



SYSTEM AND METHOD FOR MANAGING AND DISTRIBUTING PERSONAL INFORMATION OVER A NETWORK

TECHNICAL FIELD

[0001] The invention is generally related to the area of management of distributed information. In particular, the invention is related to management and distribution of personal information over a network. Various embodiments disclosed herein relate to personal information security and management.

BACKGROUND

[0002] In today's world of electronic information-sharing, we as individuals provide personal information to other individuals, such as family and friends, or to any other entities, such as businesses and organizations. Consequently, our personal information may end up being stored electronically in many different places, such as in our friends' computers, mobile phones, and tablet devices; and in databases, such as those of financial institutions, healthcare providers, government agencies, and the like.

[0003] Our personal information can include non-sensitive information, such as, but not limited to, phone numbers and email addresses, as well as sensitive information, such as, but not limited to, social security numbers, credit card numbers, and bank account numbers. If an individual's personal information changes, it is typically up to the individual to inform everyone of the change, which is a manual process (via phone, email, text message, website, etc). This notification process takes time and effort on the part of the individual. Additionally, the individual may not remember everyone that has his/her information, so some individuals or other entities are not notified of the change. Further, there is no guarantee that the recipients of the new information will update their electronic records for this individual. As a result, there is high potential for human error in this manual notification process.

[0004] With respect to impact on business, over 40 million people in the United States move each year. On average, people will change jobs 11 times in their lifetime. Businesses experience significant budgetary waste around inaccurate personal information data. For example, recent

surveys revealed that nearly two out of three businesses find that between five and thirty percent of their marketing budget is wasted annually as a result of bad data. Further, the loss of customers due to inaccurate contact data can be very costly. For example, acquiring a new customer can cost 6 to 7 times more than retaining an existing customer. Therefore, with respect to managing personal information, new approaches are needed for keeping personal information current when it changes.

BRIEF DESCRIPTION OF THE DRAWINGS

[0005] Various inventive embodiments disclosed herein, both as to its organization and manner of operation, together with further objectives and advantages, may be best understood by reference to the following description, taken in connection with the accompanying drawings as set forth below:

Figure 1 illustrates a block diagram of a personal information management system for managing and distributing personal information over a network;

Figure 2 illustrates a block diagram of a user information container of the personal information management system of Figure 1;

Figures 3A and 3B show one example of coding the user information container of Figure 2;

Figure 4 illustrates another block diagram of the personal information management system for managing and distributing personal information between, for example, two users;

Figure 5 illustrates a schematic diagram of the communication links between two users of the personal information management system of Figure 1, according to a minimum configuration;

Figure 6 illustrates a schematic diagram of the communication links between two users of the personal information management system of Figure 1, according to an expanded configuration;

Figure 7 illustrates a schematic diagram of the communication links between two users of the personal information management system of Figure 1, according to yet another configuration;

Figures 8A and 8B illustrate a flow diagram of an example of a method of establishing the communication links between two users in the personal information management system of Figure 1; and

Figure 9 illustrates a flow diagram of an example of a method of automatically distributing personal information using the personal information management system of Figure 1.

DETAILED DESCRIPTION

[0006] In the following description, numerous specific details are set forth in order to provide a thorough understanding of the present invention. However, it will become obvious to those skilled in the art that the present invention may be practiced without these specific details. The description and representation herein are the common means used by those experienced or skilled in the art to most effectively convey the substance of their work to others skilled in the art. In other instances, well-known methods, procedures, components, and circuitry have not been described in detail to avoid unnecessarily obscuring aspects of the present invention.

[0007] Reference herein to “one embodiment” or “an embodiment” means that a particular feature, structure, or characteristic described in connection with the embodiment can be included in at least one embodiment of the invention. The appearances of the phrase “in one embodiment” in various places in the specification are not necessarily all referring to the same embodiment, nor are separate or alternative embodiments mutually exclusive of other embodiments. Further, the order of blocks in process flowcharts or diagrams representing one or more embodiments of the invention do not inherently indicate any particular order nor imply any limitations in the invention.

[0008] A personal information management system for and methods of managing and distributing personal information over a network is disclosed. For example, the personal information management system provides mechanisms by which users can update their personal information in one place and then the updated information is automatically distributed to other users. Further, the personal information management system includes mechanisms by which users can manage what portion or portions of their personal information is shared with other users, wherein the personal information shared with one recipient can be different than the personal information shared with another recipient. The personal information management system disclosed herein provides benefit over conventional manual methods of distributing updated personal information in that it is capable of automatically distributing updated personal information to any entities with which a user has a relationship. Further, the connection between one user and another persists indefinitely over time so that updated personal information can be distributed without the user having to remember every entity with which he/she has a relationship over a period of time.

[0009] Figure 1 illustrates a block diagram of a personal information management system 100 for managing and distributing personal information over a network. Personal information management system 100 includes an application server 110 that the further includes a personal information application 112 and a data store 114. Personal information application 112 includes, for example, a connections manager 116, a notifications manager 118, an authentication module 120, and a security module 122. Stored in data store 114 are, for example, user data 126 and user information containers (UICs) 128.

[0010] A plurality of users 105 is associated with personal information management system 100. Users 105 may include individuals, groups of individuals, entities, and groups of entities, where entities can be, for example, any companies or organizations of any kind. Users 105 access application server 110 via a plurality of user computers 130, which are connected to application server 110 via a network 140. User computers 130 can be any computer devices, such as, but not limited to, desktop computers, laptop computers, handheld computing devices, mobile phones, and tablet devices.

[0011] Further, there may be certain information storage 132 on user computers 130. For a certain user 105, information storage 132 at his/her user computer 130 may contain personal information of other users 105. For example, information storage 132 can be an address book, contacts in an email application, contacts on a mobile phone, a customer relationship management (CRM) database of a business, and the like. Further, a certain user 105 may have multiple sets of information storage 132. In other words, information about one user 105 can be stored in multiple places of other user 105. Additionally, the information stored in information storage 132 is static, while updated/dynamic data resides at user data 126 and UICs 128 at data store 114 of personal information application 112.

[0012] Users 105 can use a personal information application user interface (PIA user interface) 134 at their respective user computers 130 to interact with personal information application 112 at application server 110 and manage their own personal information and the personal information of other users 105 that may be stored in information storage 132. PIA user interface 134 may be implemented as a web application and run in a web browser, such as Internet Explorer. However, PIA user interface 134 may be implemented by other means, such as a .NET application, a light weight desktop application, a mobile app, an API, and the like.

[0013] Additionally, users 105 can be classified as member-users 105 and guest-users 105. Member-users 105 are those users who have joined personal information management system 100 and therefore have access to personal information application 112 at application server 110. By contrast, guest-users 105 are those users who have not joined personal information management system 100 and therefore do not have access to personal information application 112 at application server 110, yet guest-users 105 can still receive information updates from member-users 105. Namely, guest-users 105 are granted limited access to personal information application 112 at application server 110. That is, guest-users 105 are granted just enough access to personal information application 112 to view/receive updates from member-users 105, such as via a secure URL.

[0014] Network 140 may be, for example, a local area network (LAN, wired or wireless) and/or a wide area network (WAN) for connecting to the Internet or to an Intranet. Application server 110 and user computers 130 may connect to network 140 by any wired and/or wireless means.

[0015] Application server 110 can be any networked computing configuration as long as it is accessible via network 140 by user computers 130 of users 105. For example, personal information management system 100, and more particularly personal information application 112, may support a cloud computing environment. In a cloud computing environment, application server 110 is the cloud server. Further, personal information application 112 is not limited to running on one application server 110 only. Personal information management system 100 may include multiple application servers 110 (or cloud servers) in order to ensure high-availability of computing resources.

[0016] Personal information application 112 is a software application for managing and distributing personal information over a network. For example, personal information application 112 is a software application for managing and distributing information storage 132 of users 105 over network 140. Connections manager 116 of personal information application 112 is a software module for creating and managing connections (or links) between users 105, wherein each user 105 may have connections with one or more other users 105. Further, the connections that are created and managed using connections manager 116 can be between member-users 105 and other member-users 105 or between member-users 105 and guest-users 105. Further, there may be the

possibility of connections between guest-users 105 and other guest-users 105. More details of the connections (or links) between users 105 are described with reference to Figures 5, 6, and 7.

[0017] Notifications manager 118 of personal information application 112 is a software application for managing and notifications on behalf of users 105. For example, when users 105 update information in UICs 128 at data store 114, notifications can be automatically transmitted on behalf of the updating user 105 to other users 105 who are connected to the updating user 105. Further, notifications manager 118 is used to manage notifications based on how each user 105 wishes to receive notifications from other users 105. For example, a certain user 105 may set up his/her notifications to be received daily, weekly, monthly, from individual users 105, from groups of users 105, and the like. Further, a certain user 105 may set up his/her notifications to be received in a certain way, such as via email, SMS, text message, and the like.

[0018] Authentication module 120 of personal information application 112 is used to manage the authentication process of users 105 of personal information management system 100. For example, when the user 105 signs into personal information application 112, a standard authentication process is performed that allows the user 105 to access personal information application 112. User-sign in may occur a number of ways. In one example, the user 105 may use a web browser to access PIA user interface 134 and enter credentials (e.g., username and password). In another example, PIA user interface 134 is a mobile app that user 105 uses to enter his/her credentials. In yet another example, the user sign-in process may occur automatically when the user 105 starts the mobile app.

