890 ("Hind")	*See, e.g.*, Hind at 16:18-31; 24:12-18; 15:10-13; 20:12-13; 30:5-12; 30:31-31:4; 36:13-28; 41:7-12

Table 16: "wherein a control message is received from the remote device upon user interaction with the message"

Dependent claims 36, 50 and 52 of the '619 patent recite "wherein a control message is received from the remote device upon user interaction with the message." To the extent SEVEN alleges this limitation is missing in any of the references charted in Exhibit 619-A, such a limitation would have been obvious to a person of ordinary skill in the art at the time of the alleged invention. Market forces and other consumer trends to more secure transmission of data would have motivated a person of ordinary skill to include in a device a control message to show that a message was received by a device and/or seen by a user. As the security between the transfer of data between two devices became more important with the advent of the internet and networks, one of ordinary skill in the art would have been motivated to use control data to confirm that a message had been received, wherein user input related to the message being a secure way to guarantee a message was received by a user. *See, e.g.*, Klassen at 14:1-14 ("The messaging application 160 on the first mobile device 10A recognizes the acceptance message, either on receipt or once the user opens the message, and it extracts the second public key EB from the acceptance message in step 324. In step 326, the messaging application 160 encrypts the PIN for the initiating mobile device 10A (i.e. PINA) in accordance with the predefined encryption transformation or function. The messaging application 160 then composes an acknowledgement message in step 328 for transmission through one of the communication applications 162, such as an e-mail application. The acknowledgement message includes the encrypted PINA, which may be embedded or attached to the acknowledgement message. The acknowledgement message is then sent to the second mobile device 10B in step 330."); Munje at 7:62-8:23; Braley at Abstract; [001]; [006]-[008]; [017]-028]; Dutordoir at [0005]-[0010]; Ekdahl at Abstract; [0003]; [0007]; [0018]; [0023]-[0026]; [0029]-[0030]; [0033]-[0036]; Figs.

1, 2. Further, it would have been obvious to one of skill in the art to include a control message, like a read-receipt, for confirmation that a message had been received. *See, e.g.*, Klassen at 14:1-14; Munje at 7:62-8:23; Braley at Abstract; [001]; [006]-[008]; [017]-028]; Dutordoir at [0005]-[0010]; Ekdahl at Abstract; [0003]; [0007]; [0018]; [0023]-[0026]; [0029]-[0030]; [0033]-[0036]; Figs. 1, 2. Because little or no complexity was involved in including these features and functionalities on computing devices, one of ordinary skill in the art would have found the requirement to include the sending of a control message based on user input at the recipient device obvious as shown below.

As of the alleged '619 patent priority date, the requirement of user input prior to the near-field wireless transfer of secure data between two devices was well known and commonplace in the art. *See, e.g.*, Klassen at 14:1-14; Munje at 7:62-8:23; Braley at Abstract; [001]; [006]-[008]; [017]-028]; Dutordoir at [0005]-[0010]; Ekdahl at Abstract; [0003]; [0007]; [0018]; [0023]-[0026]; [0029]-[0030]; [0033]-[0036]; Figs. 1, 2. Numerous systems and publications, including those described in Exhibit 619-A, disclosed "wherein a control message is received from the remote device upon user interaction with the message".

For these reasons, the "wherein a control message is received from the remote device upon user interaction with the message" limitation is anticipated by the references listed in Exhibit 619-A or, to the extent not anticipated, obvious to one of ordinary skill in the art at the time the invention described in the '619 patent was made. To the extent a primary or obviousness reference does not disclose this limitation, one of ordinary skill in the art would be motivated to combine the primary or obviousness references with any one or more of the Table 16 references listed below because: all the references relate to the secure transfer and access to data; using the techniques of the Table 16 references would have improved the primary or

obviousness references in the same way (for example, by adding an IR port to a device or a "send" button on a remote device); and applying the techniques of the Table 16 references to improve primary or obviousness references would have yielded predictable results.

Reference	Disclosure
International Patent Application No. WO 01/29731 to Thompson et al. ("Thompson")	*See, e.g.*, Thompson at Figs. 1-5; Abstract; 8:7-17; 15:1-20
U.S. Patent No. 7,603,556 to Brown et al. ("Brown").	*See, e.g.*, Brown at Figs. 1; -2, 4, Abstract; Summary; 8:16-9:18; 12:46-61
U.S. Patent No. 7,849,313 to Klassen et al. ("Klassen")	*See, e.g.*, Klassen at Figs. 1, 5-6; 11:33-44; 13:46-53; 14:1-14
U.S. Patent No. 8,831,576 to Munje et al. ("Munje")	*See, e.g.*, Munje at Figs. 1, 3, 6; 7:62-8:23
U.S. Patent App. No. 2004/0255034 ("Choi")	*See, e.g.*, Choi at [0069-]-[0071]; [0095]; [0111]-[0117]; [0128]; [0141]
U.S. Patent App. No. 2006/0135064 ("Cho")	*See, e.g.*, Cho at Fig. 2; Abstract; [0026]; [0028]; [0038]; [0040]; [0043]; [0045]; [0059]; Claim 1, 9
Int. App. WO 2005/002174 ("Braley")	*See, e.g.*, Braley at Abstract; [001]; [006]-[008]; [017]-028]
European Patent EP 1 578 093 ("Ekdahl")	*See, e.g.*, Ekdahl at Abstract; [0003]; [0007]; [0018]; [0023]-[0026]; [0029]-[0030]; [0033]-[0036]; Figs. 1, 2
U.S. Patent App. No. 2006/0031913 ("Pulitzer")	*See, e.g.*, Pulitzer at [0004]; [0038]; Fig. 4
U.S. Patent No. 7,174,368 ("Ross")	*See, e.g.*, Ross at 9:28-40; 13:32-39; 16:45-65

Reference	Disclosure
U.S. Patent Pub. No. 2004/0186884 ("Dutordoir")	*See, e.g.*, Dutordoir at [0005]-[0010]