EXHIBIT B

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

AGIS SOFTWARE DEVELOPMENT LLC, Plaintiff, v. APPLE INC., Defendant.	Civil Action No. 2:17-cv-513-JRG (LEAD CASE) Civil Action No. 2:17-cv-516-JRG

EXPERT REPORT OF NEIL SIEGEL REGARDING THE INVALIDITY OF U.S. PATENT NOS. 9,467,838; 9,749,829; 9,408,055; AND 9,445,251

contractual wins for TRW and Northrop Grumman over the course of my career. The contracts I helped to obtain for TRW and Northrup Grumman include several system development contracts, each individually entailing total expenditures of several hundred millions dollars, to develop: the Force XXI Battle Command Brigade-and-Below ("FBCB2" or "Blue-Force Tracker") system; the Forward-Area Air Defense Systems Command, Control, and Intelligence (FAAD C2I) and derivative systems (including the Air and Missile Defense Work-Station, and the Tactical High-Energy Laser, the world's first complete laser weapon); U.S. Army's Tactical Operations Centers; the U.S. Army's Hunter Unmanned Air Vehicle System (the Army's first unmanned air vehicle); the U.S. Missile Defense Agency Joint National Integration System Research and Development Contract; the Counter Rocket, Artillery, and Mortar System; The Global Combat Service Support System, Army-Tactical; the Battlefield Airborne Communications Node; the Integrated Air-Missile Defense Battle Command System, and many others.

16. Several of the programs and products for which I have been responsible have been recognized with various awards. For example, the FBCB2 project received: the initial award from "Cross Talk: the Journal of Defense Software Engineering" as one of the top five best-managed software products within the entire United States government; the Federal 100 Monticello Award; recognition as the "Most Innovative U.S. Government Program" from the Institute for Defense & Government Advancement; and the iCMG award for best systems architecture. Likewise, the Tactical Internet project for which I was responsible was honored as the Battlespace Information "2005 program of the year." Furthermore, my systems have been credited in multiple United States and United Kingdom government documents as being responsible for saving many lives, and I have received many letters and other forms of "kudos" from active military personnel who

credit my systems with saving their lives, saving the lives of those under their command, and/or avoiding friendly-fire incidents.

17. Although most of my inventions are protected as corporate trade secrets, I have also been awarded 19 United States patents, and more than 25 international patents. Among my most-cited patents is U.S. Patent No. 6,212,559, entitled "Automated Configuration of Internet-Like Computer Networks," which forms the basis of the "Tactical Internet" that enables FBCB2 and other systems for the US military. Another of my most-cited patents is U.S. Patent No. 5,672,840, entitled "Method and apparatus for automatically orienting a computer display," which covers the now-widely-used method of aligning a map display on a hand-held device to the cardinal points; this method, invented for the U.S. Army, is now universally adopted in a wide range of commercial devices such as cell phones and tablet computers. Another of my most-cited patents is U.S. Patent No. 7,287,023, entitled "System and method for distributed network access and control enabling high availability, security, and survivability," which provided a break-through security model that enabled the first-ever large-scale fielding of a system that mixed trusted and untrusted users on the same network, and also created now widely-adopted methods of remote security administration (such as remotely erasing an electronic device that become lost or stolen) — a method that is essential for every large-scale, secure wireless network with mobile participants, and that is used in many modern smartphones and tablets. Another of my most-cited patents is U.S. Patent No. 6,904,280, entitled "Communication system with a mobile coverage area," which provides for routing methods essential for operations on a dynamic and changing battlefield, and introduces important techniques for self-adaptation of a network to changes in its user base, topology, and inter-visibility map; these conditions prevail in civil government operations (such as police, fire, ambulance, and emergency response-and-recovery operations), in addition to on the battlefield.

system to support situational awareness, and initiated two major radio programs: EPLRS, and a data upgrade to existing SINCGARS voice radios. SIEGEL000469-71. By the mid-to-late-1990's, Sigma Star was a fielded, mature military system that allowed users to obtain near-real-time situational awareness for each of the five specific battlefield functions, and to use that situational awareness to perform command and control of the appropriate military forces. Some Sigma Star units were implemented as fixed-site and mobile command posts, but others were handheld devices that could be carried around the battlefield by individual soldiers. For example, the air defense component of Sigma Star, called the Forward-Area Air Defense Command Control and Intelligence System ("FAAD C2I"), was fielded in September 1993 with both mobile command posts, and handheld devices that integrated computers, radios, and GPS receivers. *See* SIEGEL000480 (image of device). While working at TRW, the prime contractor for FAAD C2I, I was the chief engineer of the FAAD C2I system from 1989 to 1992. From 1994 to 2001, I was the director of the business unit within the company responsible for FAAD C2I, as well as for the two other Sigma Star systems for which TRW was prime contractor.

51. The U.S. Army initiated a major improvement in the Sigma Star system in 1995 (although, by that time, the Army had abandoned the name "Sigma Star"), awarding the contract for the Force XXI Battle Command Brigade-and-Below ("FBCB2" or "Blue Force Tracker") (discussed further below) to TRW. The contract for FBCB2 specified that TRW would provide a new and improved capability to the Army's maneuver force, consisting of a specialized communication system (called the "Tactical Internet") that would support situational awareness and command-and-control at the tactical echelons of war, together with computers, GPS receivers, software, and many other elements. FBCB2 was initially fielded with actual Army units in 1998. It was first used in combat in 1999, in Bosnia and Kosovo. As outlined below, I personally led the

Wifi, cellular telephones, and satellite communications, and mixtures of these types of communications devices.

B. Overview of the Force XXI Battle Command Brigade-and-Below ("FBCB2" or "Blue Force Tracker") System

56. Well before September 20, 2004, the FBCB2 system developed by my company, TRW, exemplified the state of the art in situational awareness technology. FBCB2 was a wireless network of computers, radios, routers, and powerful software. FBCB2 told soldiers where they were, where the friendly forces were, where the enemy was, where threats or obstacles were, and what the commander's operational orders were. By September 20, 2004, FBCB2 was the centerpiece of situational awareness technology and the specialized communications systems needed for situational awareness and command-and-control within the US military.

1. The Development and Deployment of FBCB2

57. TRW began performing research for FBCB2 in 1992. The US Army released a formal request-for-proposals to develop the FBCB2 system in 1994. Multiple contractors bid on the project, and the contract was awarded to TRW in January 1995. *See* SIEGEL000006.

58. I personally led and oversaw the development of FBCB2 from the beginning, starting with the 1992 research project, and continued to do so for many years, through 2004. From 1989 to 2002, I was the chief engineer of the FAAD C2I system that TRW (since acquired by Northrop Grumman) developed for the U.S. Army. The FAAD C2I system was in many ways a pathfinder system for FBCB2, in that it provided real-time situational awareness and command-and-control over a suitable communications system for the subset of U.S. Army tactical forces that comprised the Air Defense branch of the Army. FAAD C2I also included a hand-held computer that included a computer, GPS, north-finding device, and radio, and thereby provided situational awareness, command-and-control, and emergency communications for individual soldiers. The

via mathematical manipulation, to and from latitude and longitude) to the server, and the server broadcast that information to other FBCB2 devices. *See* SIEGEL000009-10. SIEGEL000014; SIEGEL000782. The recipient FBCB2 devices displayed the location information of the sender devices as symbols on the georeferenced maps at the appropriate latitude and longitude. *See* SIEGEL000009-10. Each FBCB2 device continuously reported new location to the server. *See* SIEGEL000009-10; SIEGEL000014. The location reporting rate was time and distance triggered, such that a device would send updated location information at a predetermined time interval, unless it moved further than a pre-specified distance before that time interval had passed. APL-AGIS_00012859. U.S. Patent No. 5,672,840, of which I am named inventor, describes the reporting filter incorporated in the FAAD C2I system based on an angular filter (e.g., reporting whenever the display was rotated more than a certain amount). *See also* SIEGEL000374 at 5:31-35. In FBCB2 (starting in 1995), that concept was extended from a filter for reporting based an angular threshold to one of a threshold based on time and motion. *See* SIEGEL000990-91. The information that passed the time-motion filter was the information that was continuously broadcast to other FBCB2 devices, and the updated information was automatically plotted on each FBCB2 device's georeferenced map. *See* SIEGEL000009-10; SIEGEL000305.

71. The servers in FBCB2 consisted of computers mounted in army vehicles. That is, individual FBCB2 units were designated to receive information from FBCB2 devices and forward it to other FBCB2 devices. Because users moved around and access to a particular server could be blocked by buildings, mountains, jamming, or other difficulties, there was not a single, static server designation in FBCB2 as there typically is in an office or consumer computer network. Instead, FBCB2 devices were programmed to collaborate and *dynamically* select one of their number to act as the server. If the unit acting as a server became unavailable for some reason—

83. As a further example of remote control, an FBCB2 user could remotely "challenge" another, remote FBCB2 device (i.e., require the user of that remote FBCB2 unit to re-enter their log-in credentials; they might do this, for example, if they suspect that that particular FBCB2 unit has been captured by the enemy), or could engage in other remote-control operations such as: locking the remote FBCB2 unit (i.e., logging its user out); forcing the user at that unit to re-enter their log-in credentials; or erasing the hard drive of the remote unit. *See* APL-AGIS_00012860. These features are described in detail in U.S. Pat. No. 7,278,023, of which I am a named inventor. *See, e.g.*, SIEGEL000400-417 (the "'023 patent") at 6:56-63; 8:15-9:23; 9:24-9:46. My team at TRW developed this patent as part of our work on FBCB2, and we incorporated many of the capabilities outlined in the patent in FBCB2. The '023 patent covers a method for administering access and security on a network. '023 pat. at 3:22-24. Among other things, the system includes a "remote control module . . . provided so that the systems administrator or security officer may take the appropriate action when certain events transpire." '023 pat. at 6:56-63. The patent discloses that a system administrator or security officer may send a challenge message to a user's device. '023 pat. at 8:15-28. Upon receipt of the message, the device presents the user's role/log in screen. '023 pat. at 8:28-44. If the user enters the wrong password or fails to enter the password, and this happens more than a pre-specified number of times, then the security administrator or officer has the option to remotely lock the device's screen or totally disable the user terminal and wipe its hard drive (among other possibilities). '023 pat. 8:28-9:23. These features were implemented as part of FBCB2 in the 1990's.

84. When sending entity location information, text messages, status messages, or remote control messages, users could choose to send the message to their entire group, to a sub-group, or to individual users. Individual recipients could be selected by touching the symbol

under a given role, their device sent a message to the FBCB2 server, identifying their role in the combat team, which served as an identifier of the group or groups in which the user needed to participate. Based on receipt of that message, the server began sharing information (position reports, orders, status information, and many other types of information) with that FBCB2 user and broadcasting that user's information to others. This set-up allowed users to switch groups from a single device (by logging in as a different role) or to seamlessly log into the right groups from different devices.

