US 20080133708A1

(19) **United States**

(12) **Patent Application Publication**

Alvarado et al.

(10) **Pub. No.: US 2008/0133708 A1**

(43) **Pub. Date: Jun. 5, 2008**

(54) **CONTEXT BASED ACTION**

(76) Inventors: **Billy Alvarado**, Menlo Park, CA (US); **Ido Ariel**, Palo Alto, CA (US); **Robert Paul van Gent**, Redwood City, CA (US)

Correspondence Address:
CARR & FERRELL LLP
2200 Geng Road
Palo Alto, CA 94303

(21) Appl. No.: **11/925,959**

(22) Filed: **Oct. 28, 2007**

Related U.S. Application Data

(63) Continuation of application No. 11/363,912, filed on Feb. 27, 2006, which is a continuation of application No. 11/362,488, filed on Feb. 24, 2006, which is a continuation of application No. 11/217,203, filed on Aug. 31, 2005.

(60) Provisional application No. 60/704,781, filed on Aug. 1, 2005.

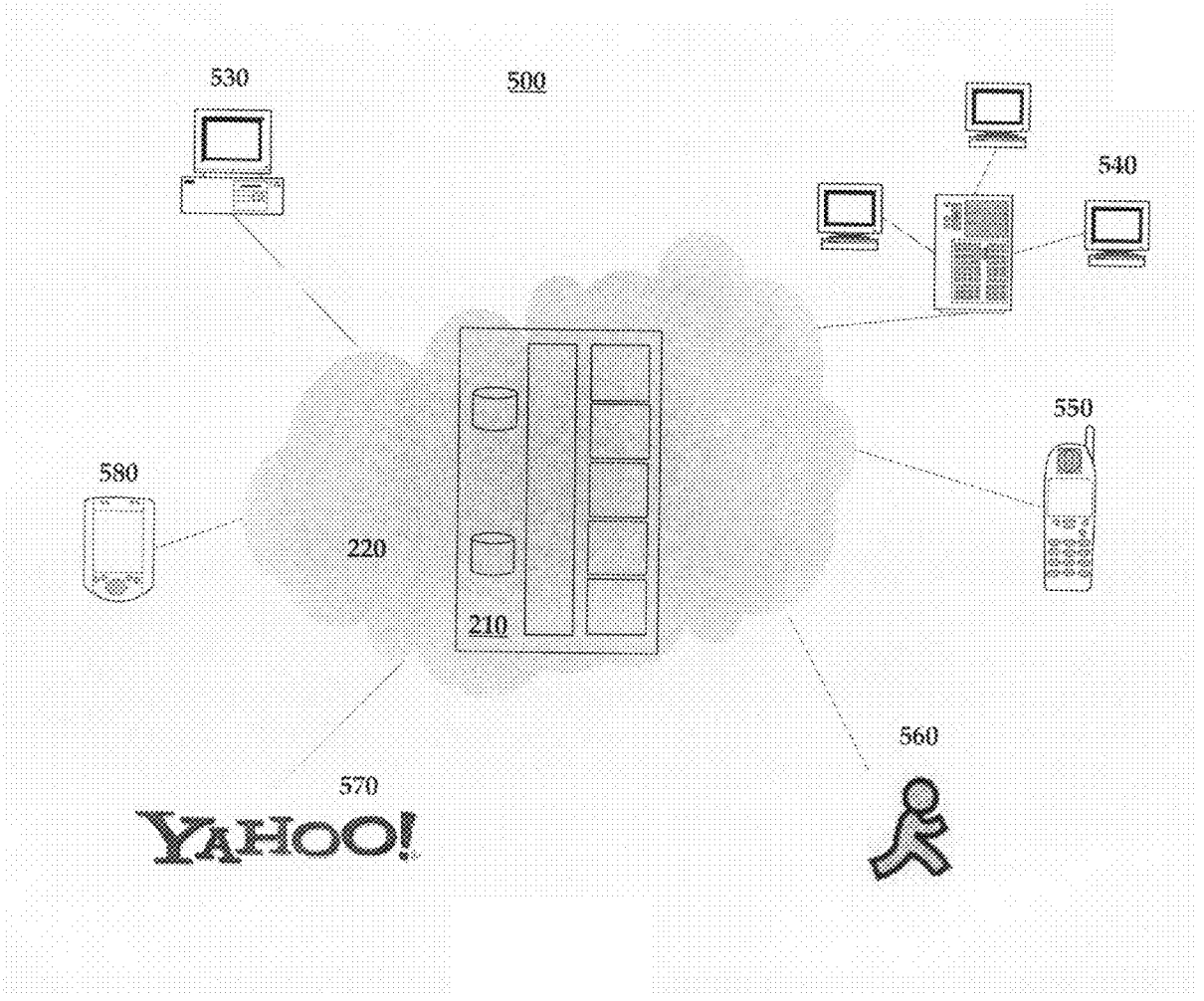
Publication Classification

(51) **Int. Cl.**
G06F 15/16 (2006.01)

(52) **U.S. Cl.** **709/218**

(57) **ABSTRACT**

Means for allowing users to manage and make productive use of PIM data are provided. User status is determined by certain contextual indicia whereby other parties may contact the user through the most appropriate means as reflected by that contextual indicia. Information concerning presence, status, location, availability and so forth are aggregated from various PIM sources and communicated to other parties who initiate contact with the user in light of the aggregated information. Various groups and permissions may be implemented with regard to the collection and sharing of information.



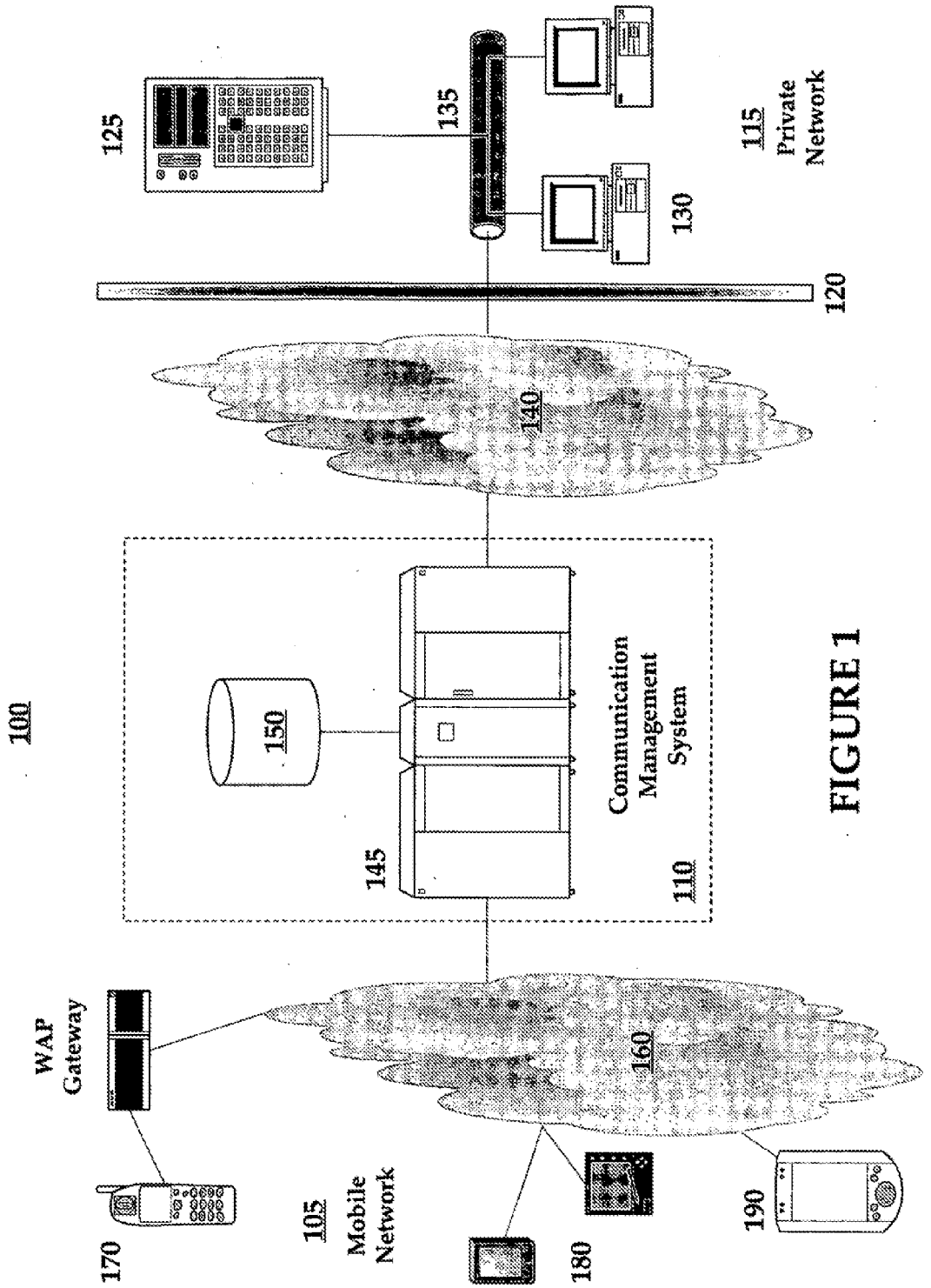

100
125
135
115
Private
Network
130
120
140
150
145
Communication
Management
System
110
WAP
Gateway
160
170
105
Mobile
Network
180
190

FIGURE 1

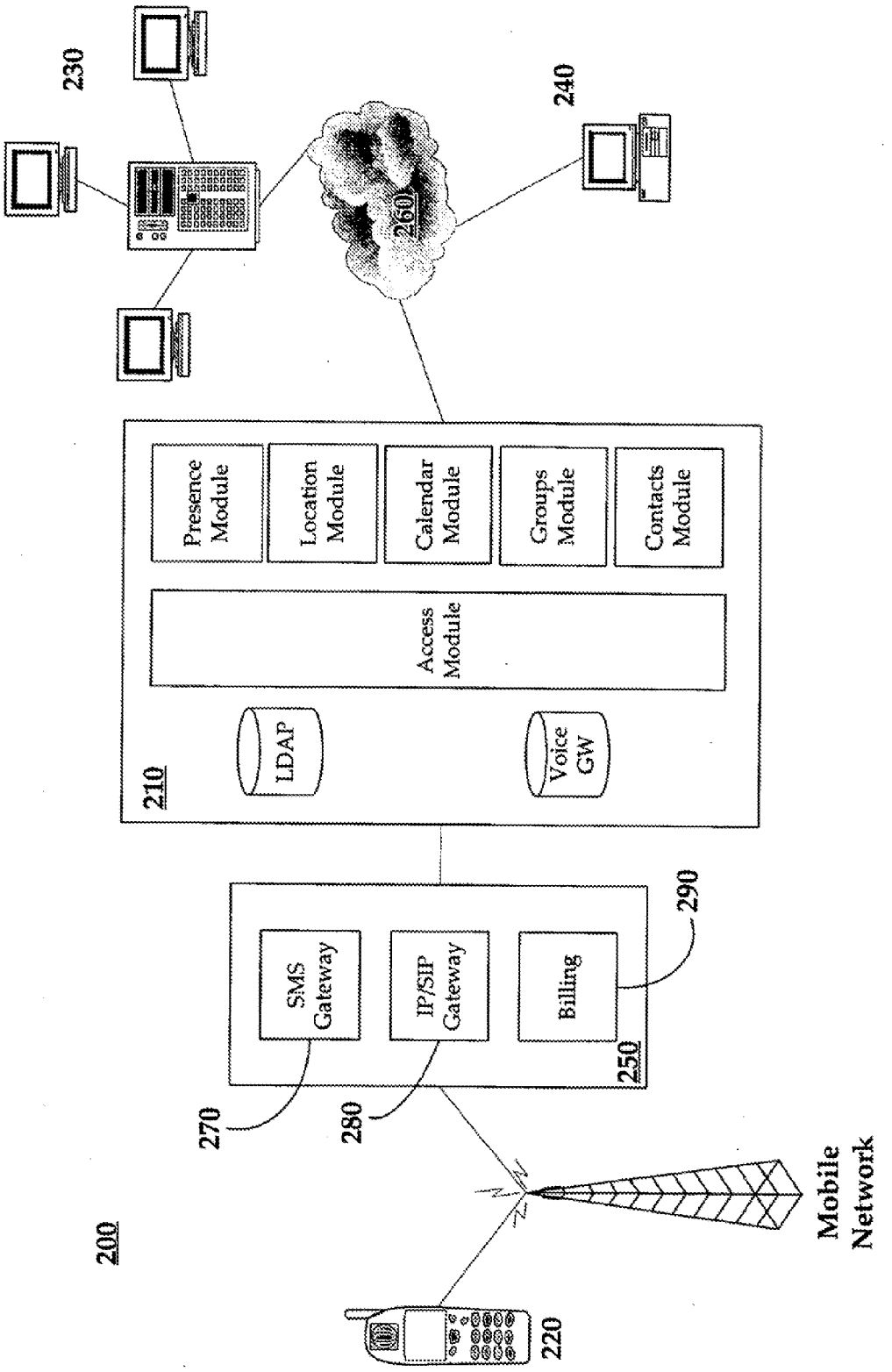

200
230
240
260
210
Presence Module
Location Module
Calendar Module
Groups Module
Contacts Module
Access Module
LDAP
Voice GW
250
SMS Gateway
IP/SIP Gateway
Billing
290
270
280
Mobile Network
220

FIGURE 2

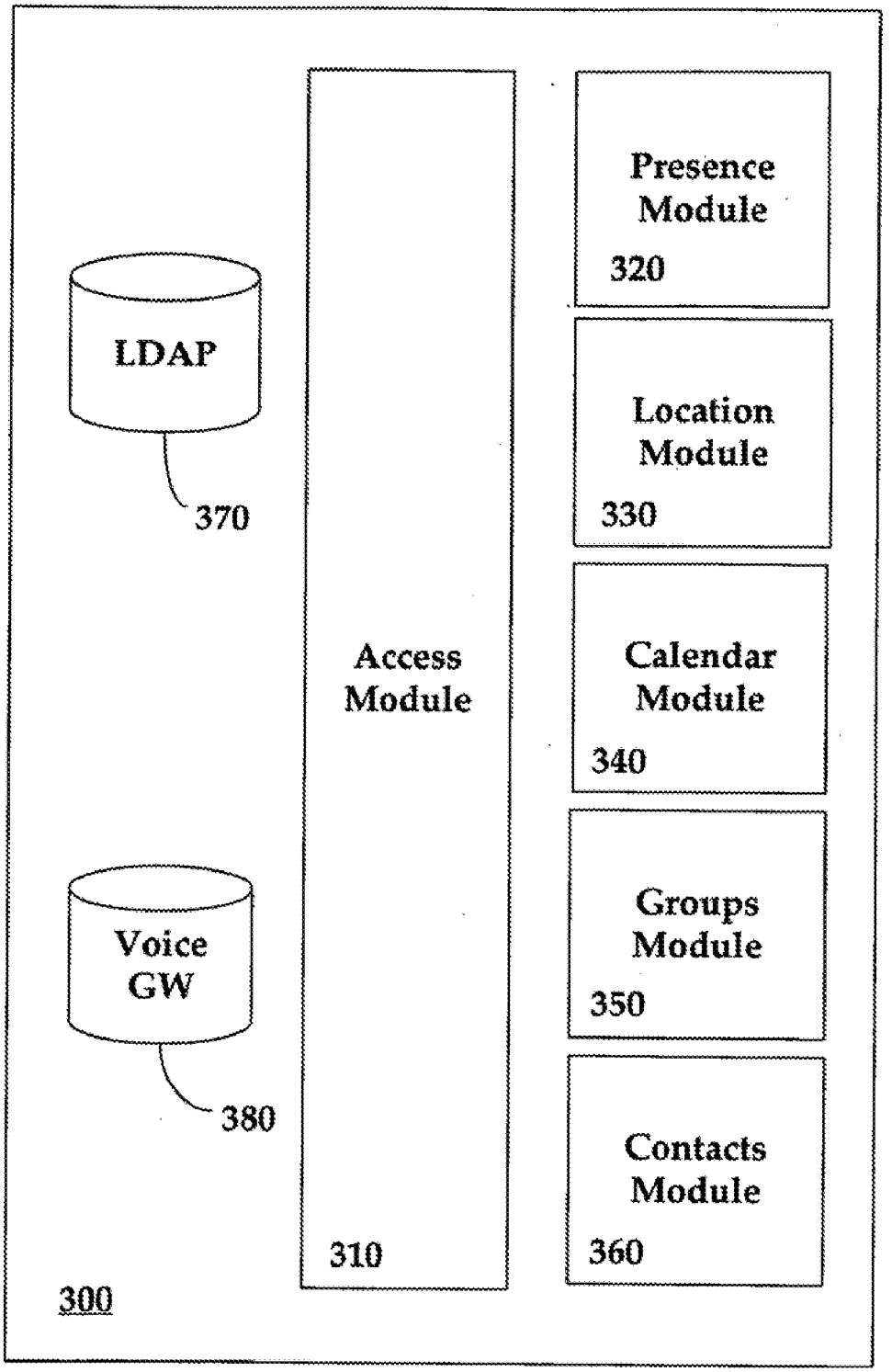

LDAP
370
Voice GW
380
Access Module
310
Presence Module
320
Location Module
330
Calendar Module
340
Groups Module
350
Contacts Module
360
300

