(12) **United States Patent**
Lincke et al.

(10) **Patent No.:** US 6,253,326 B1
(45) **Date of Patent:** Jun. 26, 2001

(54) **METHOD AND SYSTEM FOR SECURE COMMUNICATIONS**

(75) Inventors: **Scott D. Lincke**, San Carlos; **Ronald Marianetti, II**, Morgan Hill, both of CA (US)

(73) Assignee: **Palm, Inc.**, Santa Clara, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/086,888**

(22) Filed: **May 29, 1998**

(51) Int. Cl.^{7} **H06F 1/24**

(52) **U.S. Cl.** **713/201**; 713/200; 713/168; 380/255; 380/270

(58) **Field of Search** 380/255, 270, 380/277, 281, 283; 713/168, 171, 193, 200, 201

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,432,057	2/1984	Daniell et al.	364/300
4,807,182	2/1989	Queen	364/900
4,866,611	9/1989	Cree et al.	364/300
4,875,159	10/1989	Cary et al.	364/200
4,956,809	9/1990	George et al.	364/900
5,001,628	3/1991	Johnson et al.	364/200
5,065,360	11/1991	Kelly	395/800
5,124,909	6/1992	Blakely et al.	395/200
5,142,619	8/1992	Webster, III	395/157
5,159,592	10/1992	Perkins	370/85.7

(List continued on next page.)

OTHER PUBLICATIONS

Schneier, Applied Cryptography 1995, sec. 2.4.*
Brown, Mark R., "Using Netscape 3", (1996), pp. 7–38.
McFedrie, Paul, "Windows 95 Unleashed", (1996), pp. 1114–1152.

"Connectivity Pack for the HP 95LX" User's Guide, Hewlett Packard Co., (1991), pp. 1–1 to 6–5.
Droms, R., "Dynamic Host Configuration Protocol", Request for Comments #1541, Oct. 1993, 24 pages.
"Redline, Strikeout, and Document Comparison", pp. 429–435.
"LapLink for Windows SpeedSync", printed from Traveling Software, Inc. website.
"Introducing Windows 95" Microsoft Windows 93—For the Microsoft Windows Operating System, Microsoft Corporation, (1995), p. 66.
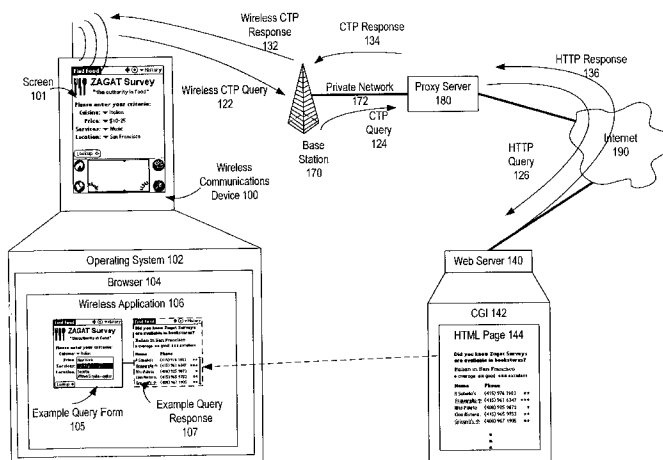
(List continued on next page.)

Primary Examiner—Thomas R. Peeso
(74) *Attorney, Agent, or Firm*—Van Mahamedi; Wilson Sonsini Goodrich & Rosati

(57) **ABSTRACT**

A communications system and methods for securely transmitting a message between a wireless client and a proxy server are provided. A method for transmitting a message from the wireless client to a proxy server is provided. The message includes at least one packet of data and is encrypted using a data encryption key. The data encryption key is encrypted using a proxy server public key prior to sending the encrypted data encryption key to the proxy server. A method for transmitting a message from the proxy server to the wireless client is also provided. The proxy server recovers the data encryption key using the proxy server private key corresponding to the proxy server public key. The proxy server encrypts the message using the data encryption key and transmits the encrypted message to the wireless client. A communications system for secure communications comprising a source of data, a proxy server and a wireless client is also provided. Each transaction in the communications system comprises at least one request message and at least one response message. For each transaction, the wireless client encrypts a data encryption key using a proxy server public key. Messages exchanged between the wireless client and the proxy server are encrypted using the transaction specific data encryption key.