97. U.S. Patent No. 6,212,559, of which I am a named inventor, covers the process of setting up groups in FBCB2. *See* SIEGEL000333-355 (the "'559 patent"). My team at TRW developed this patent as part of our work on FBCB2, and we incorporated many of the capabilities outlined in the patent in FBCB2. The '559 patent covers techniques for configuring a computer network to allow for rapid reconfiguration due to changes in the location, identity, or network topology. *See* '559 pat. at 5:23-58. Specifically, the '559 patent discloses software consisting of network configuration tools in which each unit and user (e.g., brigade, company, fleet, ship, aircraft group) is grouped and interrelated with other units according to a "unit task organization" set up within the software. *See* '559 at 5:47-6:4. A user could use the "unit task organization" capability in order to define their desired groups. *See* '559 pat. at 5:59-6:11; *see also id*. at 7:1-4, 7:33-42. A user could also thereby define the set of users who could participate in each group. *See* '559 pat. at 8:16-24. Users could be given permissions to access more than one group. *See* '559 pat. at 7:49-67; 9:6-40. Once groups were defined, the software created a network operational database that associated each user with the groups the user had permission to join. *See* '559 pat. at 8:26-30. When a user logged into the software, the user's device would send a message seeking to participate in the group or groups to which the user was assigned, and the server would then join

the user to the groups, allowing the user to exchange location and other information with all other users in the group. These features of the '559 patent were incorporated into FBCB2, as described in the preceding paragraph.

98. The method of setting up groups in FBCB2 was tailored to meet the security and operational needs of the military (e.g., ensuring users could only join groups of the appropriate security clearance and ensuring that users could efficiently join multiple groups upon login). But the basic group-joining mechanism—of having a user send a message to a server identifying the group with which they needed to exchange communications, and being joined to the group based on receipt of that message—had long existed by September 20, 2004 and would have been familiar to a person of ordinary skill in network engineering. For example, ListServ technology had been used since the 1980's to set up ad-hoc communications networks for email. SIEGEL000514. Users signed up for an email list by sending a server the name of the list (and, optionally, a password). SIEGEL000494-96. Then, everything the user sent in the future was automatically forwarded to all other people who had signed up for the same list, and the user also received all messages sent by all of the other members of the list. Thus, if this limitation is not anticipated by FBCB2, it would have been obvious in view of FBCB2 and the knowledge of a person of ordinary skill in the art at the time of the invention.

2. "The method of claim 4, wherein the first device does not have access to the respective Internet Protocol addresses of the one or more second devices included in the group."

118. When exchanging data on the Tactical Internet using TCP/IP protocols, FBCB2 devices did not need to have access to the respective Internet Protocol addresses of the one or more second devices included in the group. Instead, when a user signed on to FBCB2 and joined a group, the FBCB2 server routed the user's messages and location information to the appropriate recipients based on the type of data being sent and/or addressee information provided by the FBCB2 user. For certain data, such as location information, the sender did not need to enter any addressee information at all, because the server broadcast the data automatically to all other members of the user's group. For other types of data, such as text messages, FBCB2 allowed users to designate particular users as recipients by specifying particular individuals or groups of individuals' log-in names, role or title, or group name (e.g. a particular platoon). This addressee information was sent to the server, and the server routed the information to the appropriate IP address. The sender never, however, had to know the IP address of the intended recipient(s).

119. U.S. Patent No. 6,212,559, (the "'559 patent") of which I am a named inventor, covers the process of setting up groups and facilitating communication among groups in FBCB2. *See* SIEGEL000333-355. My team at TRW developed this patent as part of our work on FBCB2, and we incorporated many of the capabilities outlined in the patent in FBCB2. Figure 17A of the '559 patent shows that users within a communication network were identified by a user ID; a user who was attempting to modify the network or select ot her users for communications would select those users' IDs. *See* '559 pat. Fig. 7; *id*. at 4:48-49. This feature was implemented as part of FBCB2.

1. "The method of claim 1, wherein the message including the identifier corresponding to the group is a first message, and wherein the method further comprises performing by the first device: sending, to a particular second device via the first server, a second message related to remotely controlling the particular second device to perform an action, wherein the particular second device is configured to perform the action based on receiving the second message."

152. FBCB2 allowed users to send command-and-control messages via the server that would remotely control the recipient FBCB2 device. *See* SIEGEL000006.

153. For example, an FBCB2 user could send another user a message comprising location information of an entity, and that location information would automatically be displayed on the georeferenced map of the recipient user. *See* SIEGEL000012; SIEGEL000015-16; APL-AGIS_00012847-8. As a further example, and FBCB2 user could send another user a message comprising a warning or alert that would be displayed in a scrolling marquee on the other user's touch screen. *See* SIEGEL000307 (image of FBCB2 user interface showing location of scrolling marquee). As a further example, FBCB2 commanders could identify and send users the locations of "danger" zones related to enemy fire, contamination areas, or enemy obstacles. *See* SIEGEL000016. FBCB2 devices could be programmed to play audible warnings when the device approached the location of a danger zone. *See* SIEGEL000016. Thus, a commander could cause a user's device to play a sound if the user was approaching a danger zone. *See* SIEGEL000016.

154. As a further example, an FBCB2 user could remotely "challenge" another, remote FBCB2 device (i.e., require the user of that remote FBCB2 unit to re-enter their log-in credentials; they might do this, for example, if they suspect that that particular FBCB2 unit has been captured by the enemy), or could engage in other remote-control operations such as: locking the remote FBCB2 unit (i.e., logging its user out); forcing the user at that unit to re-enter their log-in credentials; or erasing the hard drive of the remote unit. *See* APL-AGIS_00012860. These features are described in detail in U.S. Pat. No. 7,278,023, of which I am a named inventor. *See,*

e.g., SIEGEL000400-417 (the "'023 patent") at 6:56-63; 8:15-9:23; 9:24-9:46. My team at TRW developed this patent as part of our work on FBCB2, and we incorporated many of the capabilities outlined in the patent in FBCB2. The '023 patent covers a method for administering access and security on a network. '023 pat. at 3:22-24. Among other things, the system includes a "remote control module . . . provided so that the systems administrator or security officer may take the appropriate action when certain events transpire." '023 pat. at 6:56-63. The patent discloses that a system administrator or security officer may send a challenge message to a user's device. '023 pat. at 8:15-28. Upon receipt of the message, the device presents the user's role/log in screen. '023 pat. at 8:28-44. If the user enters the wrong password or fails to enter the password, and this happens more than a pre-specified number of times, then the security administrator or officer has the option to remotely lock the device's screen or totally disable the user terminal and wipe its hard drive (among other possibilities). '023 pat. 8:28-9:23. These features were implemented as part of FBCB2.

2. "The method of claim 39, wherein the second message indicates the action to be performed, and wherein the action is selected from the group consisting of playing audio, initiating a phone call, vibrating, converting text to speech, changing sound intensity, and displaying information."

155. FBCB2 could remotely control another device by causing it to play audio and display information. As described above, an FBCB2 user who sent a "danger zone" location message could cause another user's device to play audio if the user approached the danger zone. Likewise, as described above and shown in the below figure (from SIEGEL000310), a user who sent a text message consisting of a warning or alarm could cause that information to be displayed as a scrolling marquee on the recipient's screen.

could be set up by system administrators. Most groups included more than two FBCB2 users. Groups were designed to allow users who needed to share information and engage in remote control operations with each other to do so quickly and effectively. For example, a group might correspond to an organization such as all of the members of a tank platoon, or all of the members of an artillery battalion. Another type of group might be functional, that is, all of people in an area who are in the artillery branch, or all of the people in the area who are in the air-defense branch. In an actual military deployment, there would in fact be many groups of both types, in addition to other types of groups, such as a group formed of all of the people who were to be involved in a particular military operation. The FBCB2 system associated individuals and devices with roles and the groups those roles had permission to access. When an FBCB2 user logged into FBCB2 under a given role, their device sent a message to the FBCB2 server, identifying their role in the combat team, which served as an identifier of the group or groups in which the user needed to participate. Based on receipt of that message, the server began sharing information (position reports, orders, status information, and many other types of information) with that FBCB2 user and broadcasting that user's information to others. This set-up allowed users to switch groups from a single device (by logging in as a different role) or to seamlessly log into the right groups from different devices.

161. U.S. Patent No. 6,212,559, of which I am a named inventor, covers the process of setting up groups in FBCB2. *See* SIEGEL000333-355 (the "'559 patent"). My team at TRW developed this patent as part of our work on FBCB2, and we incorporated many of the capabilities outlined in the patent in FBCB2. The '559 patent covers techniques for configuring a computer network to allow for rapid reconfiguration due to changes in the location, identity, or network topology. *See* '559 pat. at 5:23-58. Specifically, the '559 patent discloses software consisting of

network configuration tools in which each unit and user (e.g., brigade, company, fleet, ship, aircraft group) is grouped and interrelated with other units according to a "unit task organization" set up within the software. *See* '559 at 5:47-6:4. A user could use the "unit task organization" capability in order to define their desired groups. *See* '559 pat. at 5:59-6:11; *see also id*. at 7:1-4, 7:33-42. A user could also thereby define the set of users who could participate in each group. *See* '559 pat. at 8:16-24. Users could be given permissions to access more than one group. *See* '559 pat. at 7:49-67; 9:6-40. Once groups were defined, the software created a network operational database that associated each user with the groups the user had permission to join. *See* '559 pat. at 8:26-30. When a user logged into the software, the user's device would send a message seeking to participate in the group or groups to which the user was assigned, and the server would then join the user to the groups, allowing the user to exchange location and other information with all other users in the group. These features of the '559 patent were incorporated into FBCB2, as described in the preceding paragraph.

162. The method of setting up groups in FBCB2 was tailored to meet the security and operational needs of the military (e.g., ensuring users could only join groups of the appropriate security clearance and ensuring that users could efficiently join multiple groups upon login). But the basic group-joining mechanism—of having a user send a message to a server identifying the group with which they needed to exchange communications, and being joined to the group based on receipt of that message—had long existed by September 20, 2004 and would have been familiar to a person of ordinary skill in network engineering. For example, ListServ technology had been used since the 1980's to set up ad-hoc communications networks for email. SIEGEL000514. Users signed up for an email list by sending a server the name of the list (and, optionally, a password). SIEGEL000494-96. Then, everything the user sent in the future was automatically

forwarded to all other people who had signed up for the same list, and the user also received all messages sent by all of the other members of the list. Thus, if this limitation is not anticipated by FBCB2, it would have been obvious in view of FBCB2 and the knowledge of a person of ordinary skill in the art at the time of the invention.