FIGURE 3

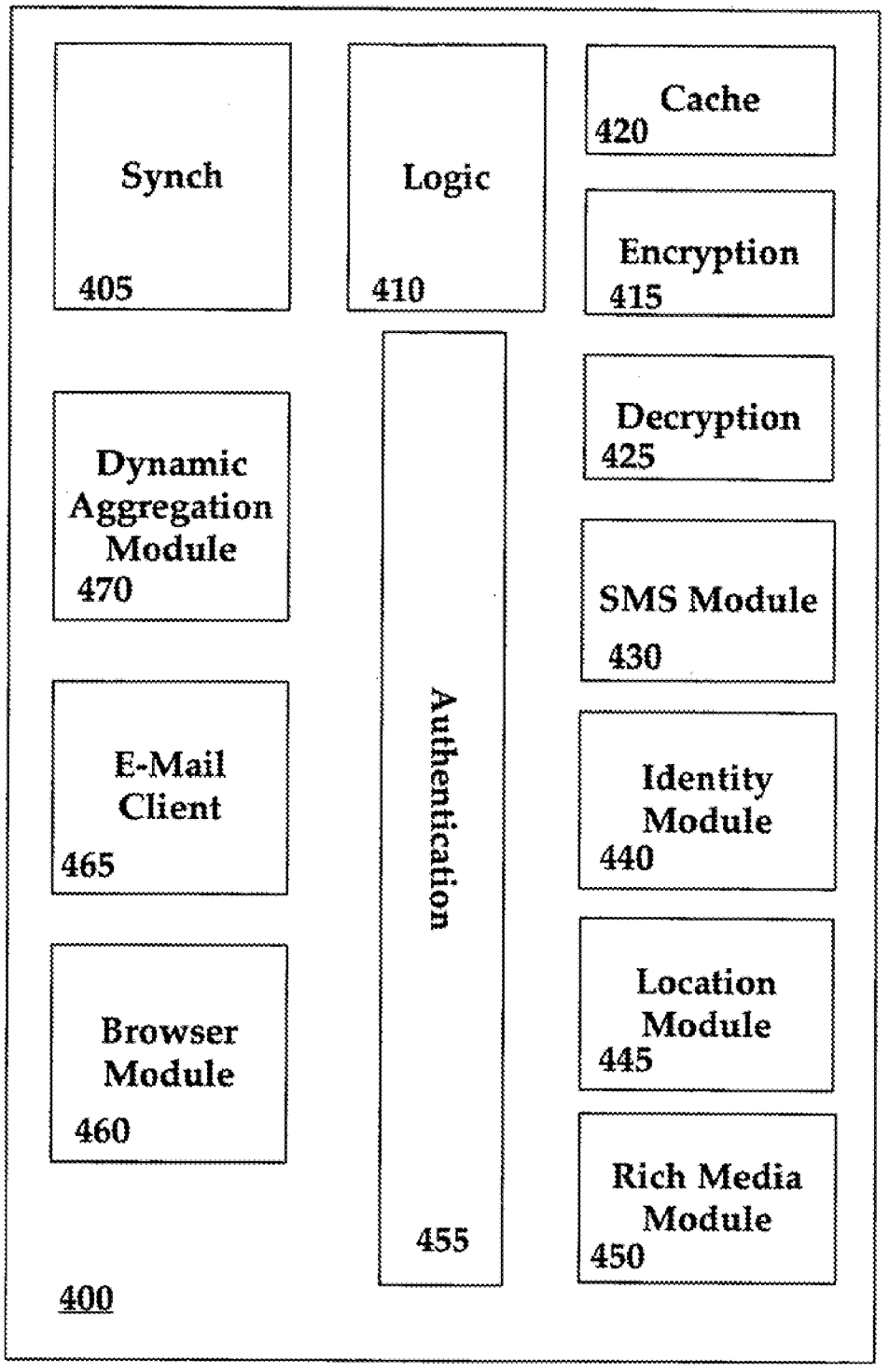

Synch
405
Logic
410
Cache
420
Encryption
415
Decryption
425
Dynamic Aggregation Module
470
SMS Module
430
E-Mail Client
465
Identity Module
440
Location Module
445
Browser Module
460
Rich Media Module
450
Authentication
455
400

FIGURE 4

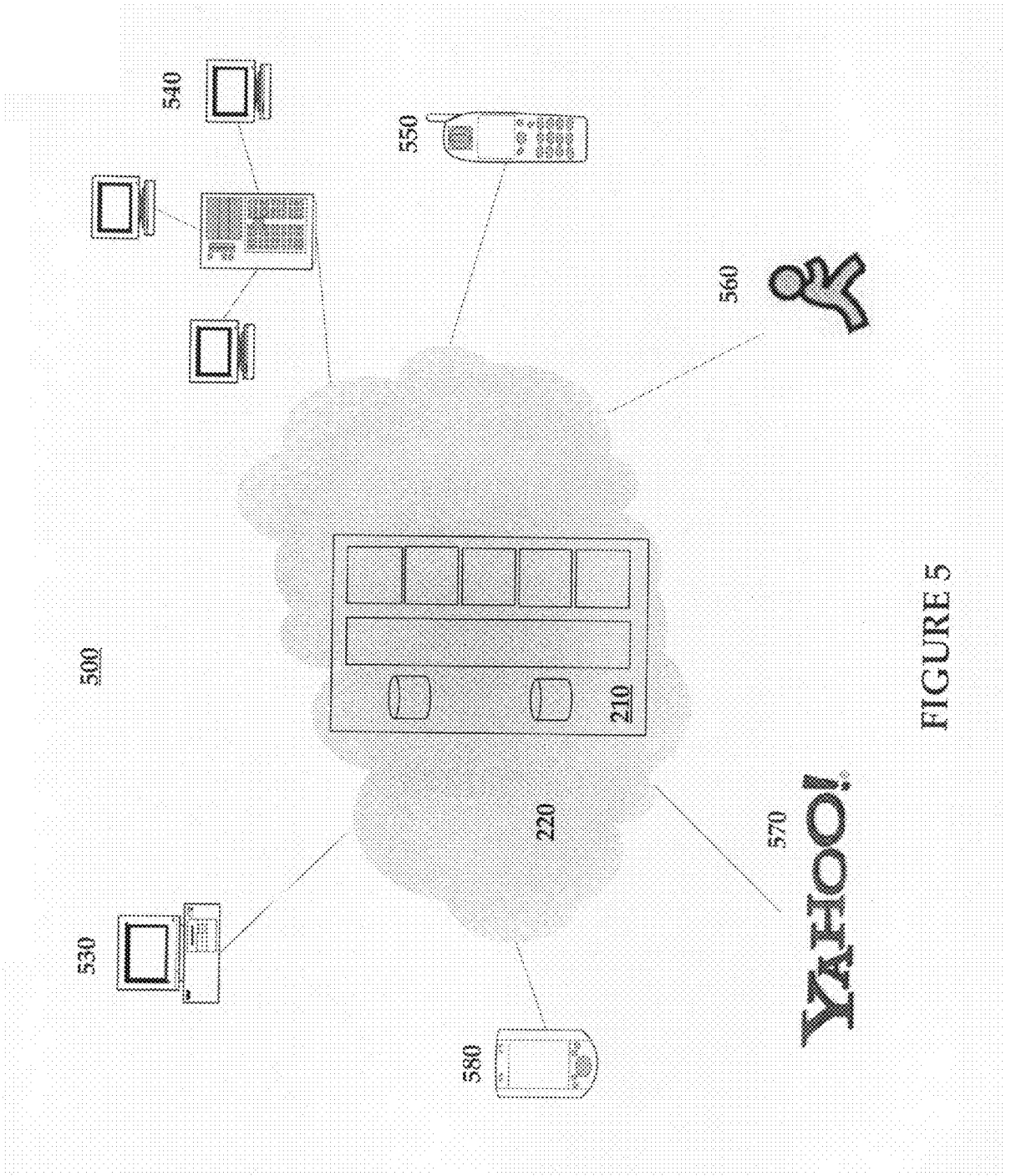


FIGURE 5

FIG. 6A

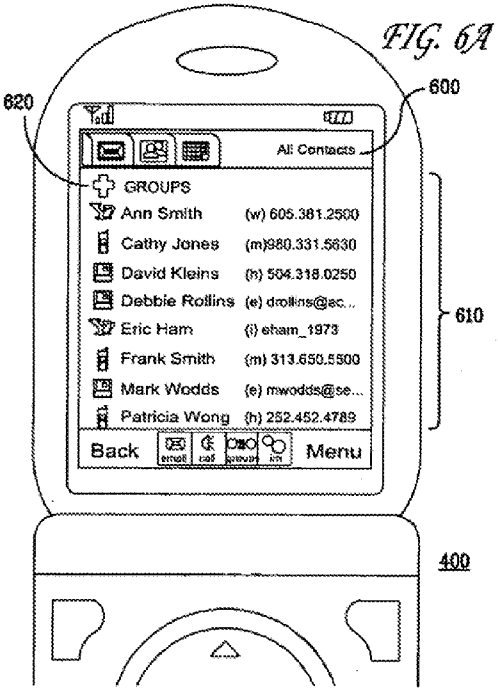

620
600
All Contacts
GROUPS
Ann Smith (w) 605.381.2500
Cathy Jones (m)980.331.5630
David Kleins (h) 504.318.0250
Debbie Rollins (e) drollins@ac...
Eric Ham (i) eham_1973
Frank Smith (m) 313.650.5500
Mark Wodds (e) mwodds@se...
Patricia Wong (h) 252.452.4789
Back
Menu
610
400

FIG. 6B

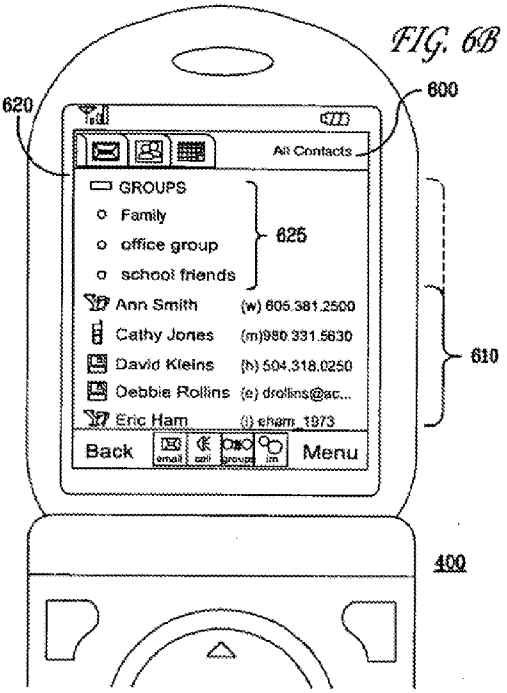

620
600
All Contacts
GROUPS
Family
office group
school friends
625
Ann Smith (w) 605.381.2500
Cathy Jones (m)980.331.5630
David Kleins (h) 504.318.0250
Debbie Rollins (e) drollins@ac...
Eric Ham (i) eham_1973
Back
Menu
610
400

FIG. 6C

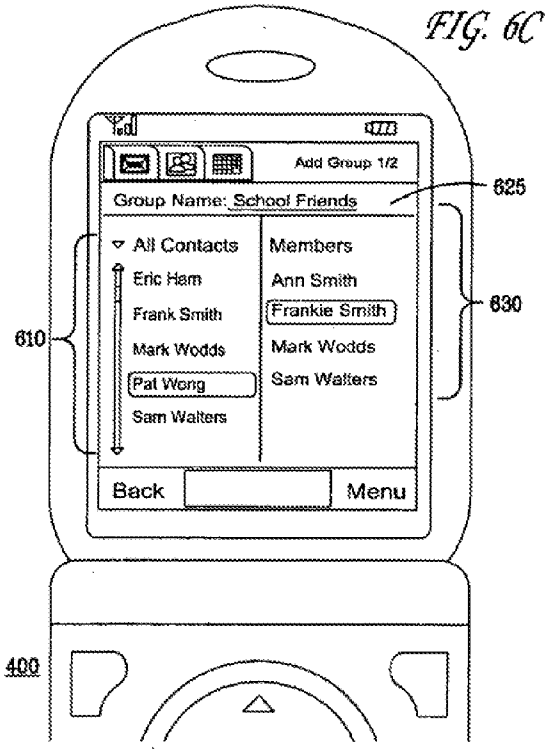

Add Group 1/2
Group Name: School Friends
625
All Contacts
Eric Ham
Frank Smith
Mark Wodds
Pat Wong
Sam Walters
610
Members
Ann Smith
Frankie Smith
Mark Wodds
Sam Walters
630
Back
Menu
400

FIG. 6D

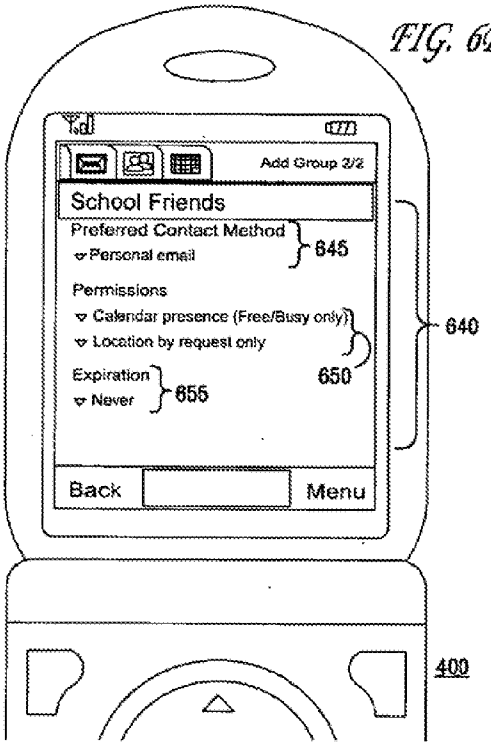

Add Group 2/2
School Friends
Preferred Contact Method
Personal email
645
Permissions
Calendar presence (Free/Busy only)
Location by request only
650
Expiration
Never
655
640
Back
Menu
400

FIG. 6E

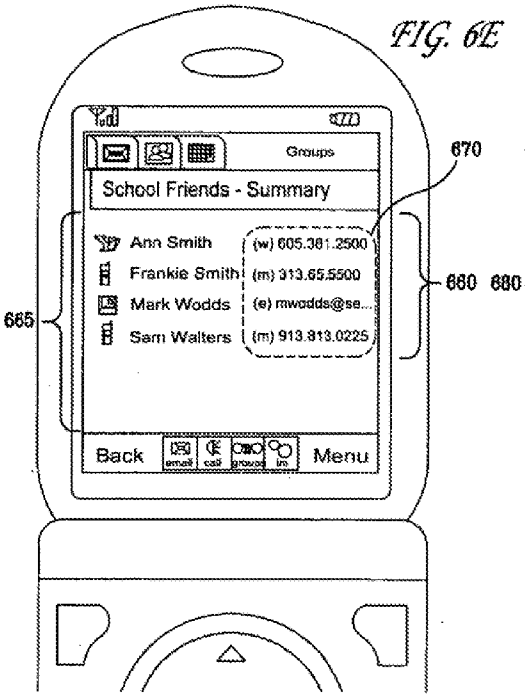

Groups
School Friends - Summary
Ann Smith
Frankie Smith
Mark Wodds
Sam Walters
(w) 605.381.2500
(m) 313.65.5500
(e) mwodds@se...
(m) 913.813.0225
Back
Menu
670
660
665