36 Claims, 14 Drawing Sheets

U.S. PATENT DOCUMENTS

5,187,787	2/1993	Skeen et al.	395/600
5,210,868	5/1993	Shimada et al.	395/600
5,235,679	8/1993	Yoshizawa et al.	395/156
5,237,678	8/1993	Kuechler et al.	395/600
5,251,291	10/1993	Malcolm	395/146
5,261,045	11/1993	Scully et al.	395/161
5,261,094	11/1993	Everson et al.	395/600
5,272,628	12/1993	Koss	364/419.19
5,283,887	2/1994	Zachery	395/500
5,301,313	4/1994	Terada et al.	395/600
5,315,709	5/1994	Alston, Jr. et al.	395/600
5,327,555	7/1994	Anderson	395/600
5,333,252	7/1994	Brewer, III et al.	395/148
5,339,434	8/1994	Rusis	395/700
5,355,476	10/1994	Fukumura	395/600
5,379,057	1/1995	Clough et al.	345/173
5,392,390	2/1995	Crozier	395/161
5,434,994	7/1995	Shaheen et al.	395/500
5,463,772	10/1995	Thompson et al.	395/600
5,475,833	12/1995	Dauerer et al.	395/600
5,488,685	1/1996	Palmer et al.	395/157
5,519,606	5/1996	Frid-Nielsen et al.	364/401
5,537,592	7/1996	King et al.	395/600
5,544,356	8/1996	Robinson et al.	395/600
5,546,539	8/1996	Poling	395/200.05
5,572,528	11/1996	Shuen	370/85.13
5,574,859	11/1996	Yeh	395/200.01
5,592,669	1/1997	Robinson et al.	395/622
5,598,536	1/1997	Slaughter, III et al.	395/200.16
5,647,002	7/1997	Brunson	380/49
5,649,195	7/1997	Scott et al.	395/617
5,666,362	9/1997	Chen et al.	370/420
5,666,530	9/1997	Clark et al.	395/617
5,673,322 *	9/1997	Pepe et al.	380/49
5,684,990	11/1997	Boothby	395/619
5,696,702	12/1997	Skinner et al.	364/551.01
5,699,513 *	12/1997	Feigen et al.	713/201
5,704,029	12/1997	Wright, Jr.	395/149
5,706,509	1/1998	Tso	395/617
5,710,922	1/1998	Alley et al.	395/617
5,724,510	3/1998	Arndt et al.	395/200.5
5,727,159	3/1998	Kikinis	395/200.76
5,727,202	3/1998	Kucala	395/610
5,729,452	3/1998	Smith et al.	364/424.03
5,742,820	4/1998	Perlman et al.	395/617
5,745,699	4/1998	Lynn et al.	395/200.75
5,758,354	5/1998	Huang et al.	707/201
5,761,439	6/1998	Kar et al.	395/200.78
5,802,312	9/1998	Lazaridis et al.	395/200.68
5,812,819	9/1998	Rodwin et al.	395/500
5,819,274	10/1998	Jackson, Jr.	707/10
5,857,191 *	1/1999	Blackwell, Jr. et al.	707/10
5,861,883	1/1999	Cuomo et al.	345/326
5,911,141	6/1999	Kelley et al.	707/10
5,918,013	6/1999	Mighdoll et al.	393/200.47
5,948,066	9/1999	Whalen et al.	709/229
6,006,258 *	12/1999	Kalajan	709/219

OTHER PUBLICATIONS

Madnick, S. et al., "Logical Connectivity: Applications, Requirements, Architecture, and Research Agenda", IEEE (1991), pp. 142–153.