3. "participating in the group, wherein participating in the group includes sending first location information to a first server and receiving second location information from the first server, the first location information comprising a location of the first device, the second location information comprising one or more locations of one or more respective second devices included in the group;"

163. FBCB2 devices exchanged location information via a server. Each device obtained its own location from a GPS receiver attached to (or built into) the device.[9] The location information consisted of latitude and longitude coordinates determined by a GPS unit installed in the FBCB2 device. *See also* SIEGEL000009-10; SIEGEL000014; SIEGEL000782. Each device reported its latitude and longitude to the server, and the server broadcast that information to other FBCB2 devices. *See also* SIEGEL000009-10.

164. The servers in FBCB2 consisted of computers mounted in army vehicles. That is, individual FBCB2 units were designated to receive information from FBCB2 devices and forward it to other FBCB2 devices. Because users moved around and access to a particular server could be blocked by buildings, mountains, jamming, or other difficulties, there was not a single, static server designation in FBCB2 as there typically is in an office or consumer computer network. Instead, FBCB2 devices were programmed to collaborate and *dynamically* select one of their number to act as the server. If the unit acting as a server became unavailable for some reason—

[9] Location information could also be obtained by other methods, including radio triangulation of the ground-to-ground radio links or an inertial navigation system on the vehicle. The FBCB2 software automatically determined which of these was the most accurate at the moment, and used that most-accurate position as the FBCB2 position to report to the FBCB2 network.

186. U.S. Patent No. 6,212,559, of which I am a named inventor, covers the process of setting up groups in FBCB2. *See* SIEGEL000333-355 (the "'559 patent"). My team at TRW developed this patent as part of our work on FBCB2, and we incorporated many of the capabilities outlined in the patent in FBCB2. The '559 patent covers techniques for configuring a computer network to allow for rapid reconfiguration due to changes in the location, identity, or network topology. *See* '559 pat. at 5:23-58. Specifically, the '559 patent discloses software consisting of network configuration tools in which each unit and user (e.g., brigade, company, fleet, ship, aircraft group) is grouped and interrelated with other units according to a "unit task organization" set up within the software. *See* '559 at 5:47-6:4. A user could use the "unit task organization" capability in order to define their desired groups. *See* '559 pat. at 5:59-6:11; *see also id*. at 7:1-4, 7:33-42. A user could also thereby define the set of users who could participate in each group. *See* '559 pat. at 8:16-24. Users could be given permissions to access more than one group. *See* '559 pat. at 7:49-67; 9:6-40. A user with appropriate permissions could assign another user to a group at any time. The patent explains that, when such an assignment was made, the software would disseminate the assignment to the user, and the user would respond by accepting the new assignment. *See* '559 pat. at 8:31-51. These features were incorporated into FBCB2, as described in the preceding paragraph.

187. The method of setting up groups in FBCB2 was tailored to meet the security and operational needs of the military (e.g., ensuring users could only join groups of the appropriate security clearance and ensuring that commanders received acknowledgement of orders). A person of ordinary skill in the art at the time of the invention would have understood that the protocols described above could be easily modified in various ways (e.g., requiring fewer confirmations or additional confirmations before joining users to a group; allowing all users to invite each other to

join any group or to request access to any group, etc.) to suit different needs. Thus, if this limitation is not anticipated by FBCB2, it would have been obvious in view of FBCB2 and the knowledge of a person of ordinary skill in the art at the time of the invention.

3. "receiving a first message comprising a request for a first updated location of the first device, wherein the first message is sent by the second device and includes data identifying the first device; in response to receiving the first message, sending, to the first device, a second message comprising a request for the first updated location of the first device; after sending the second message, receiving a response to the second message, the response including first location information comprising the first updated location of the first device;

188. In FBCB2, members of a group continuously exchanged location information with one another. Therefore, when a second FBCB2 device requested that a first FBCB2 device join its group, the device also sent the server a message requesting up-to-date location information for the first device. In turn, when the server sent the first device the second device's request to join a group, the server also requested that the first device send its up-to-date location information. In response to that request, the first device would send its location information to the server. *See* SIEGEL000009-10; SIEGEL000014. Each device obtained its own location from a GPS receiver attached to (or built into) the device.[10] The location information consisted of latitude and longitude coordinates determined by a GPS unit installed in the FBCB2 device. *See* SIEGEL000009-10; SIEGEL000014.

[10] Location information could also be obtained by other methods, including radio triangulation of the ground-to-ground radio links or an inertial navigation system on the vehicle. The FBCB2 software automatically determined which of these was the most accurate at the moment, and used that most-accurate position as the FBCB2 position to report to the FBCB2 network.

5. "after sending the first location information and the georeferenced map data to the second device, receiving second location information comprising a second updated location of the first device and sending the second location information to the second device, wherein the second device is configured to use the server-provided georeferenced map data and the second location information to reposition the symbol on the georeferenced map at a second position corresponding to the second updated location of the first device;"

191. Each FBCB2 device continuously reported its updated location to the server. *See* SIEGEL000009-10; SIEGEL000014. The location reporting rate was time and distance triggered, such that a device would send updated location information at a predetermined time interval, unless it moved further than a pre-specified distance before that time interval had passed. *See* APL-AGIS_00012859. U.S. Patent No. 5,672,840, of which I am named inventor, describes the reporting filter incorporated in the FAAD C2I system, based on an angular filter (e.g., reporting whenever the display was rotated more than a certain amount). *See* SIEGEL000374 at 5:31-35. In FBCB2 (starting in 1995), we extended that concept of a filter for reporting based an angular threshold to one of a threshold based on time and motion. *See* SIEGEL000990-91. The information that passed the time-motion filter was continuously broadcast to other FBCB2 devices, and the updated information was automatically plotted on each FBCB2 device's georeferenced map. *See* SIEGEL000009-10; SIEGEL000305.

6. "receiving a third message related to remotely controlling the first device to perform an action, wherein the third message is sent by the second device; and after receiving the third message, sending, to the first device, a fourth message related to remotely controlling the first device to perform the action, wherein the first device is configured to perform the action based on receiving the fourth message.

192. FBCB2 allowed users to send command-and-control messages via the server that would remotely control the recipient FBCB2 device. *See* SIEGEL000006.

193. For example, an FBCB2 user could send another user a message comprising location information of an entity, and that location information would automatically be displayed

on the georeferenced map of the recipient user. *See* SIEGEL000012; SIEGEL000015-16; APL-AGIS_00012847-8. As a further example, and FBCB2 user could send another user a message comprising a warning or alert that would be displayed in a scrolling marquee on the other user's touch screen. *See* SIEGEL000307 (image of FBCB2 user interface showing location of scrolling marquee). As a further example, FBCB2 commanders could identify and send users the locations of "danger" zones related to enemy fire, contamination areas, or enemy obstacles. *See* SIEGEL000016. FBCB2 devices could be programmed to play audible warnings when the device approached the location of a danger zone. *See* SIEGEL000016. Thus, a commander could cause a user's device to play a sound if the user was approaching a danger zone. *See* SIEGEL000016.

194. As a further example, an FBCB2 user could remotely "challenge" another, remote FBCB2 device (i.e., require the user of that remote FBCB2 unit to re-enter their log-in credentials; they might do this, for example, if they suspect that that particular FBCB2 unit has been captured by the enemy), or could engage in other remote-control operations such as: locking the remote FBCB2 unit (i.e., logging its user out); forcing the user at that unit to re-enter their log-in credentials; or erasing the hard drive of the remote unit. *See* APL-AGIS_00012860. These features are described in detail in U.S. Pat. No. 7,278,023, of which I am a named inventor. *See, e.g.*, SIEGEL000400-417 (the "'023 patent") at 6:56-63; 8:15-9:23; 9:24-9:46. My team at TRW developed this patent as part of our work on FBCB2, and we incorporated many of the capabilities outlined in the patent in FBCB2. The '023 patent covers a method for administering access and security on a network. '023 pat. at 3:22-24. Among other things, the system includes a "remote control module . . . provided so that the systems administrator or security officer may take the appropriate action when certain events transpire." '023 pat. at 6:56-63. The patent discloses that a system administrator or security officer may send a challenge message to a user's device. '023

pat. at 8:15-28. Upon receipt of the message, the device presents the user's role/log in screen. '023 pat. at 8:28-44. If the user enters the wrong password or fails to enter the password, and this happens more than a pre-specified number of times, then the security administrator or officer has the option to remotely lock the device's screen or totally disable the user terminal and wipe its hard drive (among other possibilities). '023 pat. 8:28-9:23. These features were implemented as part of FBCB2.

B. Claim 2 is Anticipated by FBCB2, or, at a Minimum, is Obvious Over FBCB2 in View of the Knowledge of a POSA at the Time of the Invention

195. Claim 2 of the '829 patent depends from claim 1. Claim 2 of the '829 patent recites:

> 2. The method of claim 1, wherein the action is selected from the group comprising playing audio, initiating a phone call, vibrating, converting text to speech, changing sound intensity, and displaying information.

196. I understand that the Court has construed the term "group," as used in this claim, as: "more than two participants associated together." I have applied that construction in my analysis of this claim.

197. Claim 2 of the '829 patent is invalid because it is anticipated by FBCB2 or, at a minimum, is obvious over FBCB2 in view of the knowledge of a POSA. The limitations of claim 1 are anticipated by FBCB2, or, at a minimum, obvious in view of FBCB2, for the reasons discussed above. Claim 2 is anticipated or obvious for the additional reasons described below.

198. FBCB2 could remotely control another device by causing it to play audio and display information. As described above, an FBCB2 user who sent a "danger zone" location message could cause another user's device to play audio if the user approached the danger zone. Likewise, as described above and shown in the below figure (from SIEGEL000310), a user who sent a text message consisting of a warning or alarm could cause that information to be displayed as a scrolling marquee on the recipient's screen.

recipients based on the type of data being sent and/or addressee information provided by the FBCB2 user. For certain data, such as location information, the sender did not need to enter any addressee information at all, because the server broadcast the data automatically to all other members of the user's group. For other types of data, such as text messages, FBCB2 allowed users to designate particular users as recipients by specifying particular individuals or groups of individuals' log-in names, role or title, or group name (e.g. a particular platoon). This addressee information was sent to the server, and the server routed the information to the appropriate IP address. The sender never, however, had to know the IP address of the intended recipient(s).

216. U.S. Patent No. 6,212,559, (the "'559 patent") of which I am a named inventor, covers the process of setting up groups and facilitating communication among groups in FBCB2. *See* SIEGEL000333-355. My team at TRW developed this patent as part of our work on FBCB2, and we incorporated many of the capabilities outlined in the patent in FBCB2. Figure 17A of the '559 patent shows that users within a communication network were identified by a user ID; a user who was attempting to modify the network or select ot her users for communications would select those users' IDs. *See* '559 pat. Fig. 7; *id*. at 4:48-49. This feature was implemented as part of FBCB2.