FIG. 6F

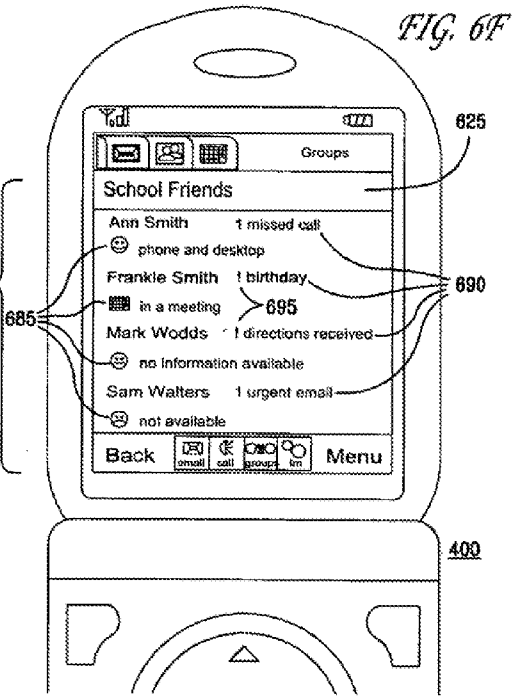

Groups
School Friends
Ann Smith 1 missed call
phone and desktop
Frankie Smith ! birthday
in a meeting
695
Mark Wodds ! directions received
no information available
Sam Walters 1 urgent email
not available
Back
Menu
625
680
685
690
400

FIG. 7A

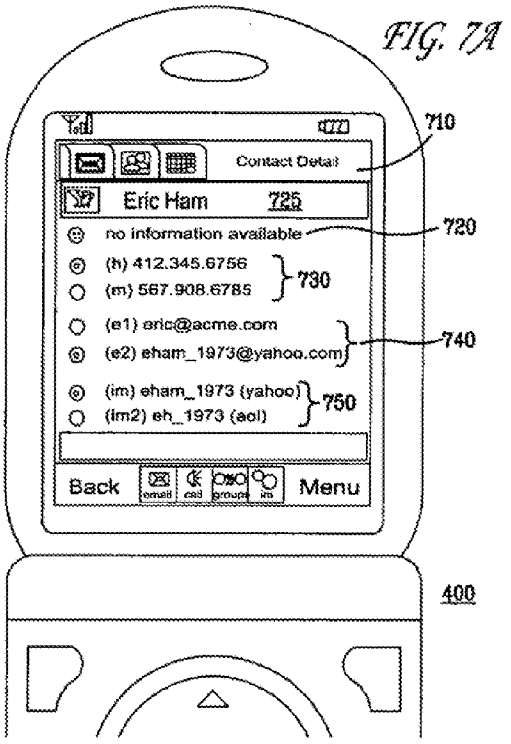
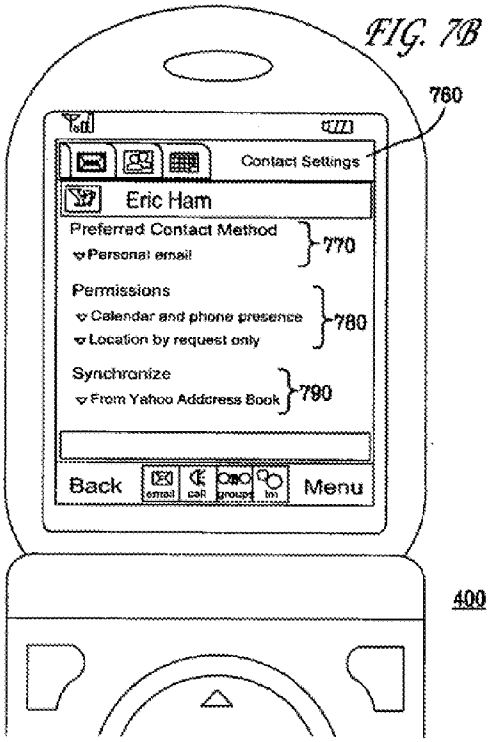

710
Contact Detail
Eric Ham
725
720
no information available
(h) 412.345.6756
(m) 567.908.6785
730
(e1) eric@acme.com
(e2) eham_1973@yahoo.com
740
(im) eham_1973 (yahoo)
(im2) eh_1973 (aol)
750
Back
email
call
groups
im
Menu
400

FIG. 7B


760
Contact Settings
Eric Ham
Preferred Contact Method
Personal email
770
Permissions
Calendar and phone presence
Location by request only
780
Synchronize
From Yahoo Address Book
790
Back
email
call
groups
im
Menu
400

CONTEXT BASED ACTION

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] The present application is a continuation and claims the priority benefit of U.S. patent application Ser. No. 11/363,912 filed Feb. 27, 2006 and entitled "Context-Based Action," which is a continuation and claims the priority benefit of U.S. patent application Ser. No. 11/362,488 filed Feb. 24, 2006 and entitled "Context-Aware Data Presentation," which is a continuation and claims the priority benefit of U.S. patent application Ser. No. 11/217,203 filed on Aug. 31, 2005 and entitled "Universal Data Aggregation," which claims the priority benefit of U.S. provisional patent application No. 60/704,781 filed on Aug. 1, 2005 and entitled "Networked Personal Information Management." The disclosures of the aforementioned application are incorporated herein by reference.

[0002] The present application is related to U.S. patent application Ser. No. 10/339,368 filed Jan. 8, 2003 and entitled "Connection Architecture for a Mobile Network." The present application is also related to U.S. patent application Ser. No. 10/339,369 filed Jan. 8, 2003 and entitled "Secure Transport for Mobile Communication Network." These related applications are commonly assigned and are incorporated herein by reference.

[0003] The present application is also related to U.S. patent application Ser. No. 11/229,340 filed Sep. 16, 2005 and entitled "Linking of Personal information Management Data" and U.S. patent application Ser. No. 11/303,048 filed Dec. 14, 2005 and entitled "Publishing Data in an Information. Community."

BACKGROUND OF THE INVENTION

[0004] 1. Field of the Invention

[0005] The present invention relates to control and utilization of personal information management (PIM) data such as calendar and contact information in the context of personal and professional activities. More specifically, the present invention relates to control and utilization of PIM data in the context of mobile devices such as smart phones and PDAs.

[0006] 2. Description of Related Art

[0007] Presently available groupware applications and other related collaboration products that facilitate shared work and access to documents and information (e.g., data pools) are, to a certain extent, 'closed networks.' That is, certain information cannot be shared amongst users of different groupware products because the protocols setting forth the rules and standards by which communication of data takes place are different. For example, an individual using Microsoft® Outlook® as an e-mail client via a Microsoft® Exchange® Server can exchange e-mail messages with an individual using a Lotus® Notes client via an IBM® Lotus® Domino Server. Those same users cannot, however, access the contact or calendar data of one another due to protocol differences between an Exchange® Server and a Domino Server.

[0008] There have been some software applications mat have attempted to bridge the protocol gap such as the Trillian instant messaging (IM) client from Cerulean Studios. Trillian is a multi-protocol chat client that supports AOL® Instant Messenger, ICQ®, MSN® Messenger, Yahoo!® Messenger and IRC through a single interface by enabling simultaneous connections to existing instant messaging networks via a direct connection to whatever servers actually power the messaging network. Trillian, however, cannot share mast types of corporate or personal data as it is limited to Instant Messaging.

[0009] There is a need in the art for a system that allows for the aggregation and access of all types of PIM data in a centralized matter notwithstanding network protocols or other proprietary limitations of particular PIM data resources. Through the aggregation of this data in a centralized manner, the PIM data can then be manipulated or utilized by a particular user or shared amongst a family of users in order to allow for more informed personal and professional relationships. Through the aggregation and sharing of PIM data without regard for protocol and/or proprietary limitations, larger communities may be built between individuals and businesses.

SUMMARY OF THE INVENTION

[0010] The present invention provides more productive control over PIM data by aggregating data from multiple sources and enabling the bridging of information communities and organizations.

[0011] The present invention provides for the aggregation of corporate data from enterprise data depositories such as Microsoft® Exchange® and IBM® Lotus® Domino servers and Internet Service Providers (ISPs) such as Yahoo!® and MSN® as well as the data aggregation platform with regard to user permissions and preferred contact methods.

[0012] The present invention provides for the aggregation of presence information from corporate applications such as Lotus® Sametime and Microsoft® IM in addition to ISP communities such as AOL® and Yahoo!®.

[0013] The present invention provides for the aggregation of status information from a mobile device profile.

[0014] The present invention provides for the aggregation of physical location information from an operator network or device via GPS.

[0015] The present invention provides for the aggregation of user contact information via incoming e-mail messages and telephone contacts.

[0016] The present invention provides for the sharing of information with other users through context based recognition whereby third-parties may contact a user via the most appropriate means of communication at any given time as reflected by status information.

[0017] The present invention allows for users to be more productive and to better manage their PIM Data by identifying particular user context and enabling intelligent choices by other parties.

BRIEF DESCRIPTION OF THE DRAWINGS

[0018] FIG. **1** is an illustration of an exemplary communication network architecture comprising a mobile network, a communication management system and a private network.

[0019] FIG. **2** is an illustration of an exemplary dynamic data aggregation and management system comprising an exemplary data aggregation server, an exemplary client device and various sources of Personal Information Management (PIM) data.

[0020] FIG. **3** is an exemplary data aggregation server providing for aggregation and management of PIM data.

[0021] FIG. **4** is an exemplary client device allowing for access to and manipulation of dynamically aggregation personal and professional contact information.

[0022] FIG. **5** is an illustration of exemplary networked relationships amongst a variety of sources of PIM data and a data aggregation server.

[0023] FIGS. **6**A-**6**F are exemplary embodiments of groups lists as enabled by an exemplary groups module on an exemplary data aggregation and management platform.

[0024] FIG. **7**A is an exemplary view of aggregated contact information for a particular contact.

[0025] FIG. **7**B is an exemplary view of various preferences and permissions of the user identified in FIG. **7**A.

DETAILED DESCRIPTION OF AN EXEMPLARY EMBODIMENT

[0026] FIG. **1** illustrates an exemplary communication network architecture **100**. Communication network architecture **100** comprises a mobile network **105**, a communication management system **110** and a private network **115**. Communication management system **110** generally manages communications between the mobile network **105** and the private network **115**.

[0027] A network should be generally understood as a group of associated devices (e.g., computing devices) that are coupled to one another via a communications facility. For example, mobile network **105** is illustrative of an exemplary group of mobile computing devices such as mobile phones, smart phones, PDAs, tablet PCs and WI-FI equipped laptops. Private network **115** is illustrative of an enterprise server and various workstation clients such as that found in any number of corporate entities and businesses. Private network **115** may also be embodied as a single computer (e.g., a home computer) coupled to a series of other computing devices via an Internet connection as provided by an ISP. Mobile network **105**, communication management system **110** and private network **115** may also be reflective of a network in that they relate a variety of computing devices coupled to one another via a variety of communications channels (e.g., mobile telephone base stations, Internet and so forth). In that regard, networks should be interpreted as being inclusive rather than exclusive.

[0028] Private network **115** may be separated from the communication management system **110**, mobile network **105** and any other networks by a firewall **120**. Firewall **120** is traditionally a set of software applications located at a network gateway server (not shown) to protect the resources of the private network **115** (e.g., corporate or private data) from unauthorized users and/or malicious data entities (e.g., viruses and spy-ware) that might exist outside the private network **115**. Firewall **120** may also be a security policy used with the aforementioned software application. Firewall **120**, in the case of a personal computer (PC), may be software directly implemented on the PC.

[0029] The mobile network **105** comprises a variety of mobile devices mat may communicate over the internet through, for example, a wireless or landline mobile network. A variety of mobile networks and communications channels for enabling Internet access are well known in the art.

[0030] Private network **115** may be any enterprise network, individual user network, or local computer system that maintains data for one or more users. In an exemplary embodiment, the private network **115** may comprise an enterprise server **125** configured to be accessed by multiple PCs **130**. In one example, the enterprise server **125** may be a Microsoft® Exchange® server and the PCs **130** may access data such as electronic mail (e-mail) on the enterprise server **125** through a client software application (not shown) such as Microsoft® Outlook®. The enterprise server **125** can store e-mail mailboxes, contact lists, calendars, tasks, notes, or any other type of local data or electronic documents (e.g., word processing documents, PowerPoint® presentations, Excel spreadsheets). PCs **130** are coupled to the enterprise server **125** over a Local Area Network (LAN) **135**, which is coupled to a Wide Area Network (WAN) **140** such as the Internet.

[0031] In some embodiments, PCs **130** may operate independently of enterprise server **125** (e.g., a home personal computer or a business enterprise without an enterprise server **125**). PC **130** may comprise or be coupled to memory (not shown) to store e-mail mailboxes, contact lists, calendars, tasks, notes, or any other type of local data or electronic document that might otherwise be stored on enterprise server **125**. In these embodiments, a personal client application (not shown) may also provide for communication with a management server **145** or a Personal Client Server (PCS) (not shown) coupled to the management server **145**. This latter configuration would be functionally similar to an enterprise client (not shown) at the enterprise server **125** configured to allow communication with the management server **145**. The particularities of a given communications architecture implementation are left to the requirements of a user, their particular network and available communications hardware and software. In that regard, the present disclosure's reference to a PCS should not be interpreted as an operational necessity but an alternative embodiment of the present invention.

[0032] Communication management system **110** comprises at least one management server **145** configured to manage transactions between mobile devices in the mobile network **105** and the private network **115**. A user database **150**, which may be coupled to or directly integrated with management server **145**, comprises configuration information for different users. For example, the user database **150** may comprise login data for users in the private network **115** and/or mobile network **105**.

[0033] Communication management system **110** may further comprise one or more Smart Device Servers (SDS) (not shown) and/or one or more of the aforementioned PCS (not shown) in addition to any other specially configured equipment that might be necessary to enable communications between the mobile network **105** and private network **115** in addition to communications with the communication management system **110**. Optional SDS (not shown), for example, manages communications with particular smart mobile devices **190** (e.g., smart phones like the Treo 600) whereas an optional PCS (not shown) may manage communications with personal clients (not shown) that may reside on PC **130**.

[0034] Mobile devices in the mobile network **105** may comprise cellular phones **170** comprising Wireless Application Protocol (WAP) interfaces configured to communicate with management server **145** through a WAP gateway. Other mobile devices may include tablet PCs, PDAs and Internet kiosks **180** or any smart mobile device **190** operating as a communication start/end-point.

[0035] Communication channels **160** are any communication pathways that allow the aforementioned mobile devices to communicate between the mobile network **105** with the Internet and/or any other communications network. For

example, communications channel **160** may be a land line, cellular channels, 802.11 wireless channels, or satellite channels.

[0036] In an independent PC configuration, the personal client application (not shown) installed on the PC **130** establishes a data connection between the PC **130** and management server **145** over the appropriate networks (e.g., LAN **135** and WAN **140**) as well as any necessary intermediate hardware or software applications that might further be necessary such as an optional PCS (not shown). The data connection between the PC **130** and management server **145**, in one embodiment, is initiated by the personal client as an outbound connection, which is then authenticated by the management server **145**. For example, the personal client on PC **130** may present authentication information to the management server **145**, which the management server **145** may attempt to reconcile with information in the user database **150**. A similar connection process occurs in the context of an enterprise server **125** with an enterprise client and a related data connection.

[0037] If the management server **145** authenticates the personal client or enterprise client, the data connection is established through firewall **120** (if applicable) to establish access with the communication management system **110**, which is outside the private network **115**. Management server **145**, after having established the data connection, may provide connection sharing information or other communication configuration parameters as might be related to an associated mobile device in the mobile network **105**.