[0019] Security module 122 of personal information application 112 is used to perform any system security functions with respect to keeping the contents of user data 126 and UICs 128 secure. Security module 122 may use standard security techniques, such as encryption, secure hashtags (or hash tags), and the like.

[0020] Data store 114 can be, for example, data repositories (like databases) and/or flat files that can store data. Further, personal information management system 100 is not limited to one data store 114 only. Personal information management system 100 may include multiple data stores 114. As users 105 join personal information management system 100, user information is stored in user data 126 in data store 114. User data 126 may contain, for example, account information, user names, group names, user/group credentials, and the like.

[0021] UICs 128 in data store 114 are files that contain personal information about users 105. There is a unique UIC 128 for each user 105. Each user can manage the type and amount of personal information in his/her own UIC 128. Each user can manage the portions of the contents of his/her own UIC 128 that he/she wishes to share with any other user 105. Each unique UIC 128 can contain, for example, but is not limited to, the user 105's name, gender, one or more addresses (e.g., home address, work address, summer address), one or more phone numbers (e.g., home phone, work phone, cell phone), one or more email addresses (e.g., home email, work email, any other email), one or more credit card numbers, social security number, one or more bank account numbers, one or more events (e.g., wedding anniversary, birthdays), and the like. Again, information stored in information storage 132 at user computers 130 is static, while updated/dynamic data resides at user data 126 and UICs 128 at data store 114 of personal information application 112. More details of an example of the content of a UIC 128 are shown and described with reference to Figures 2, 3A, and 3B.

[0022] Figure 2 illustrates a block diagram of an example of a UIC 128 of personal information management system 100 of Figure 1. Each unique UIC 128 stored in user data 126 includes, for example, one or more UIC elements 142, wherein each UIC element 142 can include one or more UIC element objects 144. Each UIC element 142 in UIC 128 contains a different type of information about the user 105. For example, one UIC element 142 contains the user 105's name (a name-UIC element 142), another UIC element 142 contains the user 105's gender (a gender-UIC element 142), yet another UIC element 142 contains the user 105's address information (an address-UIC element 142). In like manner, UIC elements 142 can include a phone-UIC element 142, an email-UIC element 142, a payment-UIC element 142, an event-UIC element 142, and the like.

[0023] Again, one UIC element 142 can include one or more UIC element objects 144. A UIC element object 144 is one record of information. For example, if a user 105 has three phone numbers, the phone-UIC element 142 will include three UIC element objects 144. For example, a first UIC element object 144 in the phone-UIC element 142 contains a home number, a second UIC element object 144 in the phone-UIC element 142 contains a work number, and a third UIC element object 144 in the phone-UIC element 142 contains a cell number. In another example, a first UIC element object 144 in the address-UIC element 142 contains a home address and a second UIC element object 144 in the address-UIC element 142 contains a work address.

[0024] Figures 3A and 3B show one example of coding UIC elements 142 and UIC element objects 144 in a UIC 128. In this example, the UIC 128 is coded using JavaScript Object Notation (JSON). However, this is exemplary only. UIC 128 can be coded in other ways, such as in XML format. Figures 3A and 3B show that the code for UIC 128 includes, for example, a PIA-UIC element 142 with one UIC element object 144, a name-UIC element 142 with one UIC element object 144, a gender-UIC element 142 with one UIC element object 144, an event-UIC element 142 with one UIC element object 144, an address-UIC element 142 with one UIC element object 144, an email-UIC element 142 with two UIC element objects 144, a phone-UIC element 142 with two UIC element objects 144, and payment-UIC element 142 with one UIC element object 144.

[0025] PIA-UIC element 142 is an UIC element 142 that provides reference to the personal information application 112 itself. The UIC element object 144 of PIA-UIC element 142 includes attributes, such as “network_country,” “network_id,” and “connect_id.” The “connect_id” attribute is, for example, the user 105A-CONNECTION ID that is referenced below in Figures 5, 6, and 7.

[0026] The “network_country” and “network_id” attributes exist to allow a user 105 to specify where they want their master UIC 128 to be located. For example, if a certain user 105 is a U.S. citizen, this user 105 may prefer his/her UIC 128 to be stored in the United States. However, if a certain user 105 is a citizen of Sweden, this user 105 may prefer his/her UIC 128 to be stored in Sweden. In another scenario, if personal information management system 100 allows “mini” servers to run on a personal device like a user 105’s phone or iPad (a user computer 130), then the phone or iPad becomes a server that is part of the personal information management system 100-network. In this case, that user 105’s phone or iPad also becomes their master UIC 128 data store. Therefore, while Figure 1 shows personal information application 112 residing at application server 110, it is possible for personal information application 112 to be running on any computing device that is connected to the network 140. For example, personal information application 112 can be running on one or more of user computers 130.

[0027] Note that UIC 128 can include metadata. For example, there is a “metadata” field in address-UIC element 142 and in phone-UIC element 142. Further, certain information in UIC 128 can be verified by the user 105. For example, there is an “object verified” field in address-UIC element 142, email-UIC element 142, phone-UIC element 142, and payment-UIC element 142.

Absence of the “object verified” field indicates that the information in the UIC element object 144 is not verified.

[0028] Referring again to Figure 2, optionally, UIC 128 can include a UIC attribute 146, which can contain additional data about the UIC 128, such as metadata. Optionally, a UIC element object 144 can include an element object attribute 148, which can be, for example, key/value pairs, such as metadata, object_verified, phone_number, etc. Additionally, UIC 128 can include a link to a photo or to any other file of the user 105 using a photo-UIC element 142. Namely, instead of embedding an actual digital photo in a UIC 128, which can make the UIC 128 very large and consume large amounts of data store 114, the UIC element object 144 of the photo-UIC element 142 in UIC 128 can include a link or path to a remote (separate) secure data store (not shown) in which the digital photo is stored. In this way, when the user 105 changes his/her photo, the new photo is automatically referenced.

[0029] Figure 4 illustrates another block diagram of personal information management system 100 for managing and distributing personal information between, for example, two users. In this example, a user 105A and a user 105B are associated with personal information management system 100, wherein user 105A is a member-user 105 and user 105B can be either a member-user 105 or a guest-user 105. Figures 5, 6, and 7 to follow describe examples of connections (or links) that are possible between user 105A and user 105B in personal information management system 100.

[0030] Figure 5 illustrates a schematic diagram of the communication links between two users of personal information management system 100 of Figure 1, according to a minimum configuration. In this example, user 105A is a member-user 105 and user 105B can be either a member-user 105 or a guest-user 105. Connections manager 116 of personal information application 112 manages the process of establishing links between any two users 105.

[0031] First, user 105A establishes a relationship with user 105B by, for example, adding an individual or any entity to his/her contacts list in personal information application 112. In so doing, a connection or link is created between user 105A and user 105B, which is shown as user 105B-CONNECTION ID. With respect to user 105B-CONNECTION ID, user 105B is the “connection” and user 105A is the “connector.” This means that user 105B manages the user 105B-CONNECTION ID and that user 105A is connected to the user 105B-CONNECTION ID.

[0032] Next, when user 105A initiates the relationship with user 105B, a connection is automatically created for user 105B to user 105A. At first, this connection is flagged as “pending.” For example, a connection or link is automatically created between user 105B and user 105A, which is shown as user 105A-CONNECTION ID. With respect to user 105A-CONNECTION ID, user 105B is the “connector” and user 105A is the “connection.” This means that user 105A manages the user 105A-CONNECTION ID and that user 105B is connected to the user 105A-CONNECTION ID.

[0033] User 105A-CONNECTION ID and user 105B-CONNECTION ID are unique connection identifiers between the two entities, user 105A and user 105B. There will always be a CONNECTION ID for each user 105. The CONNECTION IDs are stored in user data 126 and in UICs 128 at data store 114. User 105A-CONNECTION ID belonging to user 105A is specific for user 105B. The user 105A-CONNECTION ID is used to push information from user 105A to user 105B. Similarly, user 105B-CONNECTION ID belonging to user 105B is specific for user 105A. The user 105B-CONNECTION ID is used to push information from user 105B to user 105A. For example, if between user 105A wants to connect to another user 105 (e.g., a user 105C, not shown), a different user 105A-CONNECTION ID is created that is specific for user 105C.

[0034] The user 105B-CONNECTION ID and the user 105A-CONNECTION ID are created regardless of whether user 105B is a member-user 105 or a guest-user 105. Even if user 105B is a temporary guest-user 105 on the network, user 105A can share his/her personal information with user 105B. However, if user 105B is a guest-user 105, user 105B may not be able to share his/her personal information with user 105A. Even so, a link (i.e., user 105B-CONNECTION ID) has been established and retained for user 105B. Therefore, if user 105B decides later to join personal information management system 100, then the link is already present. If user 105B is a member-user 105, then user 105B will be able to share user 105B-CONNECTION ID with user 105A. However, if user 105B is a guest-user 105, then user 105B may not be able to share user 105B-CONNECTION ID with user 105A. Referring again to Figure 5, at the point an outer connection loop is created in which the direction of information flow is clockwise (CW).