G. Claim 34 is Anticipated by FBCB2, or, at a Minimum, is Obvious Over FBCB2 in View of the Knowledge of a POSA at the Time of the Invention

217. Claim 34 of the '829 patent recites:

> 34. A system comprising:
>
> one or more server devices programmed to perform operations comprising:
>
> forwarding, to a first device, a request to join a group, wherein the request is received from a second device and the group includes the second device;
>
> based on acceptance of the request by the first device, joining the first device to the group, wherein joining the first device to the group comprises authorizing the first

and could assist, the platoon member would acknowledge the order and the platoon member could be joined to the group at the appropriate time, and would at that time: begin sharing its location information with the server to be sent to other member of the group; receiving location information from other members of the group and displaying location information from those members; and exchanging messages and engaging in remote control operations with other members of the group. But if the platoon member did not send an acknowledgement message, then the platoon member would not be joined to the group at the designated time and the requestor would be notified of this lack of acknowledgement, and could select a different person to perform that role.

222. U.S. Patent No. 6,212,559, of which I am a named inventor, covers the process of setting up groups in FBCB2. *See* SIEGEL000333-355 (the "'559 patent"). My team at TRW developed this patent as part of our work on FBCB2, and we incorporated many of the capabilities outlined in the patent in FBCB2. The '559 patent covers techniques for configuring a computer network to allow for rapid reconfiguration due to changes in the location, identity, or network topology. *See* '559 pat. at 5:23-58. Specifically, the '559 patent discloses software consisting of network configuration tools in which each unit and user (e.g., brigade, company, fleet, ship, aircraft group) is grouped and interrelated with other units according to a "unit task organization" set up within the software. *See* '559 at 5:47-6:4. A user could use the "unit task organization" capability in order to define their desired groups. *See* '559 pat. at 5:59-6:11; *see also id*. at 7:1-4, 7:33-42. A user could also thereby define the set of users who could participate in each group. *See* '559 pat. at 8:16-24. Users could be given permissions to access more than one group. *See* '559 pat. at 7:49-67; 9:6-40. A user with appropriate permissions could assign another user to a group at any time. The patent explains that, when such an assignment was made, the software would disseminate the assignment to the user, and the user would respond by accepting the new

assignment. *See* '559 pat. at 8:31-51. These features were incorporated into FBCB2, as described in the preceding paragraph.

223. The method of setting up groups in FBCB2 was tailored to meet the security and operational needs of the military (e.g., ensuring users could only join groups of the appropriate security clearance and ensuring that commanders received acknowledgement of orders). A person of ordinary skill in the art at the time of the invention would have understood that the protocols described above could be easily modified in various ways (e.g., requiring fewer confirmations or additional confirmations before joining users to a group; allowing all users to invite each other to join any group or to request access to any group, etc.) to suit different needs. Thus, if this limitation is not anticipated by FBCB2, it would have been obvious in view of FBCB2 and the knowledge of a person of ordinary skill in the art at the time of the invention.

3. "receiving a first message comprising a request for a first updated location of the first device, wherein the first message is sent by the second device and includes data identifying the first device; in response to receiving the first message, sending, to the first device, a second message comprising a request for the first updated location of the first device; after sending the second message, receiving a response to the second message, the response including first location information comprising the first updated location of the first device;"

224. In FBCB2, members of a group continuously exchanged location information with one another. Therefore, when a second FBCB2 device requested that a first FBCB2 device join its group, the device also sent the server a message requesting up-to-date location information for the first device. In turn, when the server sent the first device the second device's request to join a group, the server also requested that the first device send its up-to-date location information. In response to that request, the first device would send its location information to the server. *See* SIEGEL000009-10; SIEGEL000014. Each device obtained its own location from a GPS receiver

The FBCB2 devices were portrayed as blue symbols, to denote that the other users were friendly forces. *See* SIEGEL000418; SIEGEL000484 (showing example); SIEGEL000671 (same); SIEGEL000782 (same); SIEGEL000783 (same).

5. "after sending the first location information and the georeferenced map data to the second device, receiving second location information comprising a second updated location of the first device and sending the second location information to the second device, wherein the second device is configured to use the server-provided georeferenced map data and the second location information to reposition the symbol on the georeferenced map at a second position corresponding to the second updated location of the first device;"

227. Each FBCB2 device continuously reported its updated location to the server. *See* SIEGEL000009-10; SIEGEL000014. The location reporting rate was time and distance triggered, such that a device would send updated location information at a predetermined time interval, unless it moved further than a pre-specified distance before that time interval had passed. *See* APL-AGIS_00012859. U.S. Patent No. 5,672,840, of which I am named inventor, describes the reporting filter incorporated in the FAAD C2I system, based on an angular filter (e.g., reporting whenever the display was rotated more than a certain amount). *See* SIEGEL000374 at 5:31-35. In FBCB2 (starting in 1995), we extended that concept of a filter for reporting based an angular threshold to one of a threshold based on time and motion. *See* SIEGEL000990-91. The information that passed the time-motion filter was continuously broadcast to other FBCB2 devices, and the updated information was automatically plotted on each FBCB2 device's georeferenced map. *See* SIEGEL000009-10; SIEGEL000305.

6. "receiving a third message related to remotely controlling the first device to perform an action, wherein the third message is sent by the second device; and after receiving the third message, sending, to the first device, a fourth message related to remotely controlling the first device to perform the action, wherein the first device is configured to perform the action based on receiving the fourth message."

228. FBCB2 allowed users to send command-and-control messages via the server that would remotely control the recipient FBCB2 device. *See* SIEGEL000006.

229. For example, an FBCB2 user could send another user a message comprising location information of an entity, and that location information would automatically be displayed on the georeferenced map of the recipient user. *See* SIEGEL000012; SIEGEL000015-16; APL-AGIS_00012847-8. As a further example, and FBCB2 user could send another user a message comprising a warning or alert that would be displayed in a scrolling marquee on the other user's touch screen. *See* SIEGEL000307 (image of FBCB2 user interface showing location of scrolling marquee). As a further example, FBCB2 commanders could identify and send users the locations of "danger" zones related to enemy fire, contamination areas, or enemy obstacles. *See* SIEGEL000016. FBCB2 devices could be programmed to play audible warnings when the device approached the location of a danger zone. *See* SIEGEL000016. Thus, a commander could cause a user's device to play a sound if the user was approaching a danger zone. *See* SIEGEL000016.

230. As a further example, an FBCB2 user could remotely "challenge" another, remote FBCB2 device (i.e., require the user of that remote FBCB2 unit to re-enter their log-in credentials; they might do this, for example, if they suspect that that particular FBCB2 unit has been captured by the enemy), or could engage in other remote-control operations such as: locking the remote FBCB2 unit (i.e., logging its user out); forcing the user at that unit to re-enter their log-in credentials; or erasing the hard drive of the remote unit. *See* APL-AGIS_00012860. These features are described in detail in U.S. Pat. No. 7,278,023, of which I am a named inventor. *See,*

e.g., SIEGEL000400-417 (the "'023 patent") at 6:56-63; 8:15-9:23; 9:24-9:46. My team at TRW developed this patent as part of our work on FBCB2, and we incorporated many of the capabilities outlined in the patent in FBCB2. The '023 patent covers a method for administering access and security on a network. '023 pat. at 3:22-24. Among other things, the system includes a "remote control module . . . provided so that the systems administrator or security officer may take the appropriate action when certain events transpire." '023 pat. at 6:56-63. The patent discloses that a system administrator or security officer may send a challenge message to a user's device. '023 pat. at 8:15-28. Upon receipt of the message, the device presents the user's role/log in screen. '023 pat. at 8:28-44. If the user enters the wrong password or fails to enter the password, and this happens more than a pre-specified number of times, then the security administrator or officer has the option to remotely lock the device's screen or totally disable the user terminal and wipe its hard drive (among other possibilities). '023 pat. 8:28-9:23. These features were implemented as part of FBCB2.

H. Claim 35 is Anticipated by FBCB2, or, at a Minimum, is Obvious Over FBCB2 in View of the Knowledge of a POSA at the Time of the Invention

231. Claim 35 of the '829 patent recites:

> 35. A computer-implemented method comprising:
>
> performing, by a second device:
>
> receiving, from a first device via a first server, a request to join a group, wherein the group includes the first device;
>
> sending, to the first server, an indication of acceptance of the request, wherein the first server is configured to join the first device to the group based on the acceptance of the request, and wherein joining the first device to the group comprises authorizing the first device to repeatedly share device location information and repeatedly engage in remote control operations with each device included in the group;
>
> sending a first message to the first server, wherein the first message comprises data identifying the first device and a request for a first updated location of the first

acknowledge acceptance of the order, then the soldier's device would not be joined to the group; instead, the system administrator or senior officer would be informed that that the order was not accepted. Likewise, the senior officer could change the task organization so that the senior officer *himself* was joined to the same group at that same time (i.e., because both the senior officer and soldier were part of the same mission), such that both the officer and soldier would be joined to the group at once. This feature was critical to allow FBCB2 users to plan military operations. For example, if a member of a platoon needed to be deployed to assist another platoon, a senior officer with appropriate permissions could assign that role to the platoon member. If the platoon member was available and could assist, the platoon member would acknowledge the order and the platoon member could be joined to the group, along with the senior officer, at the appropriate time. Then both the platoon member and the senior officer would: begin sharing its location information with the server to be sent to other member of the group; receiving location information from other members of the group and displaying location information from those members; and exchanging messages and engaging in remote control operations with other members of the group. . But if the platoon member did not send an acknowledgement message, then the platoon member would not be joined to the group at the designated time and the requestor would be notified of this lack of acknowledgement, and could select a different person to perform that role.

237. U.S. Patent No. 6,212,559, of which I am a named inventor, covers the process of setting up groups in FBCB2. *See* SIEGEL000333-355 (the "'559 patent"). My team at TRW developed this patent as part of our work on FBCB2, and we incorporated many of the capabilities outlined in the patent in FBCB2. The '559 patent covers techniques for configuring a computer network to allow for rapid reconfiguration due to changes in the location, identity, or network topology. *See* '559 pat. at 5:23-58. Specifically, the '559 patent discloses software consisting of

network configuration tools in which each unit and user (e.g., brigade, company, fleet, ship, aircraft group) is grouped and interrelated with other units according to a "unit task organization" set up within the software. *See* '559 at 5:47-6:4. A user could use the "unit task organization" capability in order to define their desired groups. *See* '559 pat. at 5:59-6:11; *see also id*. at 7:1-4, 7:33-42. A user could also thereby define the set of users who could participate in each group. *See* '559 pat. at 8:16-24. Users could be given permissions to access more than one group. *See* '559 pat. at 7:49-67; 9:6-40. A user with appropriate permissions could assign another user to a group at any time. The patent explains that, when such an assignment was made, the software would disseminate the assignment to the user, and the user would respond by accepting the new assignment. *See* '559 pat. at 8:31-51. These features were incorporated into FBCB2, as described in the preceding paragraph.