[0038] Management server **145** and the related client at the enterprise server **125** or PC **130** may then enter a quiescent mode until a transaction (e.g., the arrival of data at the server **125** or PC **130**) that requires the transfer of data between the private network **115** and mobile network **105** (e.g., pushing of e-mail). In some embodiments, if the data connection is inadvertently terminated, the client at the enterprise server **125** or PC **130** will automatically reestablish a data connection with the management server **145**.

[0039] The data connection may be maintained even when there is no exchange of data between the management server **145** and mobile network **105** and an associated mobile device. In one embodiment, the data connection is a Transmission Control Protocol/Internet Protocol (TCP/IP) connection although any connection protocol may be used that provides connectivity between the private network **115** and communication management system **110**. Alternative embodiments may utilize a proxy server and/or a Secure Socket Layer (SSL) for the purposes of maintaining the security of information transmitted between the private network **115** and communication management system **110**.

[0040] After establishing the data connection, a mobile data connection may be established between the mobile device in the mobile network **105** and the management server **145**. The mobile data connection may, in some embodiments, be established prior to and/or maintained notwithstanding the presence of a data connection between the private network **115** and communication management system **110**. For example, a mobile device in mobile network **105** may seek to establish and maintain a connection as soon as a communication channel **160** is available that facilitates establishing that connection. The mobile data connection may further be subject to polling (e.g., accessing the communication management system **110** on a regularly scheduled basis); manual synchronization and/or the generation of or request for data at the mobile device.

[0041] The mobile connection, in some embodiments, may also be initiated by the communication management system as a result of the arrival of data at the enterprise server **125** or PC **130** that needs to be delivered to the mobile device **170** via the communication management system **110** and appropriate communication channel **160** (e.g., arrival of e-mail to be pushed to the mobile device).

[0042] After the mobile connection is established, the mobile device **170** may access e-mail and other PIM data at the enterprise server **125** or PC **130** via an enterprise client or personal client, respectively. In some embodiments, the use of an optional SDS (not shown) to establish connectivity between the communication management system **110** and a smart device **190** may be required as may an optional PCS (not shown) for establishing connectivity between communication management system **110** and PC **130**.

[0043] Mobile device connection, as noted, may be initiated by a mobile device in the mobile network **105**. For example, a mobile user's username and password for accessing the communication management system **110** may be established in user database **150** when the user enrolls with the communication management system **110**. The user would subsequently be required to provide this information when their mobile device attempts to automatically or manually accesses the communication management system **110**. A username/password combination is not necessarily required to access the management system **110** as other security credentials may be utilized to establish access.

[0044] For example, an authentication token may be established on the mobile device following the device's providing of the proper security credentials (e.g., a user name and password). That authentication token may be recognized by the communication management system **110** with regard to establishing future access so that the re-entry of a username and password is not required for subsequent access. The authentication token may be permanent or set to expire after a certain period of time or a certain number of uses. Certificate mapping (using SSL certificates), Host-IP access control (white-listing and black-listing certain IP addresses or networks) and device location may also be used to establish access to the communication management system **110**. In the latter example, the position of a device may be established by access to a particular base station (in the case of a cellular device) or a GPS-transceiver may identify the position of the device. If the device is out of a specified region, the communication management system **110** may deny access (e.g., a user designates denial of access if their mobile device is taken overseas or out of state as that location suggests it has been stolen).

[0045] Security credentials may also be provided through a combination of various mobile identifiers, for example, Mobile Identification Numbers (MIN), International Mobile Subscriber Identity (IMSI) and Electronic Serial Number (ESN). Additional layers of security may be provided through the use of a secure hash algorithm or a Virtual Private Network (VPN). Notwithstanding the particular access methodology, the credentials are ultimately verified by the management server **145** or some related software/hardware (e.g., optional SDS (not shown)) and possibly with further regard to user information stored in the user database **150**.

[0046] Similar authentication methodologies may be utilized for establishing a data connection between the communication management system **110** and a computing device in the private network **115**.

[0047] Once connectivity is established by the mobile device, the user may access e-mail, files or Personal Information Management (PIM) data residing at the enterprise server **125**, PC **130** or communication management system **110** at the management server **145**.

[0048] Management server **145** may be configured to reformat and render local data from the private network **115** according to the particularities of the user's mobile device in addition to functioning as a routing engine for data transactions between the mobile devices of the mobile network **105** and the private network **115**.

[0049] FIG. **2** is an illustration of a data aggregation and management system **200** comprising an exemplary dynamic data aggregation server **210**, an exemplary client device **220** and various sources of PIM data including an enterprise server **230** and a PC **240**. Various intermediate operations and services **250** are also shown. The intermediate operations and services **250** may be directly integrated as a part of data aggregation server **210**, may stand alone as a third-party service accessible by data aggregation server **210** and/or device **220** or be remotely coupled to the data aggregation server **210** (e.g., physically separate from the physical architecture of the data aggregation server **210**); for example, a switch or customer service center.

[0050] PC **240** may be a desktop PC coupled to the data aggregations server **210** by way of client connection software like SEVEN Personal Edition available from SEVEN Networks, Inc. of Redwood City, Calif. This client connection software may provide a secure link to data stored at the PC **240** such as e-mail, personal contacts and documents via and other PIM data. A client device **220** such as a smart phone or other mobile device may access this data via the data aggregation server **210** and/or a communications management system like that described in FIG. **1** and any variety of communication networks (e.g., wireless). PC **240** and its client connection software may be configured with certain features such as end-to-end encryption to ensure secure transmission of personal data or notification functionalities to inform a user that new content (e.g., e-mail) has arrived at the PC **240** and should be forwarded to client device **220** via, for example, a push operation through the data aggregation server **210** and/or a communications management system.

[0051] Enterprise server **230** may be a corporate enterprise server configured to manage e-mail, data and various applications. Enterprise server **230** (and PC **240**) may utilize a firewall (not shown) like that described in FIG. **1**. Although a firewall is described, a firewall is not necessary for the operation and interaction of the enterprise server **230** (or PC **240**) with data aggregation server **210** and/or client device **220**.

[0052] Enterprise server **230** is coupled to the data aggregation platform **210** via appropriate client server software, which, like the client software of PC **240**, intermediately couples the enterprise server **230** to client device **220** via a data connection to the data aggregation server **210** and/or a communications management system like that described in FIG. **1**. An example of such software is SEVEN Server Edition available from SEVEN Networks, Inc. of Redwood City, Calif. Additional software installed at the enterprise server **230** may provide various users (e.g., clients or workstations) the ability to interact with the enterprise server **230** and have access to application data (e.g., email).

[0053] Data aggregation server **210** comprises the various modules necessary to aggregate and management certain PIM data. Data aggregation server **210** may be directly integrated with the management server (**145**) of FIG. **1** or otherwise coupled to the communication management system (**110**) described in FIG. **1**.

[0054] Data aggregation server **210** is optionally coupled to the enterprise server **230** and/or PC **240** via network **260**. Network **260** further enables communications access to additional sources of PIM data like those described in FIG. **5** below. Access to an enterprise server **230** or PC **240** by the data aggregation server **210** is not required for the operation of the data aggregation server **210**. The data aggregation server **210** may operate independently of an enterprise server **230** and PC **240** so long as certain information required by the data aggregation server **210** and an associated client device **220** is otherwise available (e.g., PIM data such as calendar and/or contact data). Coupling the data aggregation server **210** to PC **240** and/or enterprise server **230** merely provides additional or enhanced functionality that might otherwise be unavailable absent such a coupling.

[0055] Similarly, the e-mail redirection and data access functionality offered by connection software at PC **240** and enterprise server **230** may also operate independent of the data aggregation server **210**. In an embodiment of the present invention, data aggregation server **210** and PC **240** and/or enterprise server **230** may operate in parallel without ever being 'aware' of the operation of the other. Another embodiment of the present invention, however, may integrate certain features of data aggregation server **210** with enterprise server **230** and/or PC **240** to provide for the aforementioned enhanced functionality.

[0056] In an embodiment of the present invention, data aggregation server **210** may be operating on and/or integrated into with a service provider network (e.g., Cingular Wireless for wireless networking or AT&T Inc. for telecommunications such as digital subscriber lines (DSL)) as is further described in FIG. **5**. Through integration or operational contact with a service provider's network, instant access to a community of millions of subscribers (i.e., the service provider's customers) is provided. This integration may also allow for access to additional features such as news, media content, maps and directions as well as e-mail, Short Messaging Service (SMS) and any other value-added features as made available by the service provider. The service provider's network and the data aggregation server **210** may operate independently of or in conjunction with enterprise server architecture **230** and/or PC **240**.

[0057] As noted above, the data aggregation server **210** may also be integrated with the communication management system (**110**) and/or management server (**145**) of FIG. **1**. In that regard, data aggregation server **210** may be a part of the management server (**145**), which may be an operational part of the communications management system (**110**) of FIG. **1**, That communication management system (**110**) may be a part of the aforementioned service provider network and is further described in FIG. **5**.

[0058] Data aggregation server **210** may comprise various access controls, gateways and operational modules, which are described in detail in FIG. **3**.

[0059] Intermediate operations and services **250** may comprise any variety of operations and services deemed necessary and/or desirable by a service provider. In FIG. **2**, an SMS Gateway **270**, IP/SIP Gateway **280** and Billing and Transaction Service **290** are illustrated. The inclusion of these par-

ticular operations and services is not to suggest their presence is a prerequisite for practice of the presently clamed invention.

[0060] SMS Gateway **270** may comprise a software and/or hardware utility enabling users to send and receive SMS messages on a GSM or PCS digital cellular network. SMS Gateway **270** may support a number of IP interfaces such as POP3 and SMTP for integration with an e-mail environment as well as HTTP/XML interfaces and SNMP traps for notification of events. SMS Gateway **270** may further support local programming interfaces such as Object Linking and Embedding (OLE), Dynamic Data Exchange (DDE) and Command Line Interface (CLI), SMS gateway **270** may be further coupled to an SMSC (not shown). A Push Gateway may be functionally integrated with SMS Gateway **270** and may further operate proxy applications such as a WAP Gateway for the translation of WAP requests into HTTP requests.

[0061] An IP/SIP Gateway **280** may operate in conjunction with an SIP Stack located in client device **220** to integrate the PSTN, which uses the Signaling System 7 protocol to offload PSTN data onto a wireless or broadband network.

[0062] Billing and transaction service **290** may be configured and/or utilized for calculating the minutes a user is on a network and/or the amount of bandwidth the user has consumed and how this usage pertains to a service plan and/or billing cycle. Other features that may be utilized by the user of client device **220** and subject to a service fee may be calculated by billing and transaction service **290** such as SMS, roaming and 411.

[0063] Client device **220**, in an embodiment of the present invention, is a mobile device such as a cellular telephone configured to allow access to the data aggregation server **210** as well as data in enterprise server **230** and/or PC **240**. Client device **220** may operate through intermediate operations and services **250** in order to access the data management server **210**. Client device **220** may comprise various authentication controls and operational modules that interact with certain modules in the data aggregation server **210**, the intermediate operations and service **250** as well as an enterprise server **230** and/or PC **240**.

[0064] FIG. **3** is an exemplary data aggregation server **300** providing for the aggregations and management PIM data such as personal and professional contact and calendar information.

[0065] A module, as referenced in the present invention, is a collection of routines that perform various system-level functions and may be dynamically loaded and unloaded by hardware and device drivers as required. The modular software components described herein may also be incorporated as part of a larger software platform or integrated as part of an application specific component.

[0066] The modules of the present invention, in one embodiment actively seek out data. That is, the modules recognize the existence of certain data connections to PIM data and other informational stores at mobile devices, desktop PCs, enterprise servers and any computing device coupled to the data aggregation server **300**. Client software may be utilized at these different data stores to enable the access to information and to provide for certain authorization/access exchanges as are discussed in, for example, the context of access module **310**. The data aggregation server **300**, via the appropriate module (e.g., presence module **320**) and/or modules (e.g., presence module **320** in conjunction with access module **310**) will attempt to contact a client or some other indicia (e.g., an IP address) reflecting the existence of PIM or other informational data and try to acquire the same.

[0067] In another embodiment of the present invention, the data aggregation server **300** (via its various modules) may actually attempt to establish a data connection when a connection is not in existence. For example, if an enterprise server closes a TCP/IP connection to preserve bandwidth, the data aggregation server **300** may attempt to (re)establish that data connection in order to acquire certain PIM or other informational data.

[0068] In yet another embodiment of the present invention, the aforementioned clients or other software associated with the data management server **300** may attempt to push PIM and other informational data directly to the data aggregation server **300**. For example, a desktop PC may be configured with client software allowing for interaction with the data aggregation server **300**. The desktop PC client may recognize the existence of certain PIM or other informational data such as calendar and contact information. In an embodiment of the present invention, that client may push the PIM and other informational data to the server.

[0069] Limitations may be imposed on the clients with regard to what information may and may not be pushed. For example, certain information may be designated of low importance/privacy and freely pushed to the data aggregation server **300**. Other information may be designed of medium importance and require, for example, the authorization of a user before that information is pushed to the data aggregation server **300**. Still further information may be designated high priority/importance and never be pushed to the data aggregation server **300** due to privacy concerns. Similar limitations may be imposed in a pull scenario wherein the various modules of the data aggregation server **300** seek out that information and pull the information from an associated information source such as a desktop PC.

[0070] In another embodiment of the present invention, a client operating at, for example, a desktop PC may push certain information to a mobile device. That mobile device may then push the same information to the data aggregation server **300**. Similarly, that information may be pulled from the mobile device after having been pushed from the desktop PC.

[0071] The present invention does not intend to limit the means by which information is acquired (e.g., push or pull), the existence or non-existence of intermediaries (e.g., data pushed from a desktop PC to a mobile device to a data aggregation server **300**) or any security policy that may or may not be in place with regard to the aggregation of PIM and other informational data. A single data aggregation server **300** may further utilize various data acquisition methods for different types of data. For example, the data aggregation server **300** may actively seek to acquire location information via a location module **330** but may accept the pushing of data as it pertains to calendar and/or contacts data.

[0072] The modules of the present invention, in addition to aggregating information, may also manage the data. That is, the modules may analyze certain data in order to generate further data as is discussed in the context of a location module **330** and presence module **320**, below. The various modules of the present invention may further execute certain calls and commands as they pertain to storage and retrieval of aggregated data, which may be stored locally (e.g., at the data aggregation server **300**), in a storage area network (SAN), at a remote location or in any other medium or apparatus suitable for storage of data and accessing the same. Management

(e.g., storage) of data may also be executed by other modules of the data aggregation server **300** that are not otherwise shown.

[0073] Aggregated data may be further stored at a client device **220** whereby the data aggregation server **300** pushes relevant data (e.g., data pertaining to PIM data of the user) to the client device **220** upon availability of the relevant data or, alternatively, relevant data is acquired and pulled upon request of the user for particular data or updated data. In some instances, the data aggregation server **300** will maintain local storage of certain portions of data in order to allow certain modules to analyze certain data in order to generate further data.

[0074] Storage of the aggregated data may be subject to various security protocols that may be set by the origin of the data (e.g., a user may designate their PIM data to expire so many hours after acquisition or the data may be prohibited from storage on any device or a particular device for more than a particular period of time). Alternatively, an administrator of a particular network or a particular communications architecture (e.g., an enterprise server or a larger communications network) may implement various security limitations. Limitations and/or requirements of the storage of data may be subject to any variety of privacy, security and/or performance reasons.

[0075] By further example, in the case of contact information (e.g., names and addresses), the data aggregation server **300** may pull contact information from an Internet portal such as Yahoo!®, from a Microsoft®Exchange® Server and/or from an address book in a mobile device (e.g., client device **220**). Alternatively, the client device **220**, in conjunction with data aggregation server **300**, may synchronize the aforementioned data sources. In this example, the data aggregation server **300** may only retain certain information (e.g., metadata) as that information passes through the server **300** and as that information pertains to identifying and developing potential links between various users of the data aggregation server **300**.