"IntelliLink" The Intelligent Link, Microsoft Windows 3 Personal Information Managers, IntelliLink, Inc., (1990).

Zahn, L. et al., "Network Computing Architecture", Prentice Hall, New Jersey, pp. 1–209.

Cobb, D. et al., "Paradox 3.5 Handbook" Third Edition, Borland Bantam, New York, Oct. 1991, pp. 803–816.

Alfieri, V., "The Best Book of: WordPerfect Version 5.0", Hayden Books, Indianapolis, IN (1988), pp. 151–165.

"PC–Link Release 2 for the Casio B.O.S.S. Business Organizer Scheduling System", Travelling Software, Inc., (1989), pp. 1–60.

"I/O Applications Note" Serial Communications Using the HP 95LX, Hewlett Packard, pp. 1–12.

"Open Network Computing Technical Overview", Sun Microsystems, Inc., pp. 1–32.

"Sharp Organizer Link II, Model OZ–890" Operation Manual, pp. 1–105.

Dialog search results for references generally related to Palmtops, 15 pages.

Lamming, M., "Towards Future Personalised Information Environments", Technical Report EPC–1994–104, Proc. of FRIEND21, '94 Intl.Symp. on Next Generation Human Interface, Feb. 2–4, 1994, Japan, pp. 1–3.

* cited by examiner

Figure 1

Start

Define Wireless Application
210

Create Server Web Site Content
220

Load Wireless Application onto Wireless Device
230

Build Distributed Web Site Process 202

Fill in Wireless Application Query Form and Send CTP Query
240

Proxy Server Converts CTP Query to HTTP Request and Sends Request
250

Query
204

Web Server Generates and Sends HTTP Response to Proxy Server
260

Proxy Server Converts HTTP Response to CTP Response and Sends CTP Response
270

Wireless Communications Device Displays Response from CTP Response
280

Response
206

Stop

Figure 2

Figure 3

Launcher 303

Apps 3:30p ▬ ▼Wireless
?! What's New?   ♫ Quote.Com
∼ Britannica   ✿ Roget's
✓ Corporate News ★ Top 40
✗ Directions   ✗ Traffic
◔ Directory $ Vegas Odds
?$ Find ATM   ✳ Weather
?✗ Find Movies
?"↑ Find Food
✳ Local News
↑ PalmPilot.Net

Example Query Form 105

Find Food   ◀ ⊕ ▼History
♫Ⓘ♈ ZAGAT Survey
   "the authority in food"

Please enter your criteria:
  Cuisine: ▼ Italian
  Price: | New York |
  Services: | San Francisco |
  Location: | Seattle |
             | Within 5 mile radius |

(Lookup ⊕)

Completed Query Form 305

Find Food   ◀ ⊕ ▼History
♫Ⓘ♈ ZAGAT Survey
   "the authority in food"

Please enter your criteria:
  Cuisine: ▼ Italian
  Price: ▼ $10-25
  Services: ▼ Music
  Location: ▼ San Francisco

(Lookup ⊕)

Toolbar 310

Example Query Response
107

Find Food   ◀ ⊕ ▼History
Did you know Zagat Surveys
are available in bookstores?