238. The method of setting up groups in FBCB2 was tailored to meet the security and operational needs of the military (e.g., ensuring users could only join groups of the appropriate security clearance and ensuring that commanders received acknowledgement of orders). A person of ordinary skill in the art at the time of the invention would have understood that the protocols described above could be easily modified in various ways (e.g., requiring fewer confirmations or additional confirmations before joining users to a group; allowing all users to invite each other to join any group or to request access to any group, etc.) to suit different needs. Thus, if this limitation is not anticipated by FBCB2, it would have been obvious in view of FBCB2 and the knowledge of a person of ordinary skill in the art at the time of the invention.

243. FBCB2 receive the map data from a second server. As discussed above, the servers in FBCB2 consisted of computers mounted in army vehicles. That is, individual FBCB2 units were designated to receive information from FBCB2 devices and forward it to other FBCB2 devices. Because users moved around and access to a particular server could be blocked by buildings, mountains, jamming, or other difficulties, there was not a single, static server designation in FBCB2 as there typically is in an office or consumer computer network. Instead, FBCB2 devices were programmed to collaborate and *dynamically* select one of their number to act as the server. If the unit acting as a server became unavailable for some reason—whether because it was blocked or due to damage in the war—the remaining units would collaborate and select another of the members to take over the role of server. Thus, a given FBCB2 device might use one or more servers during the course of a given operation. This process for dynamically electing servers was designed and built in 1997 and 1998, and is documented in 1997 project status report (*see* SIEGEL000794-5) and 1998 design document (*see* SIEGEL001003-5). Design cases are provided for both what is termed "self-election" (where an FBCB2 computer detects that no other computer is acting as a server in an area, perhaps because this computer is the first one to start up after the arrival of a new military unit in an area) and "fractured net" (this is the use-case where server disconnects due to changes in the battlefield situation are accommodated) situations. *See* SIEGEL001003-5).

3. "after receiving the first location information and the georeferenced map data, receiving second location information comprising a second updated location of the first device from the first server, and using the server-provided georeferenced map data and the second location information to reposition the symbol on the georeferenced map at a second position corresponding to the second updated location of the first device; and"

244. Each FBCB2 device continuously reported its updated location to the server. *See* SIEGEL000009-10; SIEGEL000014. The location reporting rate was time and distance triggered,

such that a device would send updated location information at a predetermined time interval, unless it moved further than a pre-specified distance before that time interval had passed. *See* APL-AGIS_00012859. U.S. Patent No. 5,672,840, of which I am named inventor, describes the reporting filter incorporated in the FAAD C2I system, based on an angular filter (e.g., reporting whenever the display was rotated more than a certain amount). *See* SIEGEL000374 at 5:31-35. In FBCB2 (starting in 1995), we extended that concept of a filter for reporting based an angular threshold to one of a threshold based on time and motion. *See* SIEGEL000990-91. The information that passed the time-motion filter was continuously broadcast to other FBCB2 devices, and the updated information was automatically plotted on each FBCB2 device's georeferenced map. *See* SIEGEL000009-10; SIEGEL000305.

245. FBCB2 presented georeferenced server-provided georeferenced maps and second sets of user-selectable symbols corresponding to a second set of devices plotted on the maps at positions corresponding to latitude and longitude. The server continuously broadcast that information to other FBCB2 devices, and the location information on the maps of those devices was updated in near-real-time. *See* SIEGEL000009-10; SIEGEL000305; SIEGEL000484; SIEGEL000782. As described above, a user could toggle to a newly-received, server-provided map at will.

4. "identifying user interaction with the display specifying an action and, based thereon, sending, to the first server, a third message related to remotely controlling the first device to perform an action, wherein the first server is configured to send a fourth message to the first device based on receiving the third message from the second device, wherein the fourth message relates to remotely controlling the first device to perform the action, and wherein the first device is configured to perform the action based on receiving the fourth message."

246. As discussed in greater detail above, FBCB2 was installed and run on a variety of devices with interactive displays, typically touch screens. *See, e.g.*, SIEGEL000001;

250. As a further example, an FBCB2 user could remotely "challenge" another, remote FBCB2 device (i.e., require the user of that remote FBCB2 unit to re-enter their log-in credentials; they might do this, for example, if they suspect that that particular FBCB2 unit has been captured by the enemy), or could engage in other remote-control operations such as: locking the remote FBCB2 unit (i.e., logging its user out); forcing the user at that unit to re-enter their log-in credentials; or erasing the hard drive of the remote unit. *See* APL-AGIS_00012860. These features are described in detail in U.S. Pat. No. 7,278,023, of which I am a named inventor. *See, e.g.*, SIEGEL000400-417 (the "'023 patent") at 6:56-63; 8:15-9:23; 9:24-9:46. My team at TRW developed this patent as part of our work on FBCB2, and we incorporated many of the capabilities outlined in the patent in FBCB2. The '023 patent covers a method for administering access and security on a network. '023 pat. at 3:22-24. Among other things, the system includes a "remote control module . . . provided so that the systems administrator or security officer may take the appropriate action when certain events transpire." '023 pat. at 6:56-63. The patent discloses that a system administrator or security officer may send a challenge message to a user's device. '023 pat. at 8:15-28. Upon receipt of the message, the device presents the user's role/log in screen. '023 pat. at 8:28-44. If the user enters the wrong password or fails to enter the password, and this happens more than a pre-specified number of times, then the security administrator or officer has the option to remotely lock the device's screen or totally disable the user terminal and wipe its hard drive (among other possibilities). '023 pat. 8:28-9:23. These features were implemented as part of FBCB2.

I. Claim 42 is Anticipated by FBCB2, or, at a Minimum, is Obvious Over FBCB2 in View of the Knowledge of a POSA at the Time of the Invention

251. Claim 42 of the '829 patent depends from claims 35 and 41. Claim 41 of the '829 patent recites:

was available and could assist, the platoon member would acknowledge the order and the platoon member could be joined to the group, along with the senior officer, at the appropriate time. Then both the platoon member and the senior officer would: begin sharing its location information with the server to be sent to other member of the group; receiving location information from other members of the group and displaying location information from those members; and exchanging messages and engaging in remote control operations with other members of the group. . But if the platoon member did not send an acknowledgement message, then the platoon member would not be joined to the group at the designated time and the requestor would be notified of this lack of acknowledgement, and could select a different person to perform that role.

267. U.S. Patent No. 6,212,559, of which I am a named inventor, covers the process of setting up groups in FBCB2. *See* SIEGEL000333-355 (the "'559 patent"). My team at TRW developed this patent as part of our work on FBCB2, and we incorporated many of the capabilities outlined in the patent in FBCB2. The '559 patent covers techniques for configuring a computer network to allow for rapid reconfiguration due to changes in the location, identity, or network topology. *See* '559 pat. at 5:23-58. Specifically, the '559 patent discloses software consisting of network configuration tools in which each unit and user (e.g., brigade, company, fleet, ship, aircraft group) is grouped and interrelated with other units according to a "unit task organization" set up within the software. *See* '559 at 5:47-6:4. A user could use the "unit task organization" capability in order to define their desired groups. *See* '559 pat. at 5:59-6:11; *see also id*. at 7:1-4, 7:33-42. A user could also thereby define the set of users who could participate in each group. *See* '559 pat. at 8:16-24. Users could be given permissions to access more than one group. *See* '559 pat. at 7:49-67; 9:6-40. A user with appropriate permissions could assign another user to a group at any time. The patent explains that, when such an assignment was made, the software would

disseminate the assignment to the user, and the user would respond by accepting the new assignment. *See* '559 pat. at 8:31-51. These features were incorporated into FBCB2, as described in the preceding paragraph.

268. The method of setting up groups in FBCB2 was tailored to meet the security and operational needs of the military (e.g., ensuring users could only join groups of the appropriate security clearance and ensuring that commanders received acknowledgement of orders). A person of ordinary skill in the art at the time of the invention would have understood that the protocols described above could be easily modified in various ways (e.g., requiring fewer confirmations or additional confirmations before joining users to a group; allowing all users to invite each other to join any group or to request access to any group, etc.) to suit different needs. Thus, if this limitation is not anticipated by FBCB2, it would have been obvious in view of FBCB2 and the knowledge of a person of ordinary skill in the art at the time of the invention.

3. "sending a first message to the first server, wherein the first message comprises data identifying the first device and a request for a first updated location of the first device, and wherein the first server is configured to send a second message to the first device based on and in response to receiving the first message from the second device, wherein the second message comprises a request for the first updated location of the first device; after sending the first message, receiving, from the first server, a response to the first message, the response including first location information comprising the first updated location of the first device;"

269. In FBCB2, members of a group continuously exchanged location information with one another. Therefore, when an FBCB2 device joined a group, the device also sent the server a message requesting up-to-date location information for the other devices in the group. In turn, when a device was joined to a group, the server sent the first device the second device's request to join a group, the server also requested that the device send its up-to-date location information. In response to that request, the device would send its location information to the server. *See*

use one or more servers during the course of a given operation. This process for dynamically electing servers was designed and built in 1997 and 1998, and is documented in 1997 project status report (*see* SIEGEL000794-5) and 1998 design document (*see* SIEGEL001003-5). Design cases are provided for both what is termed "self-election" (where an FBCB2 computer detects that no other computer is acting as a server in an area, perhaps because this computer is the first one to start up after the arrival of a new military unit in an area) and "fractured net" (this is the use-case where server disconnects due to changes in the battlefield situation are accommodated) situations. *See* SIEGEL001003-5).

5. "after receiving the first location information and the georeferenced map data, and after presenting the georeferenced map and the symbol positioned on the georeferenced map at the first position corresponding to the first updated location of the first device, receiving second location information comprising a second updated location of the first device from the first server, and using the server-provided georeferenced map data and the second location information to reposition the symbol on the georeferenced map at a second position corresponding to the second updated location of the first device; and"

274. Each FBCB2 device continuously reported its updated location to the server. *See* SIEGEL000009-10; SIEGEL000014. The location reporting rate was time and distance triggered, such that a device would send updated location information at a predetermined time interval, unless it moved further than a pre-specified distance before that time interval had passed. *See* APL-AGIS_00012859. U.S. Patent No. 5,672,840, of which I am named inventor, describes the reporting filter incorporated in the FAAD C2I system, based on an angular filter (e.g., reporting whenever the display was rotated more than a certain amount). *See* SIEGEL000374 at 5:31-35. In FBCB2 (starting in 1995), we extended that concept of a filter for reporting based an angular threshold to one of a threshold based on time and motion. *See* SIEGEL000990-91. The information that passed the time-motion filter was continuously broadcast to other FBCB2 devices,

and the updated information was automatically plotted on each FBCB2 device's georeferenced map. *See* SIEGEL000009-10; SIEGEL000305.