[0035] Next, an inner connection loop is shown in which the direction of information flow is counter-clockwise (CCW). For example, now that user 105A has created the first connection process (the outer loop), user 105A can share his/her personal information with user 105B. Namely, with respect to user 105A-CONNECTION ID, user 105A is the “conductor” and user

105B is the “recipient.” This means that for any information that is shared through user 105A-CONNECTION ID, user 105A is the conductor of that information and user 105B is the recipient of that information. In like manner, with respect to user 105B-CONNECTION ID, user 105B is the “conductor” and user 105A is the “recipient.” This means that for any information that is shared through user 105B-CONNECTION ID, user 105B is the conductor of that information and user 105A is the recipient of that information.

[0036] The aforementioned flow allows user 105B, who may not be a member-user 105, to receive user 105A’s information even though user 105B is not a member-user 105. This allows pragmatic guest-users 105 to take their time to decide whether to join personal information management system 100. However, user 105B (a guest-user 105) still benefits from the network. For example, if user 105A (a member-user 105) updates his/her personal information, a secure URL that is specific only to user 105A and user 105B is used to send user 105A’s information to user 105B. User 105A (the “conductor”) is sharing information with user 105B (the “recipient”). This allows user 105B to have a secure URL that will never change unless guest-user 105 becomes a member. At that time, the secure URL will cease to exist, instead requiring the now member-user 105 to login/authenticate to personal information application 112. The same link is used no matter how many times user 105B views the link or no matter how many times user 105A has updated his/her information. The secure URL allows user 105B to view only what user 105A is sharing with user 105B. That is, user 105A controls what information he/she wants to share with any other entity, such as user 105B, as described with reference to Figure 6.

[0037] Figure 6 illustrates a schematic diagram of the communication links between two users of personal information management system 100 of Figure 1, according to an expanded configuration. In this example, user 105A is a member-user 105 and user 105B is also a member-user 105. Two additional features of personal information management system 100 are shown in Figures 6—CUSTOM IDs and GROUPS. The overall purpose of CUSTOM IDs is to manage personal information of a certain user 105 that may be stored by another user 105 in multiple places. The overall purpose of GROUPS is to manage privacy settings.

[0038] User 105A may have personal information about user 105B stored in several places (i.e., stored in different instances of information storage 132 on one or more of his/her user computers 130). For example, user 105A may have personal information about user 105B stored in his/her phone contacts, email contact, and if a business also in a CRM system. Therefore, user

105A is provided a user 105A-CUSTOM ID that references (points to) these different instances of information storage 132 to the user 105B-CONNECTION ID of user 105B, which is an ID that is specific to personal information management system 100. For example, if user 105A is a business entity, there may be personal information about user 105B storing in both the billing database and the customer service database. Accordingly, user 105A-CUSTOM ID allows the business entity to correlate user 105B-CONNECTION ID to customer #1989Y73, which is user 105B, in both databases.

[0039] In similar fashion, user 105B is provided a user 105B-CUSTOM ID that points these different instances of information storage 132 to the user 105A-CONNECTION ID of user 105A. Another feature of CUSTOM IDs is that if, for example, the record of the user 105B-CONNECTION ID for user 105B is lost, then user 105A can query his/her user 105A-CUSTOM ID and look up the user 105B-CONNECTION ID of user 105B.

[0040] The CUSTOM ID can be any string of numbers and/or characters. In one example, the CUSTOM ID can be a sensitive ID, such as social security number, a credit card number, a bank account number, a healthcare record number, a customer number, and the like. Because the CUSTOM ID can be a sensitive ID, security module 122 applies certain security measures to CUSTOM IDs. For example, the CUSTOM ID is not stored in plain text. Instead, the CUSTOM ID is converted into a secure hash that cannot be reversed.

[0041] As shown and described in Figures 2, 3A, and 3B, the UIC 128 for any user 105 can include multiple types of personal information, such as, but not limited to, gender information, address information, phone information, email information, credit card information, a social security number, bank account information, events information, and the like. However, a user 105 may wish to limit the types and amount of personal information they wish to share with any other member-user 105 or guest-user 105. One user 105 could apply privacy settings to each of the other users 105 individually, but this would be time consuming. Instead, a user 105 can create one or more groups, then apply privacy settings to each group, then assign other users 105 to which he/she is connected to a particular group.

[0042] For example, a user 105 can create a FAMILY GROUP, a FRIENDS GROUP, and a CHARITY GROUP, wherein each GROUP contains at least one user 105. The privacy settings for FAMILY GROUP allow the user 105's name, home phone, work phone, cell phone, personal email, work email, home address, work address, and events to be viewed by those other users 105

that are assigned to this group. The privacy settings for FRIENDS GROUP allow the user 105's name, home phone, cell phone, personal email, and home address to be viewed by those other users 105 that are assigned to this group. The privacy settings for CHARITY GROUP allow the user 105's name, cell phone, personal email, and credit card number to be viewed by those other users 105 that are assigned to this group.

[0043] Accordingly, Figure 6 shows that the user 105A-CONNECTION ID of user 105A is assigned to a certain GROUP ID and that the user 105B-CONNECTION ID of user 105B is assigned to a certain GROUP ID.

[0044] Figure 7 illustrates a schematic diagram of the communication links between two users of personal information management system 100 of Figure 1, according to yet another configuration. In this example, user 105A is a member-user 105 and user 105B is a guest-user 105. Because user 105B is a guest-user 105 and does not have access to personal information application 112, user 105B cannot assign user 105A to a GROUP and there can be no CUSTOM ID for user 105B. Further, even though user 105B is a guest-user 105, personal information application 112 can create and then store a temporary UIC 128, or at least an email record or any other information, for the guest-users 105 in data store 114.

[0045] Figures 8A and 8B illustrate a flow diagram of an example of a method 800 of establishing the communication links between two users 105 in personal information management system 100 of Figure 1. Method 800 may include, but is not limited to, the following steps.

[0046] At a step 810, a member-user 105 (e.g., person or organization) initiates a connection with another entity (e.g., person or organization) who may or may not be a member-user 105. In one example and referring again to Figures 4, 5, 6, and 7, using PIA user interface 134, user 105A initiates a connection with another entity, such as user 105B, by, for example, adding user 105B to his/her contacts list in personal information application 112. User 105B may be a member-user 105 or a guest-user 105. By initiating a connection, connections manager 116 of personal information application 112 creates the user 105A-CONNECTION ID between user 105A and user 105B. Method 800 proceeds to step 812.

[0047] At an optional step 812, the initiating member-user 105 provides a CUSTOM ID to the other entity. The initiating member-user 105 can manually create the CUSTOM ID or personal information application 112 can automatically generate the CUSTOM ID. For security, once the

CUSTOM ID is created or generated, security module 122 can be used to convert the CUSTOM ID into a secure hash that cannot be reversed. Continuing the example, user 105A provides a CUSTOM ID to user 105B. This step is optional because the initiating user 105A may or may not intend to store user 105B's information in multiple places. Further, this step is optional because the function of CUSTOM IDs can be omitted altogether in personal information management system 100. Method 800 proceeds to step 814.

[0048] At a step 814, personal information application 112 searches for personal information of other entity, namely, personal information application 112 searches user data 126 and/or UICs 128 in data store 114. Continuing the example, personal information application 112 searches user data 126 and/or UICs 128 in data store 114 for personal information (e.g., name, email, phone, address, credit card number, etc) about user 105B, who may be a member-user 105 or a guest-user 105. Method 800 proceeds to step 816.

[0049] At a decision step 816, based on the search performed in step 814, personal information application 112 determines whether personal information of other entity is present. Continuing the example, personal information application 112 determines whether personal information (e.g., name, email, phone, address, credit card number, etc) about user 105B is present in user data 126 and/or UICs 128 in data store 114. If information is not present, then method 800 proceeds to step 818. However, if information is present, then method 800 proceeds to step 820.

[0050] At an optional step 818, the personal information of the other entity is added to data store 114. Continuing the example, the personal information (e.g., name, email, phone, address, credit card number, etc) about user 105B that is provided by user 105A in step 810 is added to user data 126 and/or UICs 128 in data store 114. Method 800 proceeds to step 820.

[0051] At a decision step 820, personal information application 112 determines whether the information is linked to a member-user 105. Continuing the example, personal information application 112 determines whether the information is linked to a member-user 105; namely, whether user 105B is a member-user 105. For example, the information found in step 814 will indicate whether user 105B is a member-user 105. If the information is linked to a member-user 105; namely, if user 105B is a member-user 105, then method 800 proceeds to step 822. However, if the information is not linked to a member-user 105; namely, if user 105B is a guest-user 105, then method 800 proceeds to step 828.

[0052] At a decision step 822, personal information application 112 determines whether a member connection already exists. Continuing the example, connections manager 116 of personal information application 112 queries the network to determine whether user 105B-CONNECTION ID (in the form of a member connection) already exists between user 105A and user 105B. If there is an existing member connection, then method 800 proceeds to step 824. However, if there is not an existing member connection, then method 800 proceeds to step 826.