[0076] In the case of calendar data, for example, that data may be pulled from various data sources (as described above) or may merely be synchronized (as also described above). The calendar data may be immediately pushed from one point (e.g. a desktop) to another (e.g., authorized users) wherein the data aggregation server **300** only retains information pertaining to open-meeting times for the purpose of scheduling or it may store nothing at all.

[0077] In the case of content such as pictures, blogs, photographs as may be acquired from Internet portals or websites on the World Wide Web, that content may be immediately pushed to authorized and/or requesting users as the size of the content would likely degrade performance of the data aggregation server **300**.

[0078] Access module **310** comprises or is otherwise coupled to the software, routines, hardware and/or driver devices necessary to control who and what has access to the data aggregation server **300** and the PIM data and other information aggregated and managed by the data aggregation server **300**. Access module **310** may be configured to grant or deny access based on, for example, who is making the access request (e.g., a particular user), where the request is coming from (e.g., location as may be determined by a base station or GPS), when the request is occurring (e.g., time of day), what is making the request (e.g., a mobile device) and how the connection is being made (e.g., SSL).

[0079] Access module **310** may utilize a user name/password combination to authenticate a user requesting access. A list of users and/or groups with access to the data aggregation server **300** may be created and stored in an LDAP database controlled by LDAP module **370**. This database of groups and users may be installed locally or a reside at a remote machine, a storage area network or any other device/medium at any location so long as it is suited for the maintenance and access of user access data.

[0080] Access module **310** may further utilize SSL authentication whereby a user's identity if confirmed by a security certificate. If the certificate is from a trusted authority, then the certificate is mapped to a user's entry in a certificate mapping file. If the certificate maps correctly, access is granted subject to specific rules set for that particular user (e.g., access control lists and access control entries). If the certificate is not from a trusted authority or fails to map properly, authentication fails and access is denied.

[0081] Access module **310** may utilize other access control methodologies such as Host-IP access control wherein access is limited or denied to specific clients as specified by hostnames or IP addresses of allowed or blacklisted clients. Wildcard patterns may be used to control access as it pertains to, for example, entire networks.

[0082] Access module **310** may further interoperate with presence module **320**, location module **330**, calendar module **340**, groups module **350** and/or contacts module **360** to allow for acquisition of PIM data and other information from multiple sources including desktop PCs, Internet Service Providers, web portals and work directories as is illustrated in FIG. **5** below.

[0083] Presence module **320** comprises or is otherwise coupled to the software, routines, hardware and/or driver devices necessary to identify the availability of various subscribers or users of the data aggregation server **300**. That is, presence module **320** helps identify who is presently available and through which particular contact methodology they may be contacted.

[0084] For example, through application awareness (e.g., a calendar or calendar module **340**), presence module **320** may determine that a user is presently in a meeting and therefore unavailable (i.e., not present). Alternatively, presence module **320** may, as a result of a manual setting by a user communicatively coupled to the data aggregation server **300** (e.g., a data connection from a desktop PC), determine that a user is available only through a particular contact methodology and display that information as is appropriate (e.g., available—present—via phone and e-mail).

[0085] A second user connected to the data aggregation server **300** via, for example, a mobile device may—as a result of information aggregated and made available by presence module **340**—ascertain the present unavailability of a first user in their office (i.e., their presence PIM reflects they are out of the office) and, instead, contact that user on their cellular phone where their presence is currently and affirmatively identified.

[0086] Various types of presence may be reflected by the presence module **320**. Instant messaging, e-mail, home phone, office phone, cellular phone, SMS, pager and any other form of communication device capable of reflecting availability or unavailability are within the scope of the type of presence information aggregated and managed by presence module **320**.

[0087] Location module **330** comprises or is otherwise coupled to the software, routines, hardware and/or driver devices necessary to identify the physical location of a subscriber or user of the data aggregation server **300**. Location module **330** may be utilized in the context of a GPS-enabled mobile device although such functionality is not necessary for the practice of the present invention.

[0088] For example, location module **330** may determine that a particular user is presently working at their computer in their office as a result of querying information managed by the presence module **320**. Through other modules or applications (e.g., an address book), location module **330** may determine that the user's work address is located at 901 Marshall Street, Redwood City, Calif. In this way, the location module **330** may make intelligent determinations of data even though certain information may not be directly provided to or aggregated by the module. In this way, information can also be generated or aggregated without the requirement of the aforementioned GPS functionality.

[0089] Location module **330**, through integration with a third-party system or built-in features presenter coupled to the data aggregation platform **300**, may also aggregate information to be utilized in the context of location information. For example, the location module **330** may aggregate the necessary data to provide text or visual directions to a particular user as it relates to aggregated location information.

[0090] Location module **330** may be further configured to make direct queries of users as to their location or to analyze information as provided by cellular base stations as to general locations of users.

[0091] Calendar module **360** comprises or is otherwise coupled to the software, routines, hardware and/or driver devices necessary to aggregate calendar and scheduling information of subscribers or users of the data aggregation server **300** and any metadata that may be associated with the same.

[0092] Calendar module **340** may seek to aggregate calendar information from a variety of sources of a particular user, for example a mobile device or handheld calendar and a calendar integrated with a desktop PC or enterprise server. The aggregation of calendar data by the calendar module **340** may aid in providing on-the-go synchronization of calendar information. As calendar information constantly changes and provides the greatest possibility for conflict (i.e., two disparate events at two different data stores for the same time period), an embodiment of the present invention continually aggregated calendar information for 'as soon as possible' availability and/or manipulation via calendar module **340**.

[0093] The aggregation of calendar data may be provided as part of a specific request to view that information. For example, a user may seek to access calendar information at a desktop PC via their mobile device. That calendar information may be aggregated by the calendar module **340** in addition to being conveyed to the client via a pull operation to the data aggregation server **300** and a subsequent push to the mobile device client. In another embodiment, the calendar information may be pulled from the desktop PC or enterprise server all the way to the mobile device client with a copy of the calendar data being cached by the calendar module **340** as it passes through the data aggregation server **300**, which may be integrated a communication management system like that described in FIG. **1**.

[0094] Similarly, calendar data generated at a mobile device may be aggregated by the calendar module **340** via a pull command at the data aggregation server **300** or via a similar command issued by a desktop PC. Calendar data may also be pushed directly to the calendar module **340** as a result of certain behavior at the mobile client (e.g., the entry of new calendar information followed by a synchronization operation) or part of a regularly scheduled push aggregation operation to the data aggregation server **300**. In this way, changes in calendar data that truly occur 'on the go' may be aggregated for subsequent synchronization and/or distribution as is appropriate.

[0095] Calendar module **340** may further interoperate with presence module **320** to help provide indicia of presence. For example, a presence indicator may normally be manually set by a user (e.g., 'I am Available' or 'I am Not Available'). In the event that a user fails to provide such a manual setting and the user is unavailable, the user's presence setting may be misleading thereby resulting in other users attempting to contact the user but to no avail thereby defeating one of the purposes of a presence indicator. When the calendar module **340** operates in conjunction with the presence module **320**, certain calendar information as aggregated by the calendar module **340** may aid in generating a more accurate indicator of presence as provided by presence module **320**. For example, the occurrence of a meeting in a calendar would indicate that a user is unavailable. The presence module **320** may then adjust in light of this aggregated calendar data and make an appropriate reflection of the same. When the meeting ends, presence indicators may be readjusted as is appropriate.

[0096] Like all of the PIM data aggregated by the present invention, certain information may be allocated a different degree of privacy or importance. For example, different meetings may be of different importance—that is, the meeting may be of critical importance (e.g., a major merger or acquisition) or of lesser importance (e.g., a company presentation on the new credit union membership). Based on metadata embedded in the calendar data (e.g., 'must attend' or 'important'), additional data is acquired by the calendar module **340**, which may then be shared through data distribution or utilized by other modules of the present invention.

[0097] Metadata embedded in the calendar data and recognized by the calendar module **340** may also be utilized to reflect additional information not necessarily expressly provided by that calendar data (e.g., in a subject description). For example, calendar module **340**, through data aggregation, may determine that while a meeting does not begin until 2:00 PM, because of a 'travel required' metadata indicator, any sharing of this calendar information would reflect that an attempt to schedule a meeting with that user during their 'travel time' would be ill advised despite the fact that the calendar might otherwise reflect availability. In some embodiments, metadata reflecting the need to travel and information relating to the address of the meeting (as expressly provided by the calendar entry or as may be obtained through other applications or aggregated information), may allow for the utilization of mapping technologies to provide a more accurate indicator of the exact travel time required and, as a result, more accurate information to be distributed by the data aggregation server **300**.

[0098] Numerous metadata indicators may be available to be embedded in calendar data and acquired by the data aggregation server **300** via the calendar module **340**, for example: none, important, business, personal, vacation, must attend, travel required, needs preparation, birthday, anniversary, phone call, free, tentative, busy, out of office. Additionally, in

an embodiment, a user may be able to generate their own personalized metadata and provide associate rules with regard to the same.

[0099] The calendar module **340** of the present invention, in an embodiment, may aggregate information from both personal and professional calendars. The calendar module **340** of the present invention may further aggregate information pertaining to the availability of conference rooms or conferencing equipment. The calendar module **340** may manage aggregated calendar data and take info account time zone differences in calendar data as may later be distributed to users of the data aggregation server **300**. For example, the calendar module **340** may make determinations that 1:00 PM calendar information for a user in California translates into different information when accessed by a user in the United Kingdom. Calendar module **360** may further interoperate with the presence module **320** to make determinations of locations and automatically make the appropriate time zone calculations and/or adjustments when aggregating and/or distributing information.

[0100] Groups module **350** comprises or is otherwise coupled to the software, routines, hardware and/or driver devices necessary to form groupings of different users or subscribers of the data aggregation server **300**. Groups information acquired and generated by the groups module **350** may be explicit like a ListServ; for example, add user A to group X. Groups may also be implicit and generated as the result of intelligent determinations made by the groups module **350**.

[0101] For example, the groups module **350** may determine that users A, E and G are all employed by Big Co. and wall create (if the group does not already exist) and/or add users A, E and G to the Big Co. group list. The groups module **350** may further determine that users B, C and D are all graduates of State University and create and/or add them to the State University group list. The groups module **350** may further determine that users F, H and I are all members of Professional Organization and create and/or add them to the Professional Organizations list. Furthermore, the groups module **350** may determine that users J, K and L are all Family Members and add them to the Family Members list.

[0102] Users may be members of more than one group as generated by the groups module **350**. For example, user J could be could be a Family Member and also an alumnus of State University thereby warranting their presence of both the Family Members and State University List. Users may be members of only one group. Users may not belong to any group.

[0103] Groups may be identified and/or generated as a result of acquiring data from various sources. For example, a Global Address List (GAL) may represent a comprehensive list of e-mail addresses, fax and telephone numbers, and mail stops for the employees and contractors for a particular company. In addition to being a raw source of contact data, the GAL could in and of itself be the basis for generation of a group (e.g., Company Group List).

[0104] Contact data aggregated by a contacts module **360** may be categorized and grouped by the groups module **350**, may be manually entered (e.g., input by a user) or obtained through a synchronization operation. In any of these instances, the groups module **350** is configured to aggregate the new information and group it properly.

[0105] As noted, contact data as aggregated by the contacts module **360** may be implemented by the groups module **350**. For example, if the groups module **350** determines that it has incomplete data for a member of a group or a contract entry in general, the groups module **350** may actively seek that member/user's absent information through, for example, accessing a GAL or even an LDAP database comprising user information or another operation in conjunction with the contacts module **360**.

[0106] Contacts module **360** comprises or is otherwise coupled to the software, routines, hardware and/or driver devices necessary to aggregate contact information from different sources of contact data. While the most common sources of contact PIM data are address books or contacts lists, the contacts module **360** may aggregate data through intelligent operations wherein elements of contact information are identified and more complete information is aggregated for the purpose of generating a more accurate and complete contact profile.

[0107] For example, the contacts module **360** may determine that User A contacted the present subscriber via a telephone call but the name and e-mail address of User A is not available—only their phone number. The contacts module **360** would then seek that absent information from various sources such as local directories, username/password stores, the Internet, contact lists of other users, corporate personnel directories or any other sources of information that might link the phone number to more identifying information for use in a contacts profile. Similar queries could be made based on received and sent e-mails or any other indicia of contact or interaction by the user (e.g., SMS and instant message).

[0108] The contacts module **360** may further query other information networks and/or data aggregation platforms (e.g., a platform embedded in the network of a separate service provider but with whom the present service provider has an informational sharing agreement) to determine the identity of User A. The contacts module **360** could also directly query the user for the missing information through, for example, an SMS message requesting the information be entered at the mobile device or a desktop PC.

[0109] Contact information may also be acquired from various other applications. For example, and as noted above, the receipt of an otherwise unknown phone number can begin the acquisition of contact information such as name, physical address and other identifying contact information (e.g., company, title, etc.). Information may also be obtained from e-mail headers whereby a domain name (e.g., @company.com) may be traced to a particular company or from the body of an e-mail through an e-mail signature or footer. Similarly, instant messages—as a form of contact—may be utilized to generate a profile or parts thereof. Outgoing phone calls, e-mails and SMS messages can be used in a similar fashion.

[0110] Calendar data may also be used to acquire contact information as it pertains to, for example, a corporate/work address (e.g., 10AM meeting at SEVEN Networks, Inc. at 901 Marshall Street, Redwood City, Calif. 94063) of a particular person. Based on that calendar data, the contacts module **360** may determine that the 10AM with Person X was at Person X's place of employment: SEVEN Networks, Inc. and generate appropriate contact information and profile data concerning employer and business address. In this way, the employment and address information of Person X can be populated without an express input of that information into a particular user/contact profile having ever been made. Similarly, anniversaries, birthdays and other repeating and/or important dates can be associated with particular contacts.

[0111] Contact information—and another PIM data for that matter—may be obtained from other profiles of users of the data aggregation server **300** subject to privacy and security profiles. For example. User A may have a complete profile indicating name, phone number, address, employment and e-mail information. User B's profile may only designate employment information, specifically, the name of their employer. The contacts module **360** of the data aggregation server **300** may, by matching the employment information of Users A and B, populate other fields in User B's profile. For example, User B's profile with regard to a general phone and fax number as well as corporate address can be populated as User B works for the same company as User A, that same information being fully present in the contact information/data profile for User A.

[0112] It is envisioned that in some embodiments of the present invention, various Internet spiders or web scraping technologies may be utilized by the contacts module **360** to further acquire presently unavailable information. In such an embodiment, a web scraping module (not shown) could further identify a particular contact/user profile and search various websites for information and news pertaining to that person. If it is determined, during spidering, that this particular person has changed jobs, been promoted or been subject to some other event of news-worthy importance, the contacts module **360** may update certain contacts information/profile data.

[0113] LDAP module **370** is a TCP/IP software protocol enabling users to locate organizations, individuals and other resources in an open or proprietary network (e.g., look-up queries). LDAP module **370** makes it possible for almost any application running on virtually any platform to obtain directory information, service data and public keys. LDAP module **370** may be based on the X.500 open standard whereby applications need not worry about the type or location of servers hosting the queried directories. LDAP module **370** may further identify user privileges on a network.

[0114] Voice gateway **380** terminates PSTN traffic from callers. Voice gateway **380** may comprise an automated speech recognition engine (not shown) to perform speech recognition; a dual tone multi-frequency (DTMF) module (not shown) for recognition of key tones; and audio playback and record components (not shown). Voice gateway **380** may further comprise a Voice Extensible Markup Language (VXML) interpreter (sometimes referred to as a voice interpreter) (not shown) for interpreting VXML markup, playing synthesized speech and/or listening for user responses in the instance of automated speech recognition.

[0115] Other modules may be introduced to the data aggregation server **300** so long as they do not interfere with the aggregation and management of PIM data from various sources such as an enterprise server or PC or those other sources as exemplified in FIG. **5** below.

[0116] FIG. **4** is an exemplary client device **400** (**170**) allowing for interaction with and manipulation of dynamically aggregated personal and professional contact information. Device **400** may be any variety of portable devices such as a SmartPhone, PDA, mobile device, tablet PC and so forth. Device **400** comprises various modules (e.g., synchronization module **405**, logic module **410**, etc.).