Italian in San Francisco
* average ** good *** excellent

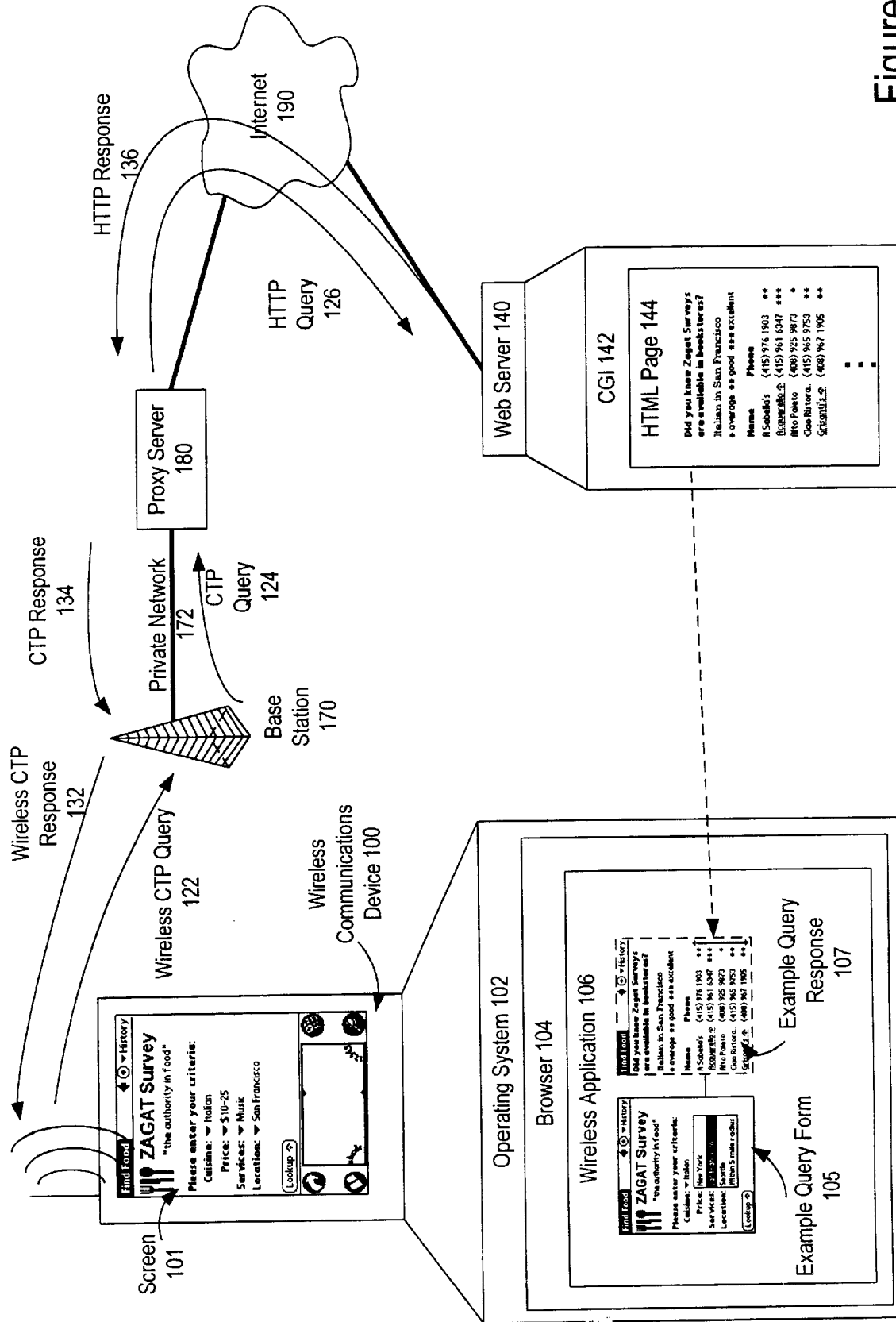| Name	Phone	
A Sabella's	(415) 976 1903	**
Acquerello ⊕	(415) 961 6347	***
Alto Paleto	(408) 925 9873	*
Ciao Ristora..	(415) 965 9753	**
Grisanti's ⊕	(408) 967 1905	**