275. FBCB2 presented georeferenced server-provided georeferenced maps and second sets of user-selectable symbols corresponding to a second set of devices plotted on the maps at positions corresponding to latitude and longitude. The server continuously broadcast that information to other FBCB2 devices, and the location information on the maps of those devices was updated in near-real-time. *See* SIEGEL000009-10; SIEGEL000305; SIEGEL000484; SIEGEL000782. As described above, a user could toggle to a newly-received, server-provided map at will.

6. "identifying user interaction with the display specifying an action and, based thereon, sending, to the first server, a third message related to remotely controlling the first device to perform an action, wherein the first server is configured to send a fourth message to the first device based on receiving the third message from the second device, wherein the fourth message relates to remotely controlling the first device to perform the action, and wherein the first device is configured to perform the action based on receiving the fourth message."

276. As discussed in greater detail above, FBCB2 was installed and run on a variety of devices with interactive displays, typically touch screens. *See, e.g.*, SIEGEL000001; SIEGEL000782; SIEGEL 000783. Every device running FBCB2 included a screen that displayed maps. *See, e.g.* SIEGEL000001 (showing FBCB2 devices presenting maps). FBCB2 was compatible with and employed a range of georeferenced map types that related locations on the map to latitude and longitude. *See* SIEGEL000311 (listing some map types).

277. An FBCB2 user could select a one or more symbols corresponding to one or more other FBCB2 devices, specify an action and, based thereon, send third data to the selected one or more devices via the first server. When remote control messages, users could choose to send the message to their entire group, to a sub-group, or to individual users. Recipients could be selected

by touching the symbol corresponding with the recipient on the map. *See* APL-AGIS_00012882 (explaining that users could send messages by clicking on a unit's icon).

278. FBCB2 allowed users to send command-and-control messages via the server that would remotely control the recipient FBCB2 device. *See* SIEGEL000006.

279. For example, an FBCB2 user could send another user a message comprising location information of an entity, and that location information would automatically be displayed on the georeferenced map of the recipient user. *See* SIEGEL000012; SIEGEL000015-16; APL-AGIS_00012847-8. As a further example, and FBCB2 user could send another user a message comprising a warning or alert that would be displayed in a scrolling marquee on the other user's touch screen. *See* SIEGEL000307 (image of FBCB2 user interface showing location of scrolling marquee). As a further example, FBCB2 commanders could identify and send users the locations of "danger" zones related to enemy fire, contamination areas, or enemy obstacles. *See* SIEGEL000016. FBCB2 devices could be programmed to play audible warnings when the device approached the location of a danger zone. *See* SIEGEL000016. Thus, a commander could cause a user's device to play a sound if the user was approaching a danger zone. *See* SIEGEL000016.

280. As a further example, an FBCB2 user could remotely "challenge" another, remote FBCB2 device (i.e., require the user of that remote FBCB2 unit to re-enter their log-in credentials; they might do this, for example, if they suspect that that particular FBCB2 unit has been captured by the enemy), or could engage in other remote-control operations such as: locking the remote FBCB2 unit (i.e., logging its user out); forcing the user at that unit to re-enter their log-in credentials; or erasing the hard drive of the remote unit. *See* APL-AGIS_00012860. These features are described in detail in U.S. Pat. No. 7,278,023, of which I am a named inventor. *See, e.g.*, SIEGEL000400-417 (the "'023 patent") at 6:56-63; 8:15-9:23; 9:24-9:46. My team at TRW

developed this patent as part of our work on FBCB2, and we incorporated many of the capabilities outlined in the patent in FBCB2. The '023 patent covers a method for administering access and security on a network. '023 pat. at 3:22-24. Among other things, the system includes a "remote control module . . . provided so that the systems administrator or security officer may take the appropriate action when certain events transpire." '023 pat. at 6:56-63. The patent discloses that a system administrator or security officer may send a challenge message to a user's device. '023 pat. at 8:15-28. Upon receipt of the message, the device presents the user's role/log in screen. '023 pat. at 8:28-44. If the user enters the wrong password or fails to enter the password, and this happens more than a pre-specified number of times, then the security administrator or officer has the option to remotely lock the device's screen or totally disable the user terminal and wipe its hard drive (among other possibilities). '023 pat. 8:28-9:23. These features were implemented as part of FBCB2.

X. THE ASSERTED CLAIMS OF THE '055 PATENT ARE ANTICIPATED OR RENDERED OBVIOUS BY FBCB2 AND THE KNOWLEDGE OF A POSA AT THE TIME OF THE INVENTION

281. My statements regarding the FBCB2 system, below, are based on my personal knowledge of that system. Although I have cited certain documents for the purpose of illustrating or further explaining certain features of the system, I have personal knowledge of every feature I describe. I derived this knowledge from my work on the FBCB2 system, which is outlined in detail in the Technical Background section of this report.

282. In the below analysis, any references to the state of the art refer to the state of the art as of September 20, 2004. Similarly, all references to the knowledge or understandings of a person of ordinary skill in the art refer to the knowledge or understandings of a person of ordinary skill in the art as of September 20, 2004. Likewise, all references to the features of FBCB2 refer to features that were part of the system as of September 20, 2004. My analysis of the invalidity

303. As a further example, an FBCB2 user could remotely "challenge" another, remote FBCB2 device (i.e., require the user of that remote FBCB2 unit to re-enter their log-in credentials; they might do this, for example, if they suspect that that particular FBCB2 unit has been captured by the enemy), or could engage in other remote-control operations such as: locking the remote FBCB2 unit (i.e., logging its user out); forcing the user at that unit to re-enter their log-in credentials; or erasing the hard drive of the remote unit. *See* APL-AGIS_00012860. These features are described in detail in U.S. Pat. No. 7,278,023, of which I am a named inventor. *See, e.g.*, SIEGEL000400-417 (the "'023 patent") at 6:56-63; 8:15-9:23; 9:24-9:46. My team at TRW developed this patent as part of our work on FBCB2, and we incorporated many of the capabilities outlined in the patent in FBCB2. The '023 patent covers a method for administering access and security on a network. '023 pat. at 3:22-24. Among other things, the system includes a "remote control module . . . provided so that the systems administrator or security officer may take the appropriate action when certain events transpire." '023 pat. at 6:56-63. The patent discloses that a system administrator or security officer may send a challenge message to a user's device. '023 pat. at 8:15-28. Upon receipt of the message, the device presents the user's role/log in screen. '023 pat. at 8:28-44. If the user enters the wrong password or fails to enter the password, and this happens more than a pre-specified number of times, then the security administrator or officer has the option to remotely lock the device's screen or totally disable the user terminal and wipe its hard drive (among other possibilities). '023 pat. 8:28-9:23. These features were implemented as part of FBCB2.

1. "The method of claim 1, further comprising performing, by the first device: receiving a message sent by a particular second device, wherein the message indicates an action to be performed by the first device; and performing the indicated action."

322. FBCB2 allowed users to send command-and-control messages via the server that would remotely control the recipient FBCB2 device. *See* SIEGEL000006.

323. For example, an FBCB2 user could send another user a message comprising location information of an entity, and that location information would automatically be displayed on the georeferenced map of the recipient user. *See* SIEGEL000012; SIEGEL000015-16; APL-AGIS_00012847-8. As a further example, and FBCB2 user could send another user a message comprising a warning or alert that would be displayed in a scrolling marquee on the other user's touch screen. *See* SIEGEL000307 (image of FBCB2 user interface showing location of scrolling marquee). As a further example, FBCB2 commanders could identify and send users the locations of "danger" zones related to enemy fire, contamination areas, or enemy obstacles. *See* SIEGEL000016. FBCB2 devices could be programmed to play audible warnings when the device approached the location of a danger zone. *See* SIEGEL000016. Thus, a commander could cause a user's device to play a sound if the user was approaching a danger zone. *See* SIEGEL000016.

324. As a further example, an FBCB2 user could remotely "challenge" another, remote FBCB2 device (i.e., require the user of that remote FBCB2 unit to re-enter their log-in credentials; they might do this, for example, if they suspect that that particular FBCB2 unit has been captured by the enemy), or could engage in other remote-control operations such as: locking the remote FBCB2 unit (i.e., logging its user out); forcing the user at that unit to re-enter their log-in credentials; or erasing the hard drive of the remote unit. *See* APL-AGIS_00012860. These features are described in detail in U.S. Pat. No. 7,278,023, of which I am a named inventor. *See, e.g.*, SIEGEL000400-417 (the "'023 patent") at 6:56-63; 8:15-9:23; 9:24-9:46. My team at TRW

developed this patent as part of our work on FBCB2, and we incorporated many of the capabilities outlined in the patent in FBCB2. The '023 patent covers a method for administering access and security on a network. '023 pat. at 3:22-24. Among other things, the system includes a "remote control module . . . provided so that the systems administrator or security officer may take the appropriate action when certain events transpire." '023 pat. at 6:56-63. The patent discloses that a system administrator or security officer may send a challenge message to a user's device. '023 pat. at 8:15-28. Upon receipt of the message, the device presents the user's role/log in screen. '023 pat. at 8:28-44. If the user enters the wrong password or fails to enter the password, and this happens more than a pre-specified number of times, then the security administrator or officer has the option to remotely lock the device's screen or totally disable the user terminal and wipe its hard drive (among other possibilities). '023 pat. 8:28-9:23. These features were implemented as part of FBCB2.

2. "The method of claim 23, wherein the indicated action is selected from the group consisting of playing audio, initiating a phone call, vibrating, converting text to speech, changing sound intensity, and displaying information."

325. FBCB2 could remotely control another device by causing it to play audio and display information. As described above, an FBCB2 user who sent a "danger zone" location message could cause another user's device to play audio if the user approached the danger zone. Likewise, as described above and shown in the below figure (from SIEGEL000310), a user who sent a text message consisting of a warning or alarm could cause that information to be displayed as a scrolling marquee on the recipient's screen.

users could also check device status metrics, such as battery level, and send each other text messages containing that information.

344. FBCB2 also allowed users to send data comprising command-and-control messages that would remotely control the recipient FBCB2 device. *See* SIEGEL000006. For example, an FBCB2 user could send another user a message comprising location information of an entity, and that location information would automatically be displayed on the georeferenced map of the recipient user. *See* SIEGEL000012; SIEGEL000015-16; APL-AGIS_00012847-8. As a further example, and FBCB2 user could send another user a message comprising a warning or alert that would be displayed in a scrolling marquee on the other user's touch screen. *See* SIEGEL000307 (image of FBCB2 user interface showing location of scrolling marquee). As a further example, FBCB2 commanders could identify and send users the locations of "danger" zones related to enemy fire, contamination areas, or enemy obstacles. *See* SIEGEL000016. FBCB2 devices could be programmed to play audible warnings when the device approached the location of a danger zone. *See* SIEGEL000016. Thus, a commander could cause a user's device to play a sound if the user was approaching a danger zone. *See* SIEGEL000016.