[0117] The present device **400** is exemplary; additional or differing embodiments of the present invention may lack certain modules (e.g., location module **445**) and/or may comprise additional modules such as an enhanced user interface framework.

[0118] Synchronization module **405** comprises or is otherwise coupled to the software, routines, hardware and/or driver devices necessary for updating or backing up data on one device with a second device. The most common instance of synchronization occurs between a mobile device (e.g., a PDA or a SmartPhone) and a desktop computer running a desktop connector or coupled to a server hosting synchronization software.

[0119] While synchronization may be the result of a physical coupling of the mobile device to the desktop computer (e.g., through a desktop cradle and cable), the pervasiveness of wireless technology (e.g., CDMA2000, 1xRTT, FOMA, GSM/GPRS, UMTS, i-Mode, MOPERA, EDGE, WCDMA, Bluetooth and Wi-Fi) and related devices as well as improvements in encryption technology (e.g., AES 128-, 192- and 256-bit keys) now allow for synchronization to occur wirelessly while a user of the mobile device is away from their office. Physical presence of the synchronizing device with the synchronized device is no longer required.

[0120] Various improvements in 'push' and 'pull' technology further allow for more than mere 'backing up' of data through a synchronization operation but also to receive and retrieve data in real-time. For example, the aforementioned SEVEN Server Edition software is a server-based, behind-the-firewall mobile service that provides end-users with real-time access to corporate and personal data such as Microsoft Exchange, Lotus Domino, IMAP4 and POP3 email; calendar; corporate directories; personal contacts; and documents.

[0121] Logic module **410** comprises or is otherwise coupled to the software, routines, hardware and/or driver devices necessary for data manipulation and control functions. In the case of hardware, logic module **410** is comprised of circuits that perform an operation. In the case of software, logic module **410** is the sequence of instructions in a program. Logic module **410** may be comprised of both hardware and software, only software or only hardware. As is known in the art, the hardware of logic module **410** may implement the software of logic module **410**. Certain software in the logic module **410** may be implemented by other modules or hardware components of device **400**.

[0122] Encryption module **415** and decryption module **425** are responsible for the encryption and decryption, respectively, of data exchanged between device **400** and communication management system **110**, which may include data aggregation server **210**. Encryption module **415** and decryption module **425** may, in some embodiments of the present invention, operate in conjunction with other modules such as authentication module **455** to allow for encryption of authentication information related to network and service access. Other embodiments of the present invention may utilize the encryption and decryption modules **415**/**425** for the purposes of exchanging data and information directly between mobile devices, for example, between Bluetooth enabled mobile devices.

[0123] An example of an encryption algorithm that may be utilized by encryption and decryption module **415** and **425**, respectively, is the 128-bit Advanced Encryption Standard (AES), which is based on Federal Information Processing Standard (FIPS) 197. The disclosure of the FIPS 197 is incorporated herein by reference. Another encryption methodology within the scope of the present invention is the Diffie-

Hellman (DH) secret-key negotiation (sometimes referred to as the Diffie-Hellman-Merkle key exchange). The algorithm for DH secret-key negotiation is disclosed in U.S. Pat. No. 4,200,770, the disclosure of which is incorporated herein by reference. DH secret-key negotiation is a cryptographic protocol that allows two parties to agree on a secret key for use over an insecure communications channel; the key can then be used to encrypt subsequent communications using a symmetric key cipher.

[0124] In an embodiment of the present invention, various data types are exchanged between the device **400** and communication management system **110**, which may include dynamically aggregated data such as presence data. Such data, when being transmitted from device **400**, may be encrypted by encryption module **415** using 128-bit AES or DH secret-key negotiation. Similar methodologies and algorithms may be used to decrypt information received by device **400** and decryption module **425**.

[0125] In some embodiments of the present invention, encryption/decryption modules **415/425** may further prevent the storage or write-to-disk (e.g., proxy caching) of transmitted/received data to further improve security whereby no one but authorized users can read or access data.

[0126] Additional embodiments of the prevent invention may provide for the encryption module **415** to obliterate data stored on the device **400** or 'lock-down' the device **400** should a user of device **400** report device **400** stolen or initiate an obliteration or lock-down command from communication system **110**, server **125** or PC **130**.

[0127] Establishing end-to-end encryption may comprise the submission of security credentials upon initial registration of a device **400** with communication management system **110**. These credentials may be used to later authenticate the user and provide access to appropriate data and resources at the communication management system **110**. In an embodiment of the invention, these security credentials are not stored outside of the system **110** architecture, which provides for improved security.

[0128] In one embodiment of the present invention, during the registration process a unique, encrypted authentication token is exchanged between the mobile device **400** and communication system **110** whereby the user of the device **400** will be able to access resources at the communication system **110** without being required to submit credentials upon each subsequent login. Security credentials may be enabled by the user of the device **400** and/or communication system **110** or by an IT administrator who may set various security policies for the device **400**, communication system **110** and related network.

[0129] For example, an administrator may implement a username/password policy whereby users are required to login using a name and password. Administrators may also enable or disable a browser mode wherein users may be able to access data not only through a mobile device **400** but also through a secure Internet web browser utilizing, for example, 128-bit SSL encryption. Certain policies (e.g., user name and password) may also be made time sensitive whereby a login expires every 'X' days. Administrators may also control the obliteration of data in devices **400** in the instance that a device **400** with access to behind-the-firewall data is lost or stolen.

[0130] In an embodiment of the present invention, encrypted data transmitted to and/or received from mobile device **400** may utilize digital signature algorithms such as SHA-1, a secure hash algorithm, as disclosed in FIPS 180-2, the disclosure of which is incorporated herein by reference. The use of a digital signature algorithm provides additional protection against the modification of data as it passes through a network, even though the data is independently encrypted (e.g., using AES).

[0131] In yet another embodiment of the present invention, encrypted data transmitted to and/or received from mobile device **400** may further utilize a multi-channel encryption protocol whereby a single block of data comprises multiple separately encrypted sections, each destined for a different end point. For example, a block of data may comprise a header section, which is accessed for routing purposes and a body section, which comprises several e-mail messages destined for the device **400**. Each section of data may be encrypted with a separate key whereby the routing information may be decrypted without requiring access to the e-mail message data.

[0132] In still another embodiment of the present invention, a Virtual Private Network (VPN) may be utilized adding yet another layer of security on top of a SSL. These various embodiments may be implemented individually, collectively, or in a piece-meal fashion depending upon the particular security concerns of the data accessed and generated by device **400**.

[0133] Application cache **420** comprises or is otherwise coupled to the software, routines, hardware and/or driver devices necessary for storing application data in memory as opposed to constantly looking up, loading, reading and executing the application data from another location. Application cache **420** helps improve the processing speed of device **400**.

[0134] Application cache **420** may be configured so that every time data is instantiated or called, the data is time-stamped. A clean-up process will occasionally remove all instances of data that are beyond a certain age as reflected by the time-stamp. By time-stamping and removing stale data, there is increased certainty that the cache **420** and the data that would otherwise be called from its native environment are synchronized. Data stored in application cache **420** may, if necessary, be manually removed. Such manual deletion may be required in instances where data is in error or has otherwise been corrupted and is preventing proper synchronization.

[0135] SMS module **430** comprises or is otherwise coupled to the software, routines, hardware and/or driver devices necessary for initiating a synchronization operation in response to the receipt of an SMS message, which may include interaction with the synchronization module **405**.

[0136] For example, an SMS message is sent from a mobile device or an SMS-gateway website and received at a network operator's Short Message Service Center (SMSC). The SMS message is then stored and forwarded from the SMSC to the recipient mobile device. If the recipient device is off or out of range, the SMS message is stored at the SMSC and delivered at the next possible opportunity or until it expires as determined by network and/or SMSC settings.

[0137] to addition to sending messages, SMS can be used to transport data to a handset; for example, ring tones and operator logos. In conjunction with the Wireless Application Protocol that allows for Internet access from a mobile device and the General Packet Radio Service, configuration data for a particular device can be delivered via an SMS message (e.g., allowing for remote configuration of a WAP browser by a service provider or mobile operator).

[0138] SMS messages may also be used to indicate the receipt of new voice mail or e-mail messages on a mobile device. SMS functionality is also of particular benefit in the context of data synchronization, especially real-time access to e-mail. Many email synchronization systems merely provide for a regularly scheduled synchronization (e.g., every 15 minutes) in order to limit the consumption of bandwidth and/or to preserve battery life on the client device. Such a synchronization schedule deprives the mobile client user of real-time access to their email as exemplified by the arrival of a critical message just seconds after the completion of a timed-synchronization operation.

[0139] The arrival of new data that meets user specified qualifications (e.g., sender, importance, subject content, message content, etc.) may result in the generation of an SMS message that is delivered to the mobile device. The SMS module **430**, upon receipt and processing of the SMS message and any instructive or identifying data contained therein, may initiate a synchronization operation in conjunction with the synchronization module **405**. For example, upon receipt of an SMS message from a server or other computer associated with device **400**, the SMS module **430** may instruct the synchronization module **405** to begin a synchronization operation with the server or associated computer.

[0140] Initiation of the synchronization operation may be governed, however, by certain limitations of the device **400**. For example, if the user of the device **400** is presently engaged in a telephone call, the synchronization operation will not take place. Further, If the user is engaged in a high-bandwidth operation (e.g., receiving streaming media) or is low on battery power, the device **400** may not effectuate the synchronization operation. Such governance may be under the control of SMS module **430**, synchronization module **405** and/or other components of the device **400** (e.g., logic module **310**).

[0141] Identity module **440** comprises or is otherwise coupled to the routines, hardware, driver devices and various device identification tools that may be used to control access to various communications networks and utilization of certain services by the device **400**. For example, identity module **440** may be comprised of an Advanced Intelligent Network (AIN) sub-module (not shown) allowing for access to the AIN. The AIN is a switched voice and data network architecture comprising a variety of network elements allowing for open, interfaced, multi-vendor, telecommunication capabilities. Through these various capabilities, phone companies and service providers are able to define and customize, test and introduce service offerings such as multimedia messaging and ceil routing. The AIN, by further example, allows a wireless user to make and receive phone calls while 'roaming.'

[0142] Optional location module **445** comprises or is otherwise coupled to the routines, hardware—including a GPS receiver (not shown)—and driver devices necessary for GPS functionality in a GPS-equipped device. Signals emitted by GPS satellites arrive at a GPS receiver in the device **400** whereby the GPS receiver can calculate its location in relation to GPS satellite transmissions through a process known as trilateration. Through trilateration, a GPS receiver measures the distance from the GPS satellite using travel time of the GPS satellite signals and thereby pinpoints the physical location of the GPS receiver.

[0143] Optional location module **445** may further comprise the Assisted Global Positioning System (A-GPS). A-GPS uses a combination of GPS satellites and cellular phone base stations to pinpoint location of the mobile device and its GPS receiver and to offer a determination of location that is more accurate than GPS alone. Mobile device GPS receivers, in correlation with an estimate of the mobile handset's location as determined by a cell-sector, can predict with greater accuracy the GPS signal the handset will receive and send that information to the mobile device handset. With this assistance, the size of the frequency search space is reduced and the time-to-first-fix (TTFF) of the signal is reduced from minutes to seconds. A-GPS handset receivers can also detect and demodulate signals that are weaker in magnitude than those required by a traditional GPS receiver. The interaction of A-GPS in a synchronized network or with an assistance server (not shown) in an asynchronous network is generally known in the art.

[0144] Rich media module **450** comprises or is otherwise coupled to the software, routines, hardware and/or driver devices necessary for enabling rich media in device **400**. Rich media includes, but is not limited to, scalable vector graphics, streaming video, animation and Multimedia Messaging Service (MMS). MMS enables the creation, deliver and receipt of text messages that also include an image, audio, and/or video clip. MMS messages may be sent from one mobile device to another or to an e-mail address. MMS generally uses the Synchronized Multimedia Integration Language (SMIL) to define the layout of multimedia content. SMIL is a markup language allowing for the separate access of audio, video and images followed by their subsequent integration and playback as a synchronized multimedia presentation.

[0145] Authentication module **455** comprises or is otherwise coupled to the software, routines, hardware and/or driver devices necessary for authenticating device **400** with regard to the presence of device **400** on a particular network or access to particular services and/or access to data at remote location (e.g., a desktop computer or enterprise server via communication system **110**). Authentication module **455** may work in conjunction with SIP Stack (not shown) and/or identity module **440** with regard to performing authentication routines and/or accessing to network services such as communication system **110**. Authentication module **455** may, in some embodiments, further operate with one or more other modules present at device **400** such as synchronization module **405**, and encryption and decryption modules **415** and **425**. Authentication module **455** may further operate with server- or network-side applications such as an IP or SIP Gateway or access module.

[0146] Authentication module **455** may rely on pre-call validation wherein the MIN and ESN of the device **400** are verified before a call is processed (i.e., before a call is originated or received). Authentication module **455** may utilize a challenge/response process as governed by the Cellular Authentication and Voice Encryption (CAVE) algorithm. A mobile device seeking access to a particular network inputs several parameters into the CAVE algorithm and transmits the result to a Mobile Switching Center (MSC), which controls the switching elements of a cellular system; the MSG makes the same calculations and compares the results. If the results match then the device **400** is deemed authentic and to have legitimate access to the network; if the results do not reconcile with one another (e.g., in the instance of a cloned phone), device **400** is denied access.

[0147] Additional authentication methodologies may be utilized by authentication module **455** including Radio Frequency (RF) Fingerprinting. Just as no two human finger-

prints are exactly identical, transmission characteristics vary slightly between individual cellular phones. Technical details such as phase noise and harmonic spectra can uniquely identify a particular cell phone transmitter. By checking this transmitter signature against a known good signature, an RF fingerprinting system can determine whether a ceil phone trying to place a call is authentic or an impostor.

[0148] Browser module **460** comprises or is otherwise coupled to the software, routines, hardware and/or driver devices necessary for enabling web browsing in a mobile device, for example, HTML and XHTML browsers. Browser module **460** may operate in conjunction with rich media module **450** to the extent a browser enabled by the browser module **460** is utilized to access a web page comprising rich media, for example, streaming media.

[0149] Browser module **460** may utilize the Wireless Application Protocol, an open international standard for applications that use wireless communication and that allows for small, consumer-class wireless devices to access the Internet. As wireless devices do not need a complete web browser implementation to provide web access, a WAP gateway provided by a network service provider may act as a go-between with a Hyper Text Transfer Protocol (HTTP) server to reduce the amount of data that needs to be sent to the device **400** by offloading computational requirements from the phone to the gateway.

[0150] For example, through this offloading methodology, only the fundamental elements of a web page will be transmitted to device **400** whereby the total number of bytes of data transmitted is reduced. The gateway may identify these fundamental elements by identifying Wireless Markup Language (WML) or Wireless Extensible Markup Language (WXML) tags embedded in the web page accessed. Once non-essential data has been stripped from the web page, the page is sent to the wireless device using a lightweight transport stack such as the Uniform Datagram Protocol (UDP).

[0151] Use of the WAP architecture in browser module **460** may further comprise the utilization of sub-protocols such as the WAP application environment (WAE); the session-layer Wireless Session Protocol (WSP); the transaction-layer Wireless Transaction Protocol (WTP); the security-layer Wireless Transport Layer Security (WTLS); and/or the Wireless Datagram Protocol (WDP).

[0152] E-mail client **465** comprises or is otherwise coupled to the software, routines, hardware and/or driver devices necessary for enabling e-mail access in device **400**. For example, e-mail client **465** allows for access to e-mail messages received in an e-mail architecture such as Microsoft Exchange 5.5 2000, 2003; Lotus Domino R5, R6, R6.5; IMPA4; and POP3 and IMAP-accessible Internet e-mail. In conjunction with other modules, for example the SMS/Push module **430** and encryption and decryption modules **415**/**425**, e-mail client **465** may access e-mail as it arrives at a remote e-mail server or desktop computer that is integrated with or coupled to data aggregation server **210** through, for example, a push and/or pull synchronization function.

[0153] E-mail client **465** may also allow for traditional user-to-user electronic mail communications, for example, delivery of a message to an e-mail address associated with a particular mobile device rather than the address of a desktop computer where that message is subsequently forwarded to an associated mobile device.