[0053] At an optional step 824, the CUSTOM ID, if provided in step 812, is processed. Continuing the example, the CUSTOM ID of user 105A is associated with the user 105B-CONNECTION ID regardless of whether user 105B-CONNECTION ID is a guest or member connection. Method 800 ends.

[0054] At step 826, the member connection is added and the CUSTOM ID, if provided in step 812, is processed. Continuing the example, connections manager 116 of personal information application 112 creates the user 105B-CONNECTION ID between user 105A and user 105B. The CUSTOM ID of user 105A, if provided in step 812, is associated with the user 105B-CONNECTION ID. Method 800 ends.

[0055] At a decision step 828, personal information application 112 determines whether a guest connection already exists. Continuing the example, connections manager 116 of personal information application 112 queries the network to determine whether user 105B-CONNECTION ID (in the form of a guest connection) already exists between user 105A and user 105B. If there is an existing guest connection, then method 800 proceeds to step 824. However, if there is not an existing guest connection, then method 800 proceeds to step 830.

[0056] At a step 830, personal information application 112 adds a guest connection and the CUSTOM ID, if provided in step 812, is processed. Continuing the example, connections manager 116 of personal information application 112 creates user 105B-CONNECTION ID (in the form of a guest connection) between user 105A and user 105B. The CUSTOM ID of user 105A, if provided in step 812, is associated with the user 105B-CONNECTION ID. Method 800 proceeds to step 832.

[0057] At a step 832, an invitation is created and transmitted to the guest entity. Continuing the example, an invitation is created and transmitted to user 105B. For example, notifications manager 118 generates a notification (e.g., email, SMS, text message) and transmits the

notification to user 105B. Once the notification is received, user 105B can choose whether to accept the connection or reject the connection. The contents of the notification can include, for example, a secure URL that user 105B can use to accept the connection and to view user 105A's personal information. The connection is in a pending state until user 105B accepts the connection. Further, the notification to user 105B can include an invitation to join personal information management system 100 and become a member-user 105. Method 800 proceeds to step 834.

[0058] At a step 834, the guest entity opens and views the invitation. Continuing the example, user 105B opens and views the invitation. Method 800 proceeds to step 836.

[0059] At a decision step 836, the guest entity decides whether to join personal information management system 100 and become a member-user 105 or to remain a guest-user 105. Continuing the example, user 105B decides whether to join personal information management system 100 and become a member-user 105 or to remain a guest-user 105. If the guest-user 105 wishes to join personal information management system 100, then method 800 proceeds to step 838. However, if the guest-user 105 does not wish to join personal information management system 100, then method 800 ends.

[0060] At a step 838, the guest entity signs up for membership to personal information management system 100. Continuing the example, user 105B signs up for membership to personal information management system 100. Method 800 proceeds to step 840.

[0061] At a step 840, personal information management system 100 processes any invitations and requests for the new member and creates the member connections. Continuing the example, personal information management system 100 processes any invitations and requests for user 105B, who is now a member-user 105, and creates user 105B's member connections with other users 105. Method 800 ends.

[0062] Figure 9 illustrates a flow diagram of an example of a method 900 of automatically distributing personal information using personal information management system 100 of Figure 1. Generally, personal information application 112, processing updates of UICs 128 can be, for example, automatic via "push" (versus polling/pulls), i.e., personal information application 112 automatically pushes the update to the receiving entity without having to wait for the entity to "poll" for updates. Method 900 may include, but is not limited to, the following steps.

[0063] At a step 910, a member-user 105 updates any portion of his/her personal information in his/her UIC 128. For example, the member-user 105 uses PIA user interface 134 to update information in any UIC element object 144 of any UIC element 142 in his/her UIC 128. For any UIC element object 144 that is updated, the modification date in the UIC element object 144 is changed and the version of the UIC element object 144 is changed. The updated UIC 128 is stored in data store 114. Note that “object_modified” is a key/value pair, which is an example of an element object attribute 148. Also, “version” is an example of an element object attribute 148.

[0064] At a step 912, in data store 114, the portion or portions of the UIC 128 of the member-user 105 that are updated are flagged as being modified. For example, if the member-user 105 changes one of his/her phone numbers, then the information in one UIC element object 144 of the phone-UIC element 142 is updated. As a result, this UIC element object 144 of the phone-UIC element 142 is flagged as being modified.

[0065] At a step 914, notifications manager 118 continuously polls UICs 128 in data store 114 for flagged information and generates and queues notifications of updates to the intended recipient-user 105 (i.e., to all the user connections). The recipients can include both member-users 105 and guest-users 105. For guest-users 105, the contents of notifications can include, for example, a secure URL to view the updated personal information, whereas member-users 105 can simply access personal information application 112.

[0066] At a step 916, notifications manager 118 delivers the notifications of updates according to user preferences. For example, a certain user 105 may set up his/her notifications to be automatically received daily, weekly, monthly, from individual users 105, from groups of users 105, and the like. Additionally, a user 105 can specify to receive no notifications, as they prefer to check for updates manually at their discretion. Further, a certain user 105 may set up his/her notifications to be received in a certain way, such as via email, SMS, text message, and the like. Further, personal information updates can be compiled into a compressed file, as specified by the member-users 105, that can be downloaded and processed at the discretion of the member-users 105. For example, member-users 105 can specify the contents of the compressed file to include only UICs 128 that have been updated in the last month, to include only updated portions not the entirety, to include specified portions only, such as updated phones and emails only, and so on.

[0067] Additionally, notifications manager 118 delivers the notifications of updates according to any other rules in personal information management system 100. For example, notifications are

not necessarily sent out in real time as updates occur. Instead, notifications may be delayed slightly.

[0068] At a step 918, recipient users 105 receive and view notifications of updates. For example, guest-users 105 may receive notifications via email, SMS, or text message, whereas member-users 105 can simply access personal information application 112 to receive the notifications.

[0069] At a step 920, recipient users 105 view and store the personal information updates. For example, recipient users 105 view and store the personal information updates in their respective information storage 132.

[0070] In summary and referring again to Figures 1 through 9, personal information management system 100 and methods 800 and 900 provide mechanisms by which users 105 can update their personal information in one place and then the updated information is automatically distributed to other users 105. Further, the personal information management system 100 includes mechanisms by which users 105 can manage what portion or portions of their personal information is shared with other users 105, wherein the personal information shared with one recipient can be different than the personal information shared with another recipient. The personal information management system 100 disclosed herein provides benefit over conventional manual methods of distributing updated personal information in that it is capable of automatically distributing updated personal information to any entities with which a user 105 has a relationship. Further, the connection between one user 105 and another user 105 persists indefinitely over time so that updated personal information can be distributed without the user 105 having to remember every entity with which he/she has a relationship over a period of time.

ABSTRACT OF THE DISCLOSURE:

A personal information management system for and methods of managing and distributing personal information over a network is disclosed. The personal information management includes a personal information application and a data store for storing user data and user information containers (UICs), wherein personal information of users' is logged in the UICs. A method of automatically distributing personal information using the personal information management system includes the steps of the user updating any portion of his/her personal information, flagging the updated portion or portions of UICs as being modified, polling the data store for flagged

information in UICs, generating and queuing notifications of updates, delivering notifications of updates according to user preferences and/or any other rules, recipient users receiving and viewing notifications of updates, recipient users viewing and storing updates to personal information.