345. As a further example, an FBCB2 user could remotely "challenge" another, remote FBCB2 device (i.e., require the user of that remote FBCB2 unit to re-enter their log-in credentials; they might do this, for example, if they suspect that that particular FBCB2 unit has been captured by the enemy), or could engage in other remote-control operations such as: locking the remote FBCB2 unit (i.e., logging its user out); forcing the user at that unit to re-enter their log-in credentials; or erasing the hard drive of the remote unit. *See* APL-AGIS_00012860. These features are described in detail in U.S. Pat. No. 7,278,023, of which I am a named inventor. *See, e.g.*, SIEGEL000400-417 (the "'023 patent") at 6:56-63; 8:15-9:23; 9:24-9:46. My team at TRW

developed this patent as part of our work on FBCB2, and we incorporated many of the capabilities outlined in the patent in FBCB2. The '023 patent covers a method for administering access and security on a network. '023 pat. at 3:22-24. Among other things, the system includes a "remote control module . . . provided so that the systems administrator or security officer may take the appropriate action when certain events transpire." '023 pat. at 6:56-63. The patent discloses that a system administrator or security officer may send a challenge message to a user's device. '023 pat. at 8:15-28. Upon receipt of the message, the device presents the user's role/log in screen. '023 pat. at 8:28-44. If the user enters the wrong password or fails to enter the password, and this happens more than a pre-specified number of times, then the security administrator or officer has the option to remotely lock the device's screen or totally disable the user terminal and wipe its hard drive (among other possibilities). '023 pat. 8:28-9:23. These features were implemented as part of FBCB2.

6. "receiving user input via user interaction with the interactive display of the first device, the user input specifying a location and a symbol corresponding to an entity other than the first device and the second devices; and based on the user input, adding the user-specified symbol to the interactive display at a position on the interactive map corresponding to the user-specified location, and transmitting the user-specified symbol and location to the second devices for addition of the user-specified symbol to respective interactive displays of the second devices at respective positions on respective interactive maps corresponding to the user-specified location."

346. FBCB2 allowed users to add entities to their own maps. For example, an FBCB2 user could mark the location of enemy forces, sources of danger (e.g. minefields or chemical and biological fallout zones), and sources of assistance (such as the location of a safe route through a minefield or fallout zone). *See* SIEGEL000014-15; APL-AGIS_00012847-8. A user could specify a symbol corresponding to an entity by either selecting a symbol (such as a bridge) that was pre-loaded into the FBCB2 system and dropping it onto their own, or by simply drawing a

32. The system of claim 28 wherein the operations further comprise:

transmitting location information including an updated location of the first device to the second devices based on displacement of the first device by at least a predetermined distance relative to a previous location of the first device, passage of at least a predetermined time interval since transmitting information including a location of the first device, or a combination of the displacement of the first device and the passage of time.

349. Claim 32 of the '055 patent is invalid because it is anticipated by FBCB2 or, at a minimum, is obvious over FBCB2 in view of the knowledge of a POSA. The limitations of claim 28 are anticipated by FBCB2, or, at a minimum, obvious in view of FBCB2, for the reasons discussed above. Claim 32 is anticipated or obvious for the additional reasons described below.

350. As discussed above with respect to claim 1, each FBCB2 device continuously reported its updated location to the server. *See* SIEGEL000009-10; SIEGEL000014. *See* SIEGEL000009-10; SIEGEL000014. The location reporting rate was time and distance triggered, such that a device would send updated location information at a predetermined time interval, unless it moved further than a pre-specified distance before that time interval had passed. *See* APL-AGIS_00012859. U.S. Patent No. 5,672,840, of which I am named inventor, describes the reporting filter incorporated in the FAAD C2I system, based on an angular filter (e.g., reporting whenever the display was rotated more than a certain amount). *See* SIEGEL000374 at 5:31-35. In FBCB2 (starting in 1995), we extended that concept of a filter for reporting based an angular threshold to one of a threshold based on time and motion. *See* SIEGEL000990-91. The information that passed the time-motion filter was continuously broadcast to other FBCB2 devices, and the updated information was automatically plotted on each FBCB2 device's georeferenced map. *See* SIEGEL000009-10; SIEGEL000305.

map of the recipient user. *See* SIEGEL000012; SIEGEL000015-16; APL-AGIS_00012847-8. As a further example, and FBCB2 user could send another user a message comprising a warning or alert that would be displayed in a scrolling marquee on the other user's touch screen. *See* SIEGEL000307 (image of FBCB2 user interface showing location of scrolling marquee). As a further example, FBCB2 commanders could identify and send users the locations of "danger" zones related to enemy fire, contamination areas, or enemy obstacles. *See* SIEGEL000016. FBCB2 devices could be programmed to play audible warnings when the device approached the location of a danger zone. *See* SIEGEL000016. Thus, a commander could cause a user's device to play a sound if the user was approaching a danger zone. *See* SIEGEL000016.

376. As a further example, an FBCB2 user could remotely "challenge" another, remote FBCB2 device (i.e., require the user of that remote FBCB2 unit to re-enter their log-in credentials; they might do this, for example, if they suspect that that particular FBCB2 unit has been captured by the enemy), or could engage in other remote-control operations such as: locking the remote FBCB2 unit (i.e., logging its user out); forcing the user at that unit to re-enter their log-in credentials; or erasing the hard drive of the remote unit. *See* APL-AGIS_00012860. These features are described in detail in U.S. Pat. No. 7,278,023, of which I am a named inventor. *See, e.g.*, SIEGEL000400-417 (the "'023 patent") at 6:56-63; 8:15-9:23; 9:24-9:46. My team at TRW developed this patent as part of our work on FBCB2, and we incorporated many of the capabilities outlined in the patent in FBCB2. The '023 patent covers a method for administering access and security on a network. '023 pat. at 3:22-24. Among other things, the system includes a "remote control module . . . provided so that the systems administrator or security officer may take the appropriate action when certain events transpire." '023 pat. at 6:56-63. The patent discloses that a system administrator or security officer may send a challenge message to a user's device. '023

pat. at 8:15-28. Upon receipt of the message, the device presents the user's role/log in screen. '023 pat. at 8:28-44. If the user enters the wrong password or fails to enter the password, and this happens more than a pre-specified number of times, then the security administrator or officer has the option to remotely lock the device's screen or totally disable the user terminal and wipe its hard drive (among other possibilities). '023 pat. 8:28-9:23. These features were implemented as part of FBCB2.

6. "receiving user input via user interaction with the interactive display of the first device, the user input specifying a location and a symbol corresponding to an entity other than the first device and the second devices; and based on the user input, adding the user-specified symbol to the interactive display at a position on the interactive map corresponding to the user-specified location, and transmitting the user-specified symbol and location to the second devices for addition of the user-specified symbol to respective interactive displays of the second devices at respective positions on respective interactive maps corresponding to the user-specified location."

377. FBCB2 allowed users to add entities to their own maps. For example, an FBCB2 user could mark the location of enemy forces, sources of danger (e.g. minefields or chemical and biological fallout zones), and sources of assistance (such as the location of a safe route through a minefield or fallout zone). *See* SIEGEL000014-15; APL-AGIS_00012847-8. A user could specify a symbol corresponding to an entity by either selecting a symbol (such as a bridge) that was pre-loaded into the FBCB2 system and dropping it onto their own, or by simply drawing a symbol at the appropriate location on their own map. SIEGEL000012; SIEGEL000015; APL-AGIS_00012847-8.

378. FBCB2 allowed users to send each other information about the location of entities other than FBCB2 devices, and to add that information to other users' georeferenced maps. For example, FBCB2 users could send each other information about the locations of enemy forces, sources of danger (e.g. minefields or chemical and biological fallout zones), and sources of

location of a danger zone. *See* SIEGEL000016. Thus, a commander could cause a user's device to play a sound if the user was approaching a danger zone. *See* SIEGEL000016.

404. As a further example, an FBCB2 user could remotely "challenge" another, remote FBCB2 device (i.e., require the user of that remote FBCB2 unit to re-enter their log-in credentials; they might do this, for example, if they suspect that that particular FBCB2 unit has been captured by the enemy), or could engage in other remote-control operations such as: locking the remote FBCB2 unit (i.e., logging its user out); forcing the user at that unit to re-enter their log-in credentials; or erasing the hard drive of the remote unit. *See* APL-AGIS_00012860. These features are described in detail in U.S. Pat. No. 7,278,023, of which I am a named inventor. *See, e.g.*, SIEGEL000400-417 (the "'023 patent") at 6:56-63; 8:15-9:23; 9:24-9:46. My team at TRW developed this patent as part of our work on FBCB2, and we incorporated many of the capabilities outlined in the patent in FBCB2. The '023 patent covers a method for administering access and security on a network. '023 pat. at 3:22-24. Among other things, the system includes a "remote control module . . . provided so that the systems administrator or security officer may take the appropriate action when certain events transpire." '023 pat. at 6:56-63. The patent discloses that a system administrator or security officer may send a challenge message to a user's device. '023 pat. at 8:15-28. Upon receipt of the message, the device presents the user's role/log in screen. '023 pat. at 8:28-44. If the user enters the wrong password or fails to enter the password, and this happens more than a pre-specified number of times, then the security administrator or officer has the option to remotely lock the device's screen or totally disable the user terminal and wipe its hard drive (among other possibilities). '023 pat. 8:28-9:23. These features were implemented as part of FBCB2.

example, if the leader of a platoon became incapacitated, a new platoon leader might need to be appointed in his place. A senior officer with appropriate permissions could assign that role to a different member of the platoon, and thereby send the new leader a message asking the leader to join the group or groups with which a platoon leader needed to share location information and engage in remote control operations.

415. U.S. Patent No. 6,212,559, of which I am a named inventor, covers the process of setting up groups in FBCB2. *See* SIEGEL000333-355 (the "'559 patent"). My team at TRW developed this patent as part of our work on FBCB2, and we incorporated many of the capabilities outlined in the patent in FBCB2. The '559 patent covers techniques for configuring a computer network to allow for rapid reconfiguration due to changes in the location, identity, or network topology. *See* '559 pat. at 5:23-58. Specifically, the '559 patent discloses software consisting of network configuration tools in which each unit and user (e.g., brigade, company, fleet, ship, aircraft group) is grouped and interrelated with other units according to a "unit task organization" set up within the software. *See* '559 at 5:47-6:4. A user could use the "unit task organization" capability in order to define their desired groups. *See* '559 pat. at 5:59-6:11; *see also id*. at 7:1-4, 7:33-42. A user could also thereby define the set of users who could participate in each group. *See* '559 pat. at 8:16-24. Users could be given permissions to access more than one group. *See* '559 pat. at 7:49-67; 9:6-40. A user with appropriate permissions could assign another user to a group at any time. The patent explains that, when such an assignment was made, the software would disseminate the assignment to the user, and the user would respond by accepting the new assignment. *See* '559 pat. at 8:31-51. These features were incorporated into FBCB2, as described in the preceding paragraph.