[0154] E-mail client **465** may be a client developed for a specific mobile device or operating environment. E-mail client **465** may also be a platform portable client. E-mail client **465** may comprise additional functionalities beyond simple receipt/review and generation/delivery of e-mail. E-mail client **465** may further comprise address book functionality. Such address book/contact functionality and the related contact data (e.g., individuals, their e-mail addresses, phone number and other data) may be directly integrated with the e-mail client **465** or separate memory (not shown) in the device **400**. The address book functionality/contact data may also be embodied in a sub- or secondary module coupled to the e-mail client **465** (not shown). In some embodiments, such address book functionality and contact data may be stored remotely, for example, at the communication system **110** or at a server or desktop computer coupled to the device **400** via the communication system **110** and a data connection (e.g., a wireless connection between the communication system **110** and device **400** as well as a related connection between communication system **110** and server **125** or PC **130**).

[0155] The address book functionality and contact data may be utilized to create an interactive, networked experience in conjunction with, for example, dynamic aggregation module **470** as further discussed herein. Utilizing contact data may contribute to a community-like experience including enhanced presence, peer-to-peer communication and information sharing.

[0156] Dynamic aggregation module **470** comprises or is otherwise coupled to the software, routines, hardware and/or driver devices necessary for enabling access to and interaction with certain other modules at the device **400** (e.g., e-mail client **465**) and data aggregation server **210** (e.g., presence module **320**, location module **330**, calendar module **340** and groups module **350**) allowing for the dynamic aggregation of information from various users and/or data depositories and the utilization and display of that information for various functionalities, such as group calendaring functionality. Dynamic aggregation module **470** organizes, filters and presents information from multiple inputs concerning context, relationship and communication means.

[0157] FIG. **5** is an illustration of exemplary networked relationships **500** amongst a variety of sources of PIM data (**530**-**580**) and a data aggregation server **510** as may be found in the present invention.

[0158] Data aggregation server **510** is an aggregation server like that described in FIGS. **2** and **3** and as may be integrated with or otherwise communicatively coupled to a service provider communications network **520** (e.g., Cingular Wireless or AT&T Inc). The data aggregation server **510** is coupled to various sources of PIM data such as PCs **530**, enterprise servers **540**, mobile phones **550**, instant messaging networks **560**, ISPs **570** or other information sources such as PDAs or Smartphones **580**.

[0159] While FIG. **5** reflects direct connections between the data aggregation server **510** (via service provider communications network **520**) and these various sources of PIM data **530**-**580**, this is not suggest the requirement or existence of a point-to-point or direct connection. For example, mobile phone **4550** will be connected to the data aggregation server **510** through not only the service provider communications network **520** in addition to a variety of base stations and other intermediate communications networks (not shown). Similarly, a computer network as provided by PC **530** or enterprise server **540** will comprise a series of routers between the source of information (e.g., the PC **530**) and the data aggre-

gation server **510**. Similarly, an Internet portal **570** like Yahoo!® or an IM network **560** like that offered by America Online™ will comprise a series of gateways, servers and/or other intermediate software and/or hardware before becoming communicatively coupled with the local and wide area networks that will further couple the Internet portal **570** or IM network **560** to the data aggregation server **510** via the service provider communications networks **520**.

[0160] PC **530** may be any type of home computing device; for example, a desktop computer or a laptop computer like PC **130** in FIG. **1**. PC **530** may be coupled to data aggregation server **510** via an ISP such as AT&T Inc., which provides DSL service or a dial-up service provider such as America Online™. The present invention envisions the use of a variety of communication channels for communicating between a PIM data source and the data aggregation server **510**, for example, the aforementioned DSL and dial-up services as well as satellite and wireless communications. Other communication mediums may be utilized as well, such as Bluetooth or InfraRed. No limitation as to the use of a particular communication medium is meant to be imposed by the present invention nor is there meant to be the requirement of a homogeneous communication link between the PIM data source and the data aggregation server **510** (e.g., there need not be—nor will there usually be—a single DSL link alt the way between PC **530** and the actual data aggregation server **510**).

[0161] PC **530** may be equipped with connection software allowing for the establishment of a data connection between the PC **530** and a communications management system (like that described in FIG. **1**) whereby data may be synchronized with an associated mobile device (e.g., mobile device **550**). Such a data connection may allow for the redirection of, for example, e-mail and mobile access to PIM data residing in a memory store at the PC **530**.

[0162] Enterprise server **540** shares similarities to PC **530** with the exception that the enterprise server **540**'s architecture is more complex with regard to the introduction of not only the server but often a series of additional application servers, data stores and work stations that may resemble (or be the same as) a computing device like PC **530**. Enterprise server **540** may be exemplified as a Microsoft® Exchange Server or a Lotus® Domino Server from IBM to manage the receipt, storage, delivery and access to e-mail as well as other application and PIM data. An enterprise server generally serves a larger group of users via a server-client relationship whereas a single PC (e.g., a home computer) generally serves an individual user. Enterprise server **540** may also comprise a software connector allowing for redirection and access to e-mail and other corporate data to an associated mobile device (e.g., mobile device **550**) via a communications management system like that described in FIG. **1**.

[0163] Mobile device **550** may be a cellular device allowing for Internet or other data access whereby a data connection with a communications management system (like that in FIG. **1**) and/or data aggregation server **510** may be established. In an exemplary embodiment of the present invention, the network architecture and service provider communications networks **520** of a mobile service provider may be directly integrated with the data aggregation server **510** of the present invention. Data aggregation server **510** may also be integrated with other network operators (e.g., shared by a plurality of service providers) or communicatively coupled to another service provider communications network **520** comprising its own data aggregation server **510** (e.g., a data aggregation server in the Cingular Wireless network may be coupled to a data aggregation server in a Sprint Nextel network).

[0164] IM network **560** provides the necessary functionality (e.g., hardware and software) to allow for real-time, text-based conferencing over the Internet or another communications network between two or more people. Many IM providers now offer the integration of still-images, avatars, audio clips and, in some instances, video clips as a part of the IM experience. IM network **560** may also provide a series of contact lists or 'buddy lists' that function as a source of contact information (i.e., PIM data) utilized by the data aggregation server **510** and, more specifically, a groups module as described in FIG. **3**. An example of an IM network service provider is America Online™. America Online™ provides instant messaging not only to America Online™ dial-up service subscribers but also as an independent application that may be downloaded and installed on a desktop computer (e.g., PC **530**) or, as is increasingly common, a mobile device (e.g., mobile device **550**).

[0165] Internet portal **570** may be a single point for the access of information over the Internet, specifically, the World Wide Web. Yahoo!® is an example of an Internet portal **570** that provides a comprehensive single point of access for, conceivably, any information the average individual would need from the World Wide Web; for example, a search engine, maps, news, weather, e-mail, calendaring, various other forms of PIM data and so forth. Consistent with being a single offering, Internet portal **570** may offer a variety of other services including instant messaging (e.g., Yahoo!® Messenger) or even Internet access (e.g., Yahoo!®/SBC® DSL). By logging on with a user ID and password, Internet portal **570** may also allow for the generation and customization of personal pages wherein the user can request the delivery of and direct the layout of particular information, including PIM data.

[0166] For example, a particular user may want headline news pertaining only to the San Francisco area but also desires weather reports in Sunnyvale, Calif., and San Francisco, Calif., as the user might live in one location and commute to the other for work. Similarly, the user may be a transplant from the East Coast and still actively follow sports teams on the East Coast. As such, the user may further organize their personal page to display sports scores concerning the Boston Bruins hockey team and the Boston Red Sox baseball team instead of information concerning the San Jose Sharks and San Francisco Giants, which might otherwise be logically be displayed in the context of news and weather for the San Francisco region.

[0167] As noted, certain of this information may be utilized in the context of identifying and generating PIM data aggregated by the data aggregation platform **510**. For example, a personal calendar displayed on the user's personal page; an address book linked to the user's personal page and so on.

[0168] PDA **580** may be a portable device offering, for example, notepad and calendar/scheduling functionality. PDA **580** may have certain network functionality to allow for data exchanges with other PDAs or compatible devices as well as a larger communications network enabling synchronization with a home or work computer where a companion calendaring program may be installed. Many PDA functionalities have been incorporated into the likes of mobile device **550** or smart phones.

[0169] The various aggregation modules of the data aggregation server **510** may acquire data from these various information sources of PIM data through integration with a particular data source. For example, the data aggregation server **510** may be integrated or configured to access and operate with an instant messaging network **560** like that offered by America Online. That is, America Online and a service provider implementing the data aggregation server **510** may reach an agreement allowing access of the data aggregation server **510** to the instant messaging network **560** thereby providing near unfettered access and certain sharing of information between the two systems as a result of systematic design. Once the data aggregation server **510** is implemented/integrated with, for example, the instant messaging network **560**, data aggregation may commence unabated as the data aggregation server **510** operates as if it is a normal operating presence in the network.

[0170] The various aggregation modules of the data aggregation server **510** may also act as a proxy with the proper user credentials to access a particular information network. For example, the data aggregation server **510** may be provided by certain user name and password information to access an Internet portal **570** like Yahoo!®. That is, a user of the services offered by the data aggregation server **510** would provide their user name and password to the data aggregation server **510**, most likely during a registration or subsequent account update procedure. Thus, any time the data aggregation server **510** seeks to access the Yahoo!® Internet portal **570** to acquire information from, for example, an online/webpage calendar, the user's username and password will be provided to the Yahoo!® Internet portal **570** just as if the user were sitting in front of a keyboard and display and manually entering the information. Once access is granted to the Internet portal **570**, aggregation of information may commence.

[0171] In some instances, various authentication tokens or cookies might be granted by various PIM data sources either as the result of a request to access certain PIM data or as a result of a correct username/password combination. Various security methodologies as discussed in the context of, for example, access module **310** (above) may also be applicable with regard to establishing credentialed relationships between the data aggregation platform **510** and various sources of PIM data.

[0172] It some instances, it is perceived that a combination of data aggregation methodologies may be necessary. For example, username and password for certain PIM data sources and system integration for others.

[0173] The data aggregation server **510** also provides for the aggregation of data from amongst different users of the service. For example, one user may provide his various user names and passwords in order to access certain PIM information stored in that particular users different PIM sources such as an instant messaging network **560** or an Internet portal **570**. But aggregating one user's information does not help to create a network of information. In order to build a larger informational community, access to other user's PIM data is required. But while an instant messaging networks may allow the data aggregation server **510** access based on system integration or username/password combinations (either directly or by proxy), any secure system will be unlikely to allow a first user to access a second user's information without some sort of permission.

[0174] While that permission may be explicitly granted by another user (e.g., User B grants User A to access their information at instant messaging network **560**), such an arrangement is unlikely because of security and privacy concerns of both the instant messaging network **560** and the user. For example, a user may have no qualms about granting another user information about certain information on an instant messaging contacts list (e.g., professional colleagues with whom both users interact in the office) but will likely be hesitant to share information concerning family members or other personal relationships. Control of who receives what information can cause the implementation of an entire new layer of security or management software that the instant messaging network **560** may be hesitant to implement because of costs or other concerns.

[0175] Such a concern is the fact that most instant messaging network (like America Online) are not in the business of providing an open network. That is, these services provide an instant messaging service to individual users and subscribers and it is up to those individual users to determine who knows who is on their contacts list; that is, America Online will not provide that information to other users. While data representative of that information may be stored by the instant messaging service that service will likely make every effort to keep that list secure and private from all other users. The service provider offering means to share or network this contact or other PIM data is unlikely due to, at the least, privacy and business/commercial relations in the marketplace.

[0176] The present data aggregation server **510** overcomes this hesitancy of different PIM data sources to openly share information. For example, User A and User B are both members/users of the data aggregation server **510**. User A may provide certain security information to the data aggregation server **510** in order to access the aforementioned instant messaging network **560**. In this way, User A can aggregate PIM data from his instant messaging network account (e.g., members of his contacts lists, those members instant messaging IDs and so forth). User A will unlikely have immediate access to similar PIM information held in an account assigned to User B for at least the reasons discussed above. Notwithstanding, User B will have provided certain security information to the data aggregation server **510** to allow the collection of PIM data in his account.

[0177] While an instant messaging network **560** may not be obliged to provide a system for sharing PIM data amongst its users, the present data aggregation server **510** does provide such interactions. User A will set up certain permissions with the data aggregation server **510** to allow User B to access User A's PIM data. User B will provide similar permissions such that User A may access User B PIM data. The permissions system of the data aggregation server **510** also allows for setting of limitation on who may access what information. Therefore, User A may allow for User B to access his contacts information—but not his calendar information. Similarly, User B may allow User A access to his calendar information but not his presence information. Permissions may be assigned to individuals via, for example, contacts module **360** or to groups of individuals as may be determined by the groups module **350**. In one embodiment of the present invention, a permissions module (not shown) may govern these relationships. In another embodiment, such permissions may be governed by the access module **310**.

[0178] Sub-permission levels may also be set in the data aggregation server **510**. For example, User A may be able to access User B's calendar information—but only particular aspects of his calendar information as may be governed by,

for example, metadata. Similar limitations may be set with regard to other PIM data (e.g., access only to personal contacts and not professional contacts).

[0179] The shared PIM data (via permissions) of the data aggregation server **510** enables the creation of a growing network of contacts and relationships. For example, User A may know User B; User B, in turn, may know User C. As a result of this single-degree of separation, User A may now have access to User Cs contact information. Additional permissions may be set with regard to how many degrees of separation information is shared (e.g., only with persons on my contact list or with persons on the contact lists of persons on my contact list).

[0180] Additional permissions may be imposed with regard to aggregating data to complete incomplete data records. For example, User A may have an entry for John Doe but no phone number for John Doe. User B, however, may know John Doe as well and have a complete data entry (e.g., name, phone, address, birthday, etc.). Permission settings may be established wherein the data aggregation server **510**, on behalf of User A, accesses the data of User B to gather the remainder of this contact information (e.g., phone number). While User A may now have a complete data record for John Doe, he may be entirely unaware of the source of that information. That is, User A may now know that information was aggregated from PIM data of User B or that John Doe is on User B's contacts list.

[0181] Access to various PIM data of other users by the data aggregation server **510** occurs as a result of the operation and interaction of various modules within the data aggregation server **510**.

[0182] In this way, certain protocol limitations may also be overcome in that it is not necessary for User A (who might be a Yahoo!) user to directly communicate with an America Online system for the purposes of acquiring information about User B. User B, instead, directly interacts with me America Online system and then User B shares that information with User A in a common protocol.

[0183] Notwithstanding the protocol particularities of certain networks or PIM data sources, the present invention may, in an embodiment, utilize whatever protocol is necessary to communicate with that network/PIM data source in a way that the particular network/PIM data source will understand communications from the various modules of the data aggregation server **510**. For example, the present invention would communicate with the Yahoo!® Internet Portal with regard to e-mail using IMAP. The present invention would communicate with a Microsoft® Exchange® Server using MAPI and so on. Distribution of data, too, may require the use of multiple protocols. For example, TCP/IP for a standard data connection to, for example, a desktop computer but use of WAP for communicating with a wireless device. In that regard, the present invention may be multi-protocol based.

[0184] FIGS. **6**A-**6**F are exemplary embodiments of a series of groups lists and functions as enabled by groups module **350** at server **300** (**210**). FIG. **6**A is an exemplary device **400** like that illustrated in FIG. **4**. Device **400**, through dynamic aggregation module **470**, has displayed all contacts **600** for the user of device **400**. The list of contacts **610** includes a groups list **620**. Groups list **620** in FIG. **6**A is presently in a minimized status, which allows for the preservation of display space.

[0185] FIG. **6**B is also an exemplary device **400** like that illustrated in FIG. **4** and referenced in FIG. **6**A. The groups list **620** has, in FIG. **6**B, been expanded to reflect individual group lists **625**. In the present figure, individual group lists **625** include a Family List, an Office Group List and a School Friends List.