Personal information

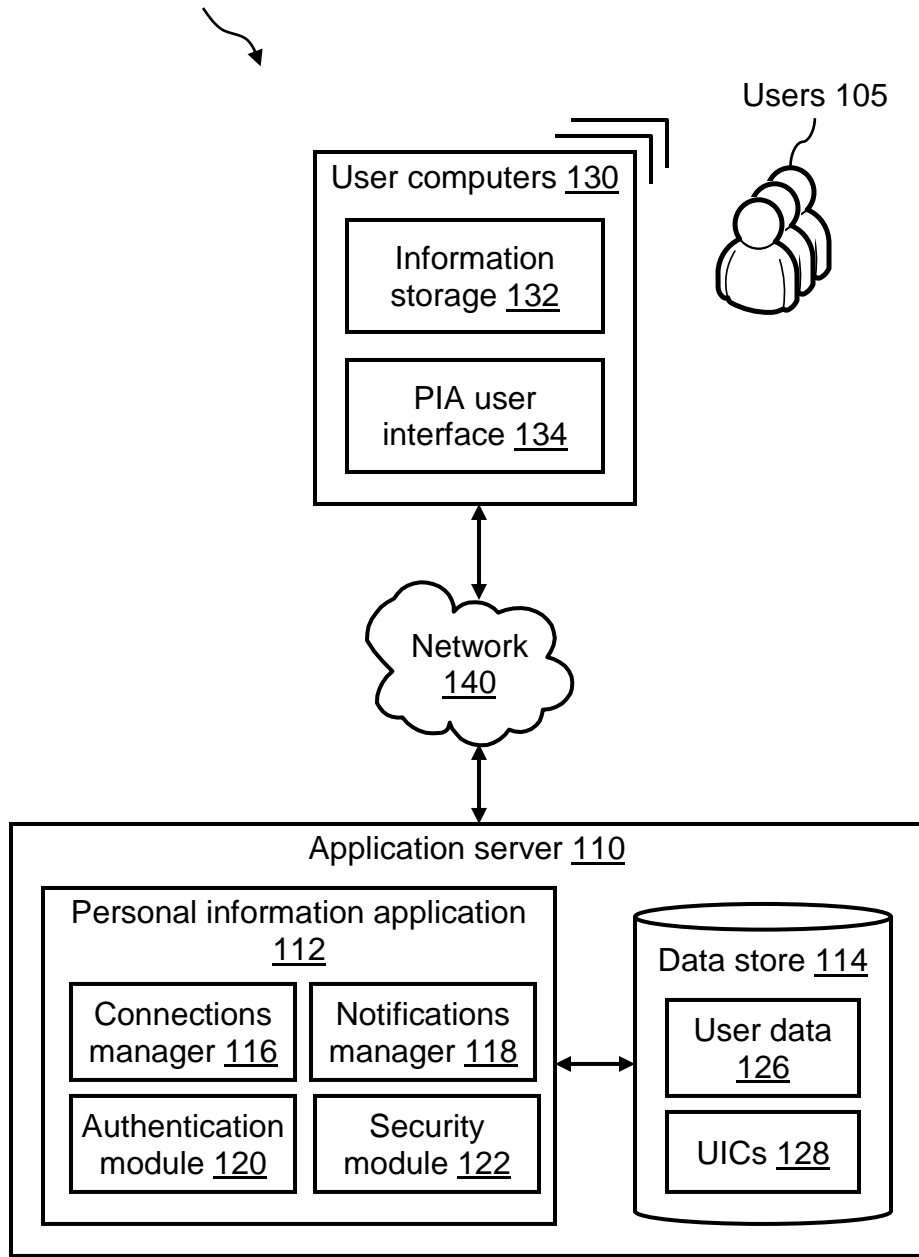


FIG. 1

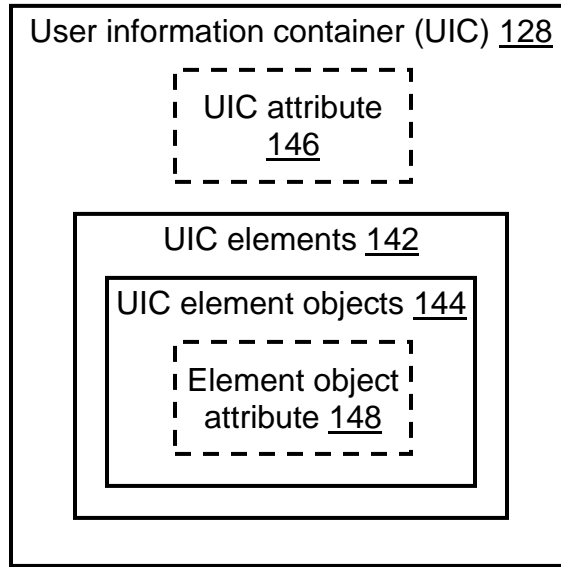


FIG. 2

UIC 128

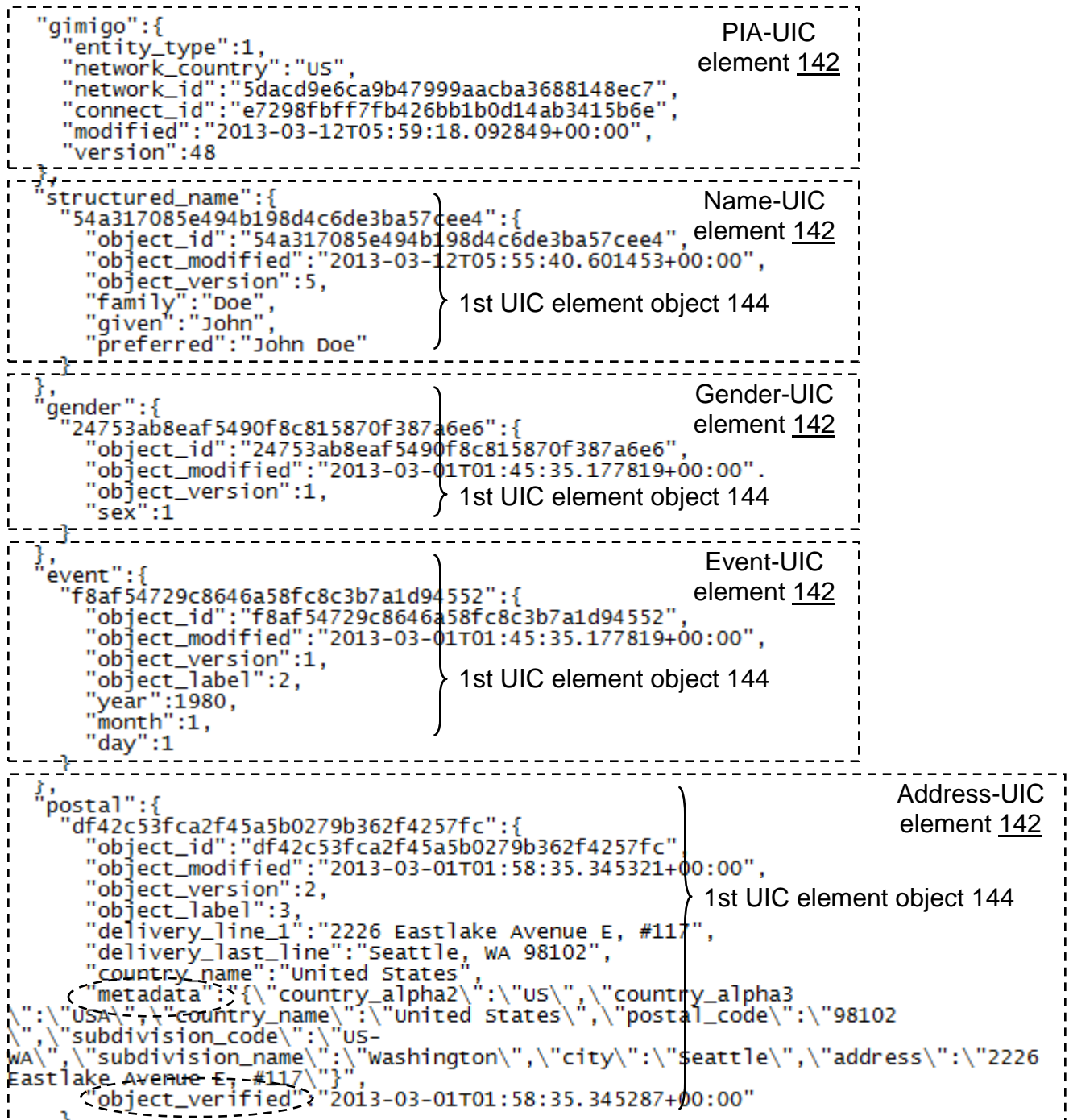