◀━━━━━━━━━━━━━━▶

DOCKET ALARM
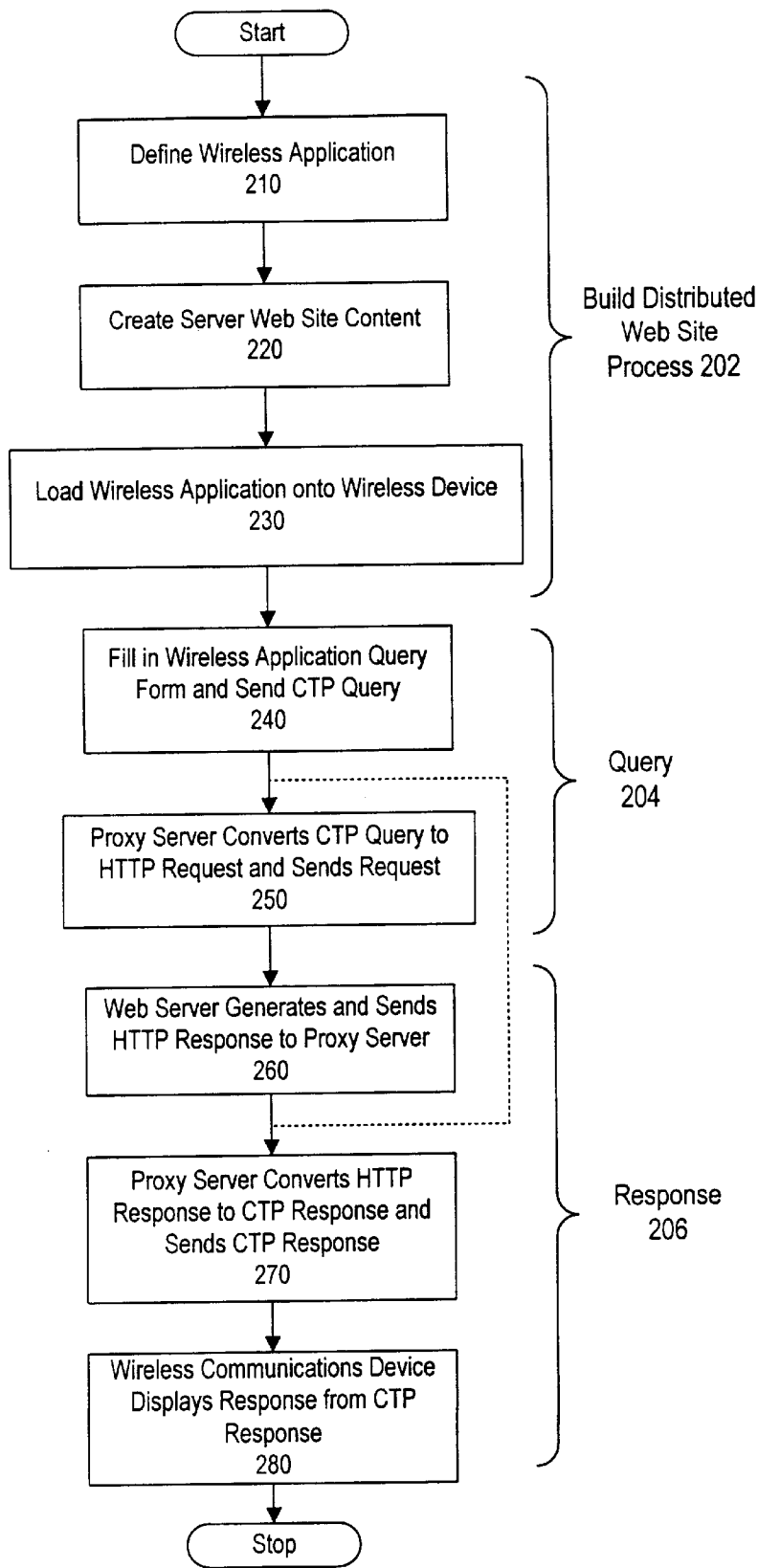