[0186] FIG. **6**C is also an exemplary device **400** like that illustrated in FIG. **4** and referenced in FIGS. **6**A and **6**B. The expanded groups list **620** has, in the present illustration, been limited to a particular individual groups list **625**, in this case the School Friends List. Individual groups lists **625** may be selected through five-way navigation, a built-in QWERTY keyboard, a stylus or any other data entry and selection method as is present in a particular device **400**.

[0187] In FIG. **6**C, the individual groups list **625**—School Friends—reflects the members **630** of that particular individual groups list **625**. All other contacts **610**, including those presently a part of individual groups list **625**, are concurrently displayed in a split-screen format. In some embodiments, only the members **630** will be displayed; other embodiments will allow for the display of members **630** as well as all other contacts **610** as is the case in the present display embodiment.

[0188] Through the concurrent display of ail contacts **610** and members **630**, a user may be able to add individuals from the ail contacts list **610** to the members **630** list. In the present embodiment the name 'Pat Wong' is highlighted. Through selection and verification of the intention to add 'Pat Wong' to members **630** list, the contact identity for Pat Wong will be replicated on the members **630** list of individual groups list **625**.

[0189] FIG. **6**D illustrates a setting screen **640** as it pertains to members **630** of an individual groups list **625**. Setting screen **640** is used to set preferred contact methods **645**, permissions **650** for a particular individual or particular members **630** and expiration dates **655** as they pertain to the present settings **640**.

[0190] In the present setting screen **640**, members **630** of the School Friends individual group list **625** are being informed of the present user's preferred contact method **645**. In the present example, the preferred contact method **645** is the personal e-mail of the user. This means that members **630** of the individual groups list **625** 'School Friends,' when accessing contact information on the data aggregation server **210**, will be able to view the personal email address of the present user as well as related presence information with this address. Members **630**, having been informed of preferred contact method **645**, should contact the present user via the personal e-mail address as it is the preferred contact method **645**.

[0191] Permissions **650** are the different levels of informational access granted to group members as they pertain to the particular user of the data aggregation server **210**. For example, in the present settings **640**, other members **630** of the present group **625** are allowed to view calendar information of the user but only as it pertains to free time and whether the present user is busy or unavailable. Location information of the user is also available but only following a request that must be approved by the user. Additional permissions may be set, such as presence (e.g. on-line or off-line for particular services) or different information as it pertains to calendar metadata (e.g., cannot miss appointments, birthdays, anniversaries and so forth). Permissions are limited only to the extent of information that may be aggregated by server **210**. That is, as more information becomes available through data aggregation, new permissions will develop, evolve and be implemented through server **210** or manually at device **400**.

[0192] Expiration **655** sets the date at which the present settings **640** expire. For example, a user may be engaged to work on a particular project with a particular group of colleagues. The user may want to have this particular group (perhaps known as Project Colleagues) to have access to certain contact information and permissions—but only while the project is ongoing. As such, the user can arrange—via expiration setting **655**—for the various settings of the group to expire on, for example, the finish date of the project. Expiration dates may also be a temporal period (e.g., 2 weeks) instead of a particular date. In the present example, the expiration **655** has been set to 'never' in that the persons that the user went to school with will always be the persons the user went to school with and, at the present, sees no reasons to limit their access to his contact information for the foreseeable future.

[0193] FIG. **6**E is an exemplary display screen as enabled by groups module **350** and dynamic aggregation module **470**. FIG. **6**E is a summary screen **660** for the present group list **625** (School Friends). An indicator of presence **665** relative to the server **210** (and communication system **110**) as well as preferred contact methodology **670** is displayed for each member **630** of the present group list **625**.

[0194] For example, Ann Smith is presently connected to server **210**/communication system **110** via Yahoo!® Messenger (**665**) but prefers being contacted at her work number (**670**). Similarly, Frankie Smith is connected to server **210**/communication system **110** via a mobile device (e.g., a cell phone) (**665**) and prefers being contacted that way as well (**670**). Mark Wodds is connected to the server **210**/communication system **110** via a desktop or laptop computing device (**670**) and prefers to be contacted via e-mail (**670**). Sam Walters is connected to the server **210**/communication system **110** via a mobile device (**665**) and prefers to be contacted at that device as well (**670**).

[0195] References to 'connected to the platform/communication system' are not meant to be interpreted as a physical, hard connection. Instead, connected is used in the sense that a user has access to information at the server **210**/communication system **110** and vice-versa. That connection may be the result of a direct point-to-point connection but is, most likely, the result of a data interchange through various routers and/or switches and base stations depending on the present mode of connection.

[0196] FIG. **6**F is an exemplary status screen display as enabled by groups module **350** in conjunction with data aggregation module **470** and indicating the status of each particular user's presence status **685** and a contact status indicator **690**.

[0197] For example, Ann Smith has a connection with server **210**/communication system **110** via her phone and desktop (via Yahoo!® Messenger as seen in FIG. **6**E). Ann Smith's mobile phone currently has an active connection with server **210**/communication system **110** as does her Yahoo!® Messenger account. This active presence is indicated by the smiling emoticon (**685**).

[0198] Sam Walters, on the other hand, is not available as indicated by the frowning emoticon (**685**). Sam Walters is connected to the server **210**/communication system **110** via a mobile phone (as was shown in FIG. **6**E). Sam Walters' phone is at present, indicating his unavailability. This unavailability may be the result of his phone having been turned off, traveling out of range or having been manually set to an indicia that he is not available to be contacted at present.

[0199] Mark Wodds, however, has no presence information available (**685**). This may be a result of Mark Wodds having set his permissions to not display any information concerning his presence or the fact that server **210**/communication system **110** may not be able to provide any presence information at the present time.

[0200] Frankie Smith, as a result of his presence settings, has allowed access to calendar information as is evidenced by the calendar icon (**685**). Notwithstanding, Frankie Smith is not available as he is presently in a meeting. This unavailability may be the result of Frankie Smith having manually set his device to evidence unavailability or because of a determination by Mr. Smith's device (through dynamic aggregation module **470** and calendar module **340**) that he is presently unavailable due to his calendar indicating his presence in a meeting. Due to the fact that he is in a meeting, it may be presumed that Frankie Smith is unable to take calls. Certain calendar settings, however, may be adjusted to reflect that the meeting is of low priority or that such a meeting is informal and that he may be interrupted. Such an indication, however, may be displayed only to particular persons (e.g., immediate family who know only to contact him if it is a dire emergency) via the proper permission.

[0201] Presence status **685** need not be limited to a particular icon (e.g., an emoticon) or text message. Any means of communications (e.g., graphic, textual, color coding) may be used.

[0202] Each member **630** of the groups list **625** also evidences a contact status indicator **690**. Contact status indicator **690** reflects recent or queued communications from a particular member **630** of the list **625** or an important event related to a member **630**. For example, a queue may be set to the last five communications or to the most recent communication. Similarly, only particular types of communications may be displayed, for example, only telephone calls versus e-mails if a user happens to know that a member of the group only shares important communications by phone. Other types of communications, such as directions, or important events like anniversaries may also be displayed as may be derived from various contact data, such as calendar data.

[0203] For example, Ann Smith recently made a phone call to the present user as indicated by contact status indicator **690**. That call went unanswered as is evidenced by the indicator '1 missed call.' If Ann Smith had called additional times, the indicator **690** may read '2 missed calls' or '3 missed calls.' In the present view, the missed call is reflected without an explanation point (!) as are certain indicators for other members (e.g., Frankie Smith's birthday indicator **690**). The use of importance indicators may further aid in determining how recently the indicator **690** was received or the urgency (**595**) of the same (e.g., high, low or Intermediate importance).

[0204] For example, the phone call of Ann Smith may have been received and missed. The missed call indicator **690**, in this instance, may have initially displayed an '!' or other importance indicator **695** when the display was first reviewed as the result of a menu selection or flipping open a phone face. At this point, the user would have seen (or at least should have seen) the importance indicator **695**. User may have elected not to have further investigated the nature of the missed call. If the user later opened his phone or accessed the current status display **680**, that Importance indicator **695** may have been removed (e.g., no exclamation point) in that the user knows that the call was received and missed. This way, the

user can quickly determine which messages or events are new or have been updated since last checking the status screen **580**.

[0205] By further example, Frankie Smith currently reflects a birthday in his contact status indicator **690**. The fact that Frankie Smith has a birthday can be the result of user having manually entered a birthday reminder into his calendar or, alternatively, that information having been entered into the calendar of Frankie Smith who has chosen to share that level of calendar information with other members **630** of the group list **625** and that are connected to server **210**/communication system **110**.

[0206] The birthday indicator could also be the result of the user having accessed the calendar of another user. For example, the present user may not have the birthday of Frankie Smith in his calendar and Frankie Smith may not allow access to his calendar to reflect that it is his birthday. The present user, however, may have access to the calendar of Ann Smith who has set her permissions to allow other people to access this level of calendar information; her calendar may reflect the birthday of Frankie Smith. As Frankie Smith is a member **630** of the present group list **625**, the groups module **350** and/or calendar module **340** may determine that this is information that the present user may find important and could provide the information about user Frankie Smith via another member **630**—Ann Smith—of the group list **625**. In some embodiments, the present user may specifically request such information or reject such information for further use when presented. Such a rejection may be in response to a prompt generated by device **400** through dynamic aggregation module **470**.

[0207] In the case of Mark Wodds, his contact status indicator **690** reflects that directions have been received. The indicator **690** further reflects an explanation point for an importance indicator **695** suggesting that the directions to a particular location were recently received or at least received since the display was last viewed. Alternatively, the directions may have been provided in response to an urgent request for the same (e.g., directions to a meeting that is just about to start).

[0208] In the case of Sam Walters, there is an e-mail waiting to be read. The indicator **690** also reflects that this e-mail is urgent as may be indicated as the result of the sender of the e-mail, for example, setting a high importance feature in Microsoft Outlook or as determined from other metadata embedded in the e-mail message.

[0209] FIG. **7**A is an exemplary view of aggregated contact information (contact detail **710**) for a particular contact (Eric Ham) as may be generated by the dynamic aggregation module **470** of the present invention.

[0210] Presence indicator **720** reflects that no presence information is presently available for Eric Ham; this is reflected by the literal text: 'no information available' in addition to the frowning emoticon. The absence of information may be the result of Eric Ham's connection to the server **210**/communication system **110** having been severed due to a service outage or his connection having been severed. Similarly, the present user may not have sufficient permission levels as granted by Eric Ham with regard to accessing his presence information. Eric Ham's means of establishing presence with server **210**/communication system **110** is through Yahoo!® Messenger as indicated by indicator of presence **725**.

[0211] Telephone contact entry **730** reflects different means of contacting Eric Ham by phone, for example, a home phone and a mobile phone. In the present contact detail **710**, a preferred telephone number for contacting Eric Ham, that is, a home number, is designated. This designation may be set by the present user or as a result of a preferred contact method **770** as identified by Eric Ham and communicated to users with access to this information via server **210**/communication system **110** and data aggregation module **470**.

[0212] E-mail contact entry **740** reflects different means of contact Eric Ham by e-mail. For example, Eric Ham could be contacted via a personal account, a work account or a professional account (e.g., an account set-up through the ACM). In the present contact detail **710** screen display, e-mail address 2 (a personal account offered by Yahoo!®) is designated as the preferred means of contacting Eric Ham. This designation may be set by the present user or as a result of a preferred contact method **770** as identified by Eric Ham and communicated to users with access to this information via server **210**/communication system **110** and data aggregation module **470**.

[0213] Instant messaging entry **750** reflects different means of contacting Eric Ham by instant messenger. For example, Eric Ham could be contacted via a Yahoo!® instant messenger account as well as an America Online instant messenger account. In the present screen display, the Yahoo!® instant messaging account is designated as the preferred means of contacting Eric Ham via instant messenger. This designation may be set by the present user or as a result of a preferred contact method **770** as identified by Eric Ham and communicated to users with access to this information via server **210**/communication system **110** and data aggregation module **470**.

[0214] FIG. **7**B is an exemplary view of various contact settings **760** of the present user as communicated to use Eric Ham and as may be utilized by the dynamic aggregation module **470** and server **210**/communication system **110** of the present invention, including calendar module **340**. This display is similar to the display illustrated in FIG. **6**D with the exception that it pertain to a particular Individual (Eric Ham) rather than a group **625** or members **630** of that group **625**. Screen of mobile device **400** reflects preferred contact methods **770**, particular permissions **780** for a particular user and synchronization settings **790** as they pertain to the present individual.

[0215] In the present contacts setting **760**, Eric Ham is being informed that the present user's preferred contact method **770** is via personal e-mail. Similarly, this setting could be adjusted to reflect a corporate e-mail account, a work phone, a home phone or a cellular phone.

[0216] Permissions as to presence **780** are being set to allow for calendar and phone and locations by request only. That is, Eric Ham will be able—through a device **400** comprising a dynamic aggregation module **470** and accessing server **210**/communication system **110**—allowed to view calendar information of the present user. Eric Ham will also be able to view whether the present user is presently available by phone. Location information of the present user is also available but only following a request that must be approved by the present user. As in FIG. **6**D, permissions **780** are limited only to the extent of information that is aggregated by server **210**/communication system **110**.

[0217] Synchronization **790** has been set with regard to allowing certain synchronization properties from a particular source, in the present example, a Yahoo! address book.

[0218] While the present invention has been described in connection with a series of preferred embodiment, these descriptions are not intended to limit the scope of the invention to the particular forms set forth herein. To the contrary, the present descriptions are intended to cover such alternatives, modifications, and equivalents as may be included within the spirit and scope of the invention as defined by the appended claims and otherwise appreciated by one of ordinary skill in the art.

1.-**24**. (canceled)

25. A system for aggregating and accessing data, the system comprising:

a server configured to acquire data from users in a peer-to-peer community, the data acquired from a data source in a service provider network and a data source outside the service provider network, wherein the data acquired from the data source outside the service provider network is acquired using a proxied credential; and

a mobile device communicatively coupled to the server, the mobile device configured for selective access of data acquired from users in the peer-to-peer community, the acquired data maintained in a storage medium coupled to the data aggregation server.

26. The system of claim **25**, wherein the server is implemented by a network service provider as a part of the service provider network.

27. The system of claim **25**, further comprising a personal computing device communicatively coupled to the data aggregation server, the personal computing device associated with a user from the peer-to-peer community.

28. The system of claim **27**, wherein the personal computing device maintains personal information management (PIM) data associated with the user from the peer-to-peer community.

29. The system of claim **27**, wherein the personal computing device is further communicatively coupled to the mobile device, the mobile device associated with the user from the peer-to-peer community.

30. The system of claim **27**, wherein the personal computing device is the data source in the service provider network and the server acquires data from the personal computing device through a pull operation initiated by the server.

31. The system of claim **27**, wherein the personal computing device is the data source in the service provider network and the server acquires data from the personal computing device through a push operation initiated by the personal computing device.

32. The system of claim **30**, wherein the pull operation initiated by the server occurs in response to a request initiated by the mobile device.

33. The system of claim **25**, wherein the acquired data includes calendar data.

34. The system of claim **25**, wherein the acquired data includes contact data.

35. The system of claim **25**, wherein the acquired data includes presence data.

36. The system of claim **25**, wherein the acquired data includes location data.

37. The system of claim **25**, wherein the server is further configured to identify a common characteristic in the data acquired from the peer-to-peer community.

38. The system of claim **37**, wherein the server is further configured to generate a group in accordance with the common characteristic in the data acquired from the peer-to-peer community.

39. A method of acquiring data in a peer-to-peer community, the method comprising:

acquiring data from a data source in a service provider network;

acquiring data from a data source outside the service provider network, wherein the data acquired from the data outside the service provider network is acquired using a proxied credential; and

storing the data acquired from the data source in the service provider network and outside the service provider network in a storage medium for selective access by a mobile device.

40. The method of claim **39**, wherein the data source outside the service provider network includes a personal computing device.

41. The method of claim **39**, wherein the data source outside the service provider network includes an enterprise server.

42. The method of claim **39**, wherein the data source outside the service provider network is an Internet portal.

43. The method of claim **39**, wherein the data selectively accessed by the mobile device includes both data from in the service provider network and outside the service provider network.

44. The method of claim **39**, wherein acquiring data from the data source outside the service provider network includes the use of a communications protocol native to the data source outside the service provider network.

* * * * *