FIG. 3A

UIC 128

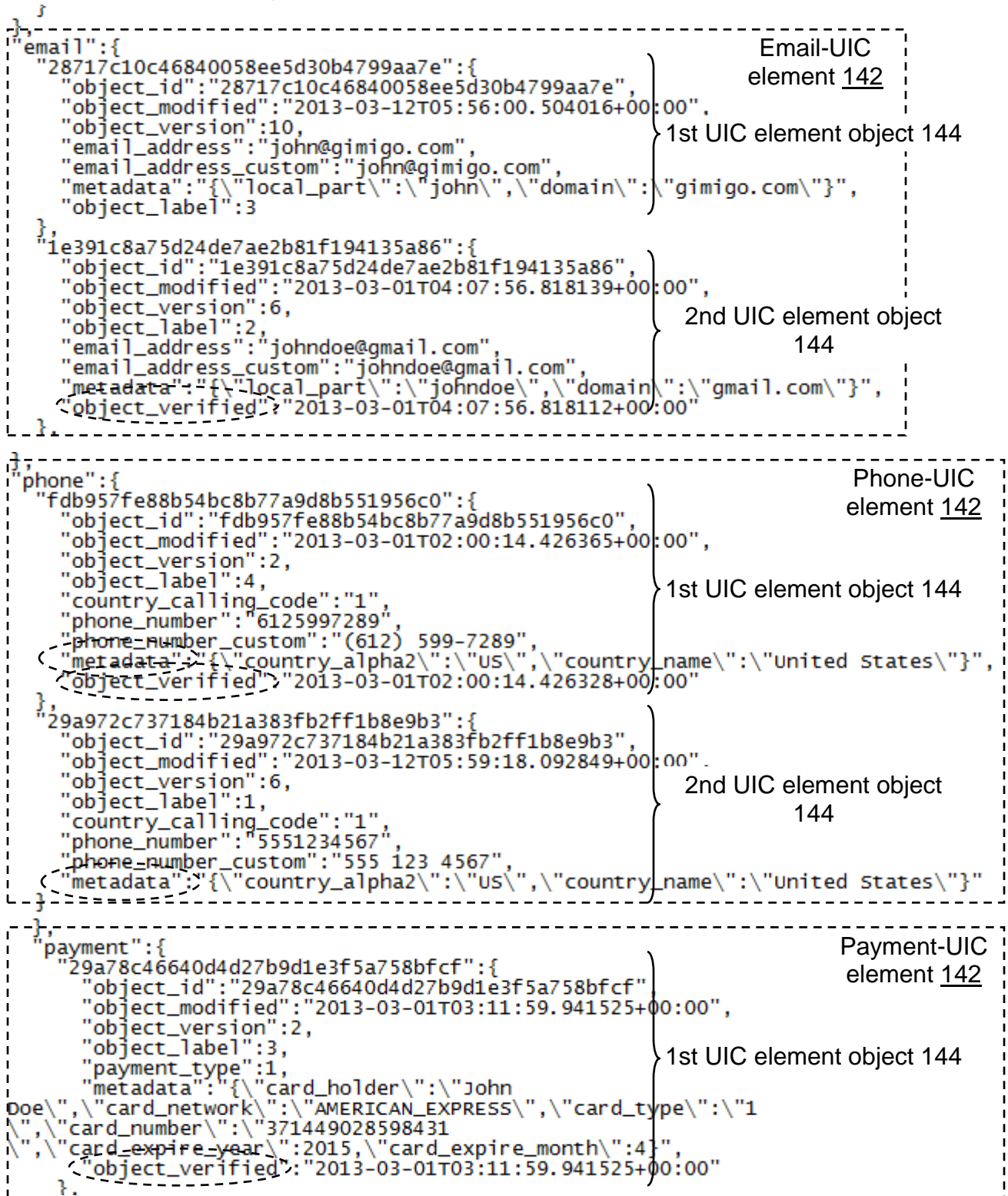


FIG. 3B

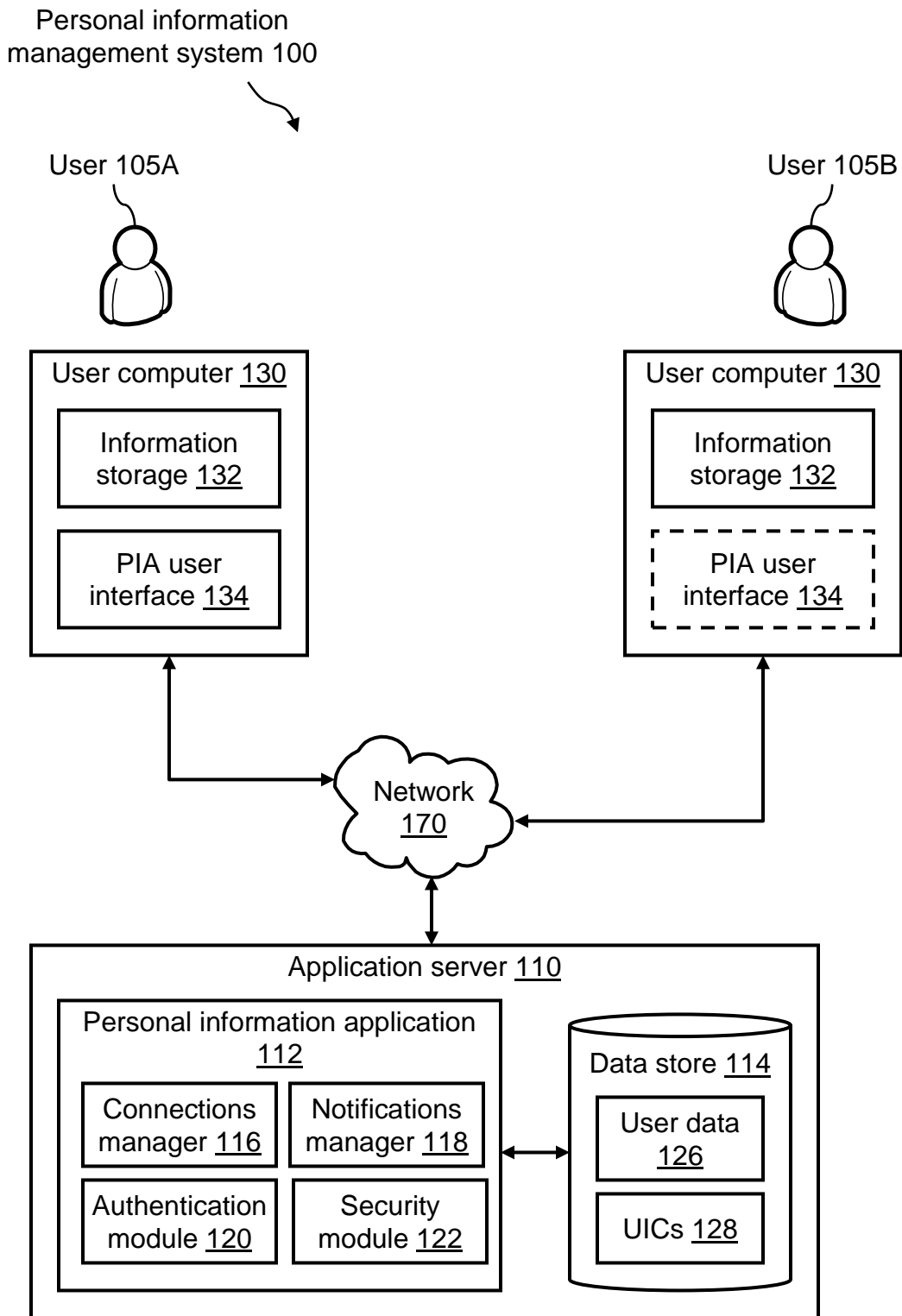


FIG. 4

Personal information management system 100