416. The method of setting up groups in FBCB2 was tailored to meet the security and operational needs of the military (e.g., ensuring users could only join groups of the appropriate security clearance and ensuring that commanders received acknowledgement of orders). A person of ordinary skill in the art at the time of the invention would have understood that the protocols described above could be easily modified in various ways (e.g., requiring fewer confirmations or additional confirmations before joining users to a group; allowing all users to invite each other to join any group or to request access to any group, etc.) to suit different needs. Thus, if this limitation is not anticipated by FBCB2, it would have been obvious in view of FBCB2 and the knowledge of a person of ordinary skill in the art at the time of the invention.

3. "wherein participating in the group includes sending first location information to a server and receiving second location information from the server, the first location information comprising a location of the first device, the second location information comprising a plurality of locations of a respective plurality of second devices included in the group;"

417. FBCB2 devices exchanged location information via a server. Each device obtained its own location from a GPS receiver attached to (or built into) the device.[18] The location information consisted of latitude and longitude coordinates determined by a GPS unit installed in the FBCB2 device. *See also* SIEGEL000009-10; SIEGEL000014; SIEGEL000782. Each device reported its latitude and longitude to the server, and the server broadcast that information to other FBCB2 devices. *See also* SIEGEL000009-10.

418. The servers in FBCB2 consisted of computers mounted in army vehicles. That is, individual FBCB2 units were designated to receive information from FBCB2 devices and forward

[18] Location information could also be obtained by other methods, including radio triangulation of the ground-to-ground radio links or an inertial navigation system on the vehicle. The FBCB2 software automatically determined which of these was the most accurate at the moment, and used that most-accurate position as the FBCB2 position to report to the FBCB2 network.

individuals' log-in names, role or title, or group name (e.g. a particular platoon). This addressee information was sent to the server, and the server routed the information to the appropriate IP address. The sender never, however, had to know the IP address of the intended recipient(s).

431. U.S. Patent No. 6,212,559, (the "'559 patent") of which I am a named inventor, covers the process of setting up groups and facilitating communication among groups in FBCB2. *See* SIEGEL000333-355. My team at TRW developed this patent as part of our work on FBCB2, and we incorporated many of the capabilities outlined in the patent in FBCB2. Figure 17A of the '559 patent shows that users within a communication network were identified by a user ID; a user who was attempting to modify the network or select ot her users for communications would select those users' IDs. *See* '559 pat. Fig. 7; *id*. at 4:48-49. This feature was implemented as part of FBCB2.

B. Claim 2 is Anticipated by FBCB2, or, at a Minimum, is Obvious Over FBCB2 in View of the Knowledge of a POSA at the Time of the Invention

432. Claim 2 of the '251 depends from claim 1. Claim 2 of the '251 patent recites:

> 2. The method of claim 1, wherein the data includes a short message service message, a text message, an image, or a video.

433. Claim 2 of the '251 patent is invalid because it is anticipated by FBCB2 or, at a minimum, is obvious over FBCB2 in view of the knowledge of a POSA. The limitations of claim 1 are anticipated by FBCB2, or, at a minimum, obvious in view of FBCB2, for the reasons discussed above. Claim 2 is anticipated or obvious for the additional reasons described below.

434. FBCB2 devices could send each other both text messages and images. SIEGEL000009-10; SIEGEL000418; APL-AGIS_00012890.

C. Claim 5 is Anticipated by FBCB2, or, at a Minimum, is Obvious Over FBCB2 in View of the Knowledge of a POSA at the Time of the Invention

435. Claim 5 of the '251 patent depends from claim 1. Claim 5 of the '251 patent recites:

> 5. The method of claim 1, further comprising sending, by the first device, updated location information comprising an updated location of the first device, the updated location information being sent based on passage of a predetermined time interval since sending previous location information comprising a previous location of the first device, displacement of the first device by a predetermined distance relative to a previous location of the first device, or both.

436. Claim 5 of the '251 patent is invalid because it is anticipated by FBCB2 or, at a minimum, is obvious over FBCB2 in view of the knowledge of a POSA. The limitations of claim 1 are anticipated by FBCB2, or, at a minimum, obvious in view of FBCB2, for the reasons discussed above. Claim 5 is anticipated or obvious for the additional reasons described below.

437. As discussed above with respect to claim 1, each FBCB2 device continuously reported its updated location to the server. *See* SIEGEL000009-10; SIEGEL000014. The location reporting rate was time and distance triggered, such that a device would send updated location information at a predetermined time interval, unless it moved further than a pre-specified distance before that time interval had passed. *See* APL-AGIS_00012859. U.S. Patent No. 5,672,840, of which I am named inventor, describes the reporting filter incorporated in the FAAD C2I system, based on an angular filter (e.g., reporting whenever the display was rotated more than a certain amount). *See* SIEGEL000374 at 5:31-35. In FBCB2 (starting in 1995), we extended that concept of a filter for reporting based an angular threshold to one of a threshold based on time and motion. *See* SIEGEL000990-91.

D. Claim 6 is Anticipated by FBCB2, or, at a Minimum, is Obvious Over FBCB2 in View of the Knowledge of a POSA at the Time of the Invention

438. Claim 6 of the '251 patent depends from claim 1. Claim 6 of the '251 patent recites:

> 6. The method of claim 1, further comprising identifying second user interaction with the interactive display selecting at least one of the user-selectable symbols corresponding to at least one of the second devices and user interaction with the display specifying an action and, based thereon, initiating a phone call or phone conference with the at least one second device.

example, if the leader of a platoon became incapacitated, a new platoon leader might need to be appointed in his place. A senior officer with appropriate permissions could assign that role to a different member of the platoon, and thereby send the new leader a message asking the leader to join the group or groups with which a platoon leader needed to share location information and engage in remote control operations.

467. U.S. Patent No. 6,212,559, of which I am a named inventor, covers the process of setting up groups in FBCB2. *See* SIEGEL000333-355 (the "'559 patent"). My team at TRW developed this patent as part of our work on FBCB2, and we incorporated many of the capabilities outlined in the patent in FBCB2. The '559 patent covers techniques for configuring a computer network to allow for rapid reconfiguration due to changes in the location, identity, or network topology. *See* '559 pat. at 5:23-58. Specifically, the '559 patent discloses software consisting of network configuration tools in which each unit and user (e.g., brigade, company, fleet, ship, aircraft group) is grouped and interrelated with other units according to a "unit task organization" set up within the software. *See* '559 at 5:47-6:4. A user could use the "unit task organization" capability in order to define their desired groups. *See* '559 pat. at 5:59-6:11; *see also id*. at 7:1-4, 7:33-42. A user could also thereby define the set of users who could participate in each group. *See* '559 pat. at 8:16-24. Users could be given permissions to access more than one group. *See* '559 pat. at 7:49-67; 9:6-40. A user with appropriate permissions could assign another user to a group at any time. The patent explains that, when such an assignment was made, the software would disseminate the assignment to the user; upon receipt of the message (i.e., when the device was turned on and logged in), the device would begin participating in the group. *See* '559 pat. at 8:31-51. These features were incorporated into FBCB2, as described in the preceding paragraph.

468. The method of setting up groups in FBCB2 was tailored to meet the security and operational needs of the military (e.g., ensuring users could only join groups of the appropriate security clearance and ensuring that commanders received acknowledgement of orders). A person of ordinary skill in the art at the time of the invention would have understood that the protocols described above could be easily modified in various ways (e.g., requiring fewer confirmations or additional confirmations before joining users to a group; allowing all users to invite each other to join any group or to request access to any group, etc.) to suit different needs. Thus, if this limitation is not anticipated by FBCB2, it would have been obvious in view of FBCB2 and the knowledge of a person of ordinary skill in the art at the time of the invention.

3. "wherein participating in the group includes sending first location information to a server and receiving second location information from the server, the first location information comprising a location of the first device, the second location information comprising a plurality of locations of a respective plurality of second devices included in the group;"

469. FBCB2 devices exchanged location information via a server. Each device obtained its own location from a GPS receiver attached to (or built into) the device.[20] The location information consisted of latitude and longitude coordinates determined by a GPS unit installed in the FBCB2 device. *See also* SIEGEL000009-10; SIEGEL000014; SIEGEL000782. Each device reported its latitude and longitude to the server, and the server broadcast that information to other FBCB2 devices. *See also* SIEGEL000009-10.

470. The servers in FBCB2 consisted of computers mounted in army vehicles. That is, individual FBCB2 units were designated to receive information from FBCB2 devices and forward

[20] Location information could also be obtained by other methods, including radio triangulation of the ground-to-ground radio links or an inertial navigation system on the vehicle. The FBCB2 software automatically determined which of these was the most accurate at the moment, and used that most-accurate position as the FBCB2 position to report to the FBCB2 network.

individuals' log-in names, role or title, or group name (e.g. a particular platoon). This addressee information was sent to the server, and the server routed the information to the appropriate IP address. The sender never, however, had to know the IP address of the intended recipient(s).

485. U.S. Patent No. 6,212,559, (the "'559 patent") of which I am a named inventor, covers the process of setting up groups and facilitating communication among groups in FBCB2. *See* SIEGEL000333-355. My team at TRW developed this patent as part of our work on FBCB2, and we incorporated many of the capabilities outlined in the patent in FBCB2. Figure 17A of the '559 patent shows that users within a communication network were identified by a user ID; a user who was attempting to modify the network or select ot her users for communications would select those users' IDs. *See* '559 pat. Fig. 7; *id*. at 4:48-49. This feature was implemented as part of FBCB2.

I. Claim 27 is Anticipated by FBCB2, or, at a Minimum, is Obvious Over FBCB2 in View of the Knowledge of a POSA at the Time of the Invention

486. Claim 27 of the '251 patent depends from claim 24. Claim 27 of the '251 patent recites:

> 27. The system of claim 24, wherein the second map is a satellite image.

487. Claim 27 of the '251 patent is invalid because it is anticipated by FBCB2 or, at a minimum, is obvious over FBCB2 in view of the knowledge of a POSA. The limitations of claim 24 are anticipated by FBCB2, or, at a minimum, obvious in view of FBCB2, for the reasons discussed above. Claim 27 is anticipated or obvious for the additional reasons described below.

488. The second FBCB2 map could be a georeferenced satellite image or aerial photograph. FBCB2 was compatible with and employed a range of georeferenced map types, including VPF, CADRG, DTED, ASRP, and NITF maps, and georeferenced satellite images and georeferenced aerial photographs. *See* SIEGEL000311 (listing some map types); *see also*