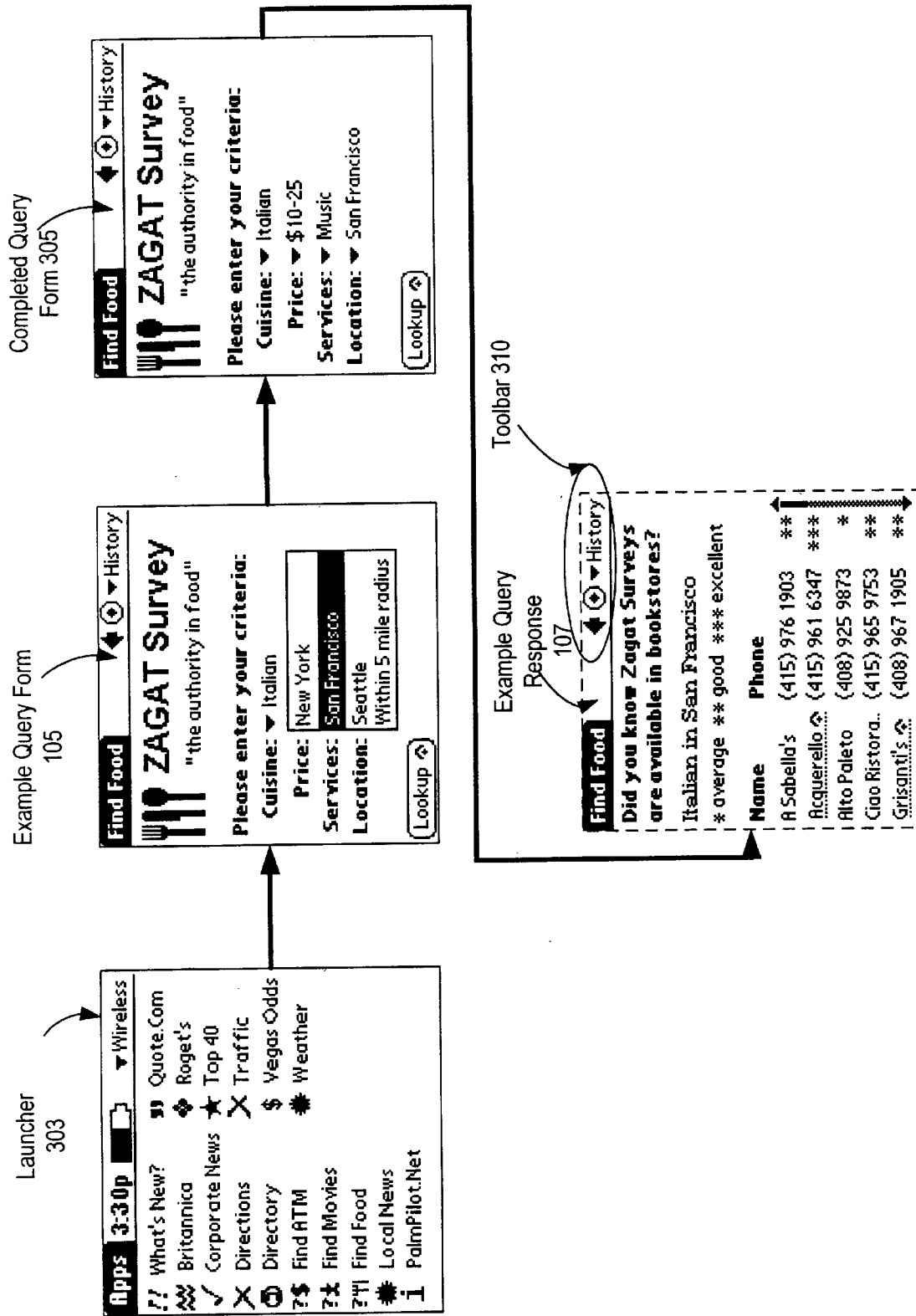
Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.