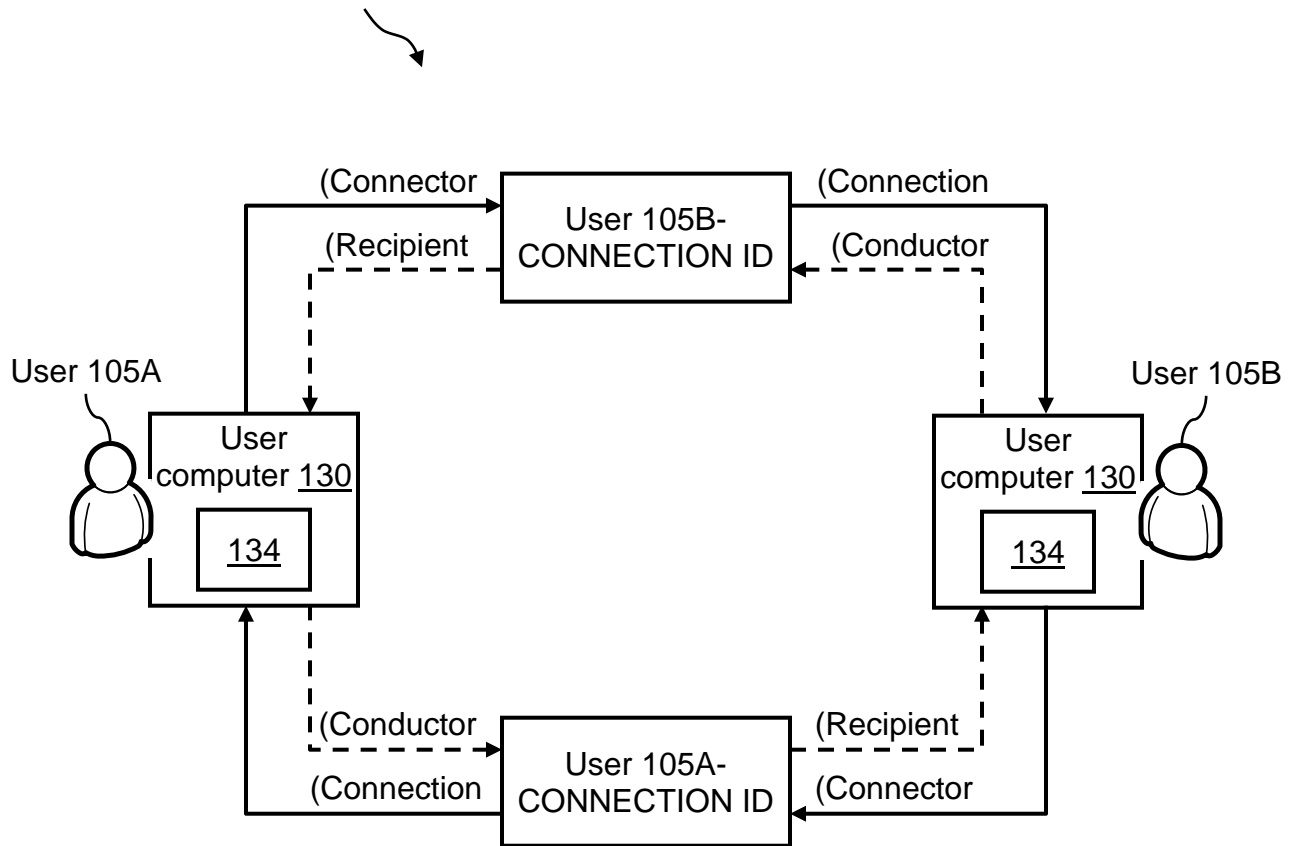


FIG. 5

Personal information management system 100

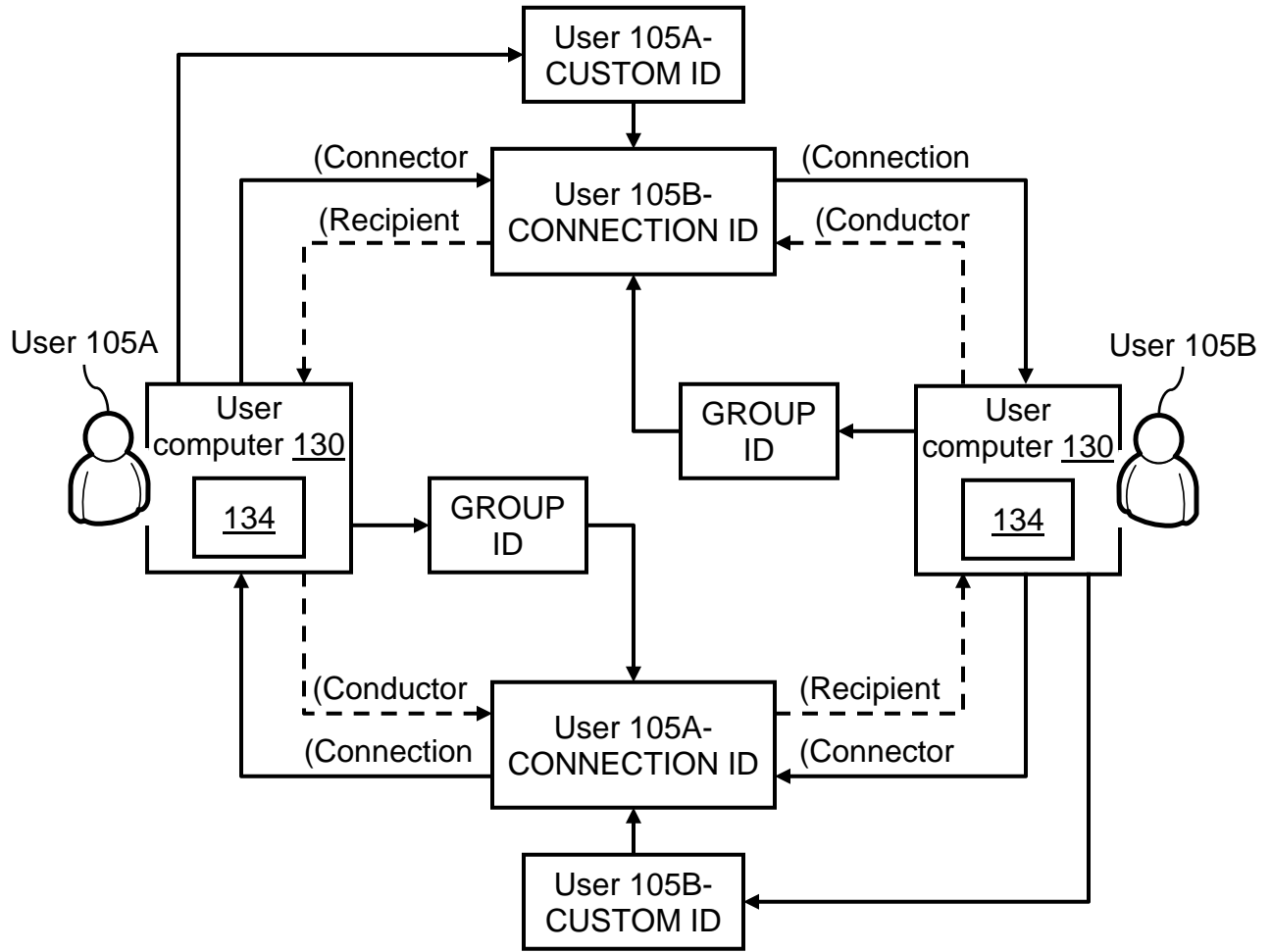


FIG. 6

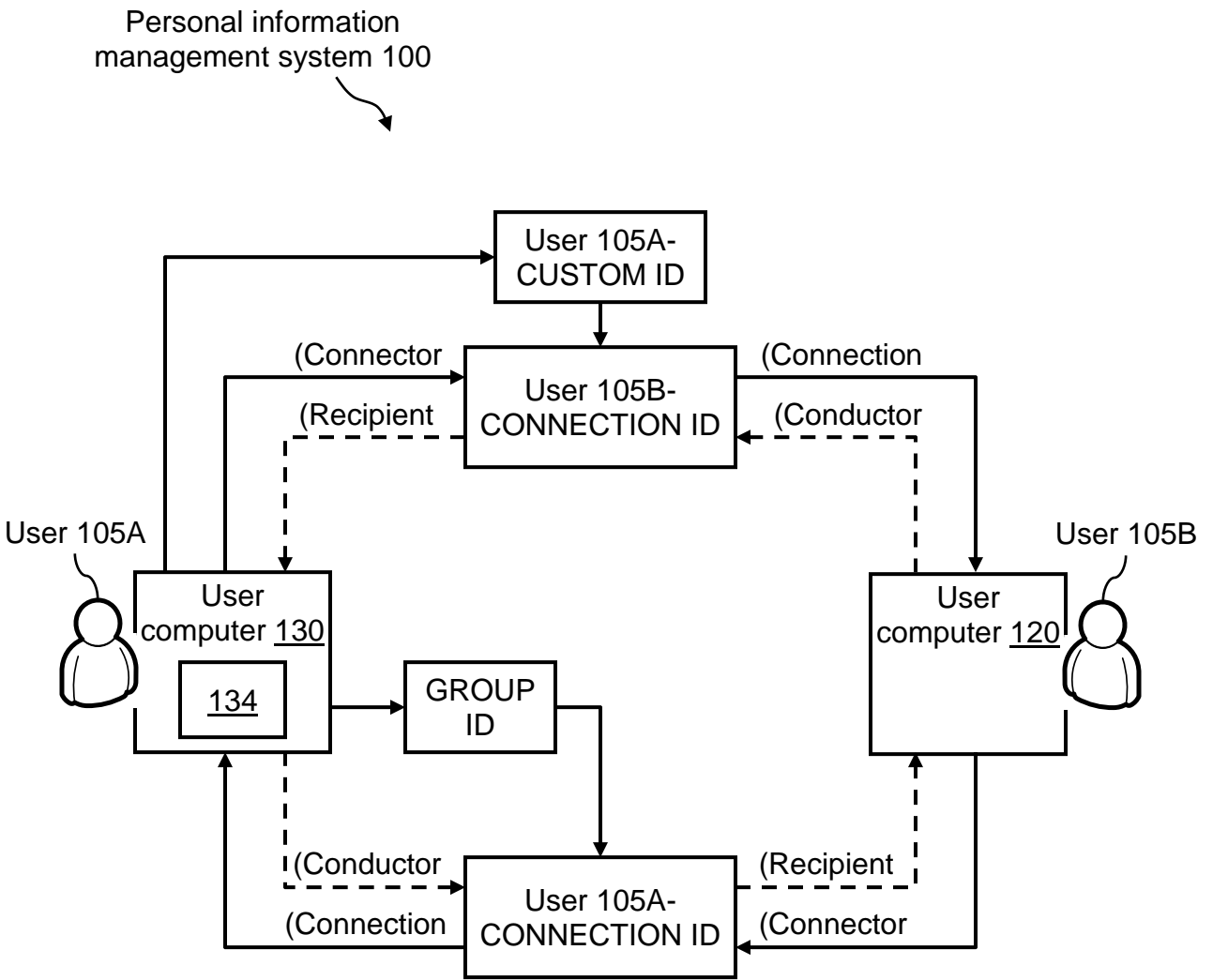
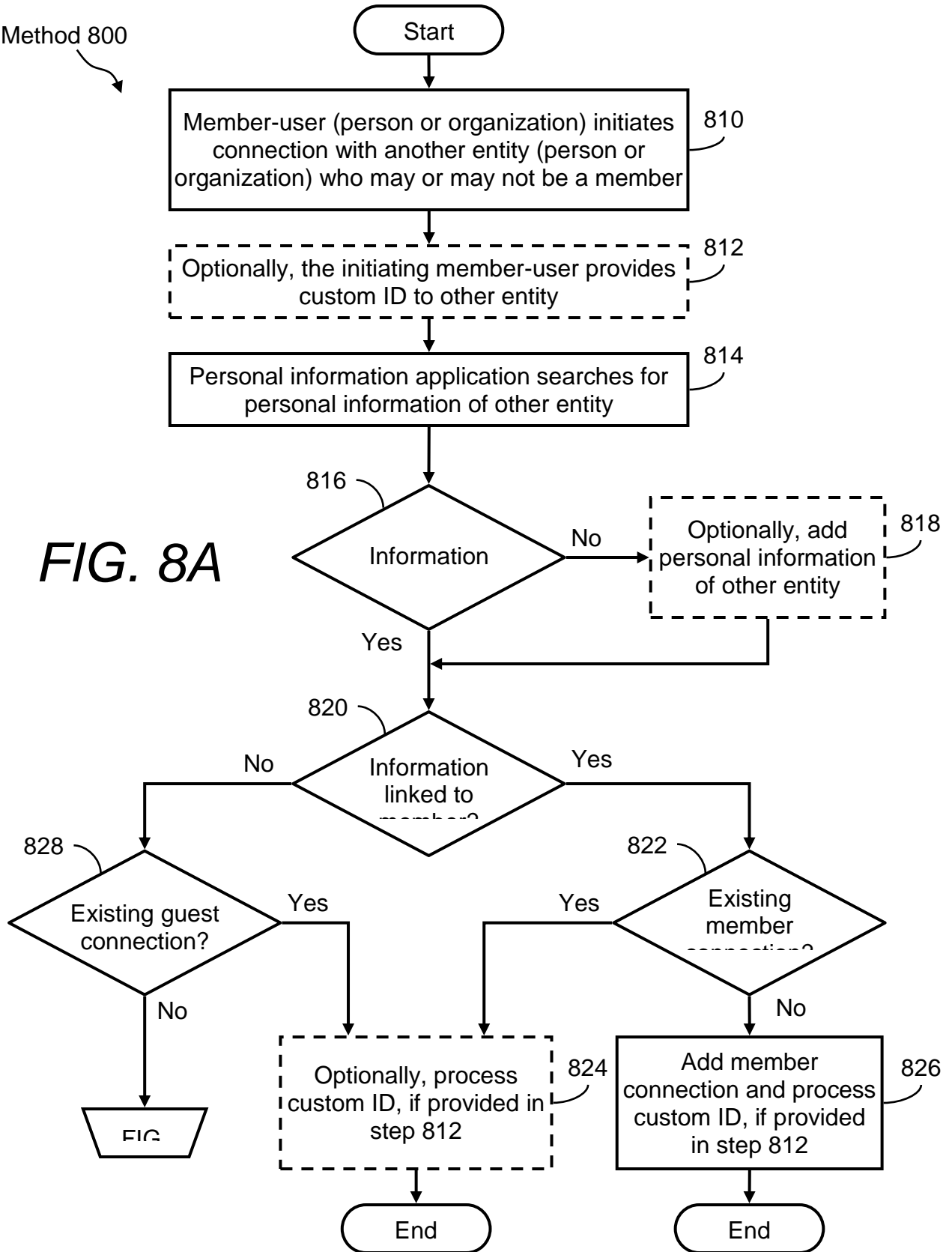
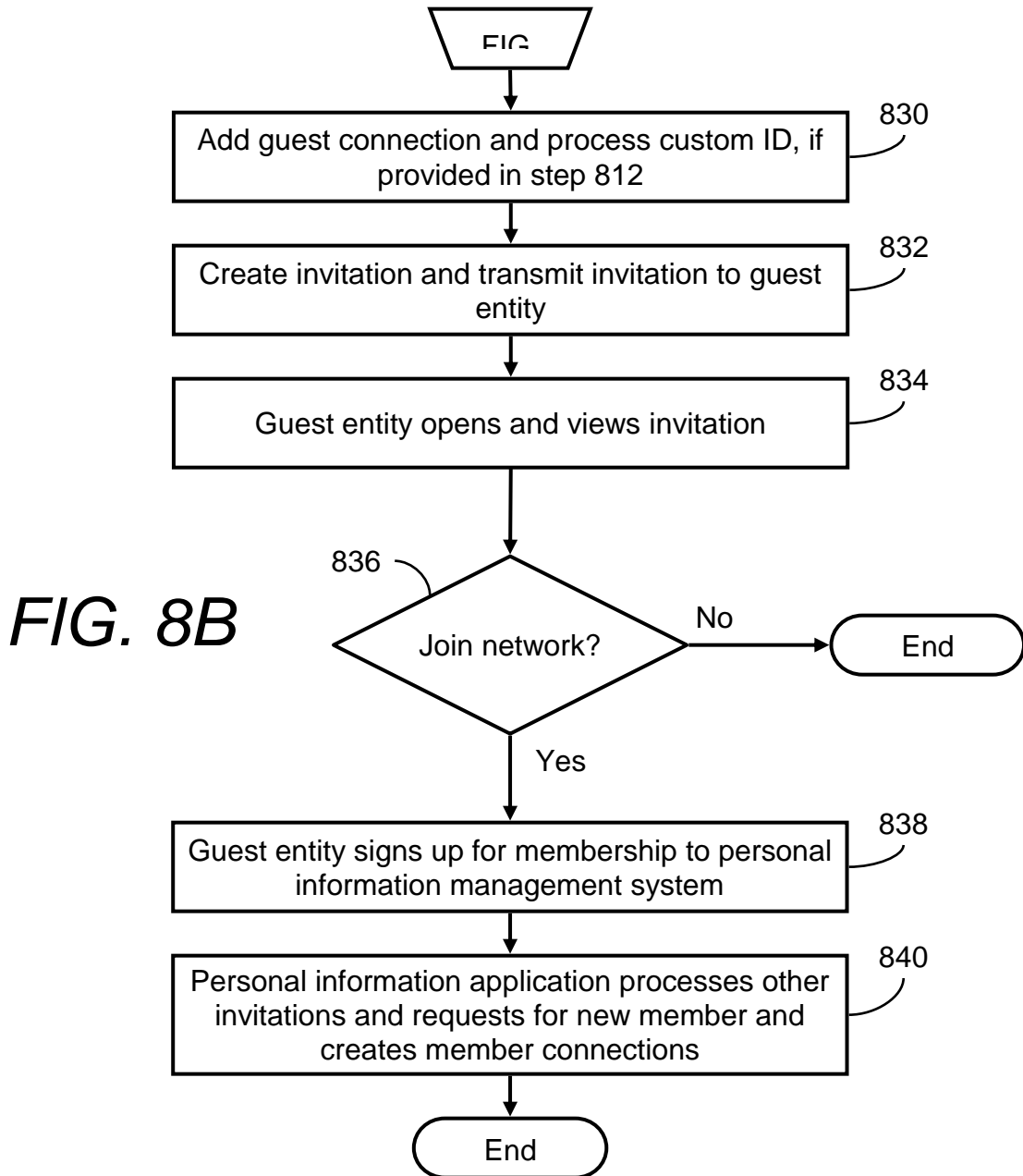


FIG. 7

Method 800



Method 800 (continued)



Method 900

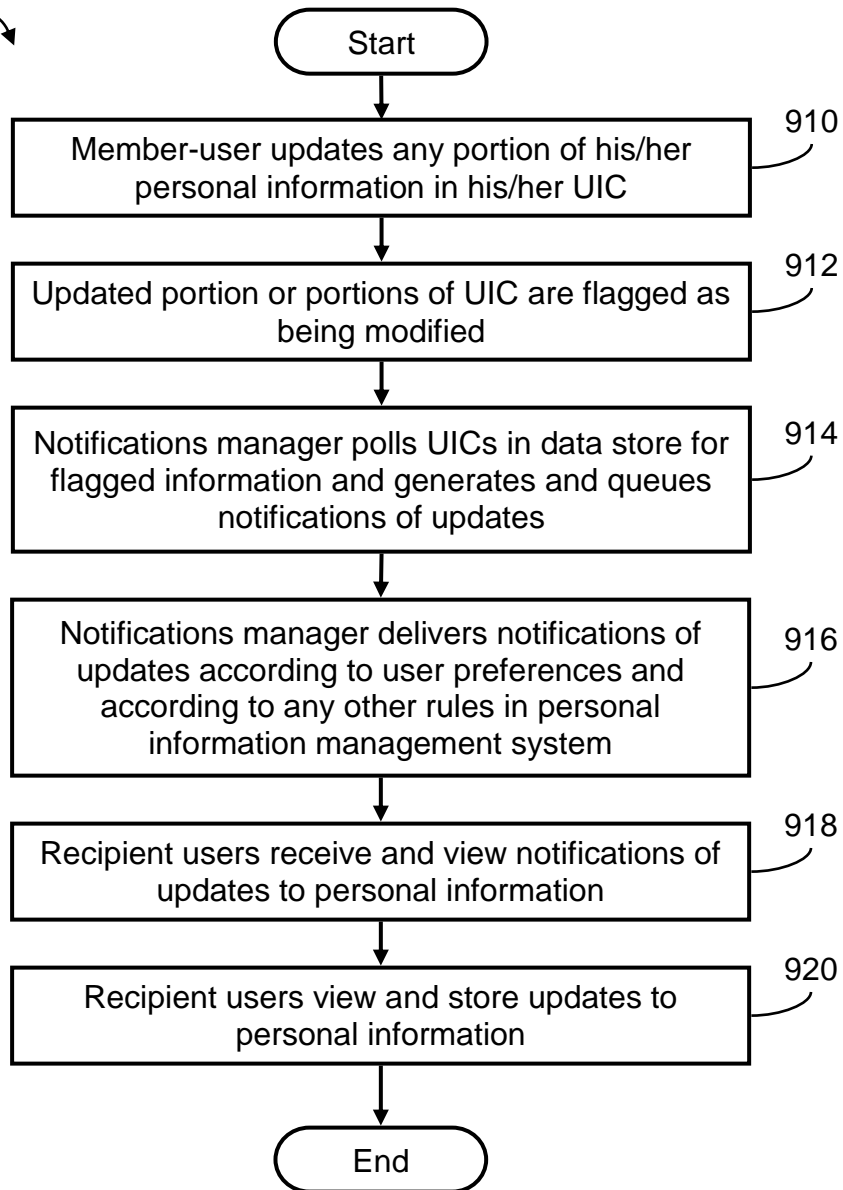


FIG. 9