

(10) International Publication Number
WO 2014/197323 A1(43) International Publication Date
11 December 2014 (11.12.2014)

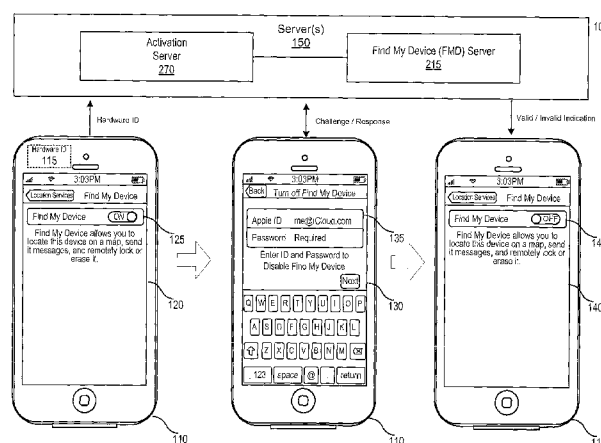
- (51) **International Patent Classification:**
G06F 9/445 (2006.01) *G06F 21/88* (2013.01)
- (21) **International Application Number:**
PCT/US2014/040275
- (22) **International Filing Date:**
30 May 2014 (30.05.2014)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
13/911,732 6 June 2013 (06.06.2013) US
- (71) **Applicant:** APPLE INC. [US/US]; 1 Infinite Loop, Cupertino, California 95014-2094 (US).
- (72) **Inventors:** PAI, Raghunandan K.; 1 Infinite Loop, M/S 53-2PG, Cupertino, California 95014 (US). NARAYANAN, Karthik; 1 Infinite Loop, M/S 60-1MME, Cupertino, California 95014 (US).
- (74) **Agent:** GOTTLIEB, Kirk A.; Fish & Richardson P.C., P.O. Box 1022, Minneapolis, Minnesota 55440-1022 (US).
- (81) **Designated States** (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM,

AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

- (84) **Designated States** (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— with international search report (Art. 21(3))

(54) **Title:** DEVICE LOCATOR DISABLE AUTHENTICATION**FIG. 1**

(57) **Abstract:** A device locator mode or find my device (FMD) mode can allow a lost, stolen, or misplaced mobile device to be located. The FMD mode can be enabled or disabled on a mobile device. Sometimes thieves or unauthorized parties attempt to disable the FMD mode. To prevent this, the mobile device can transmit a unique device identifier to a remote server. The remote server can link the device identifier to a cloud-based user account associated with the user of the mobile device. Before an FMD mode is disabled on the mobile device, before the content or settings can be erased, and/or before a mobile device is permitted to be activated/reactivated, a user of the mobile device can be challenged for the credentials of the cloud-based user account. If valid credentials are provided, FMD can be disabled, the content or settings can be reset, and/or the device can be activated/reactivated.

DEVICE LOCATOR DISABLE AUTHENTICATION

5

BACKGROUND

[0001] The present disclosure relates to computing devices and, more specifically, to authentication after a device locator mode has been enabled on a computing device.

[0002] Modern advances in computing devices have resulted in smaller, more powerful and wirelessly networked computing devices that can be easily carried by users at all times. As a
10 result, these devices are relied on greatly by their owners and often are trusted to carry their owner's personal and sensitive information.

[0003] Naturally, theft of such devices has increased as thieves are attracted to the high resale price and high demand for such computing devices as well as the possibility to steal personal information of the owner of the computing device. The high price and demand of a computing
15 device can also tempt a non-thief who finds a lost computing device to keep the device rather than search for its rightful owner. Alternatively, a person who finds a lost device and intends to return it may find it difficult to locate the owner.

[0004] Current systems attempt to address these problems by providing the location of the device to an owner of a lost device; however, these types of systems can break down when a
20 thief turns off the location feature, erases the device, or turns the device off. Other systems allow the lost device to be locked to deter theft. Again, the thief may erase the device to get around this. Other systems allow for erasing the device remotely so that personal or sensitive data stored on the lost device is protected. One problem with remotely erasing a device is that often the device is no longer locatable after the device is erased. As an unintended consequence,
25 remotely wiping a device can actually help a thief by making the device harder to find or identify.

[0005] Embodiments of the invention address these and other problems both individually and collectively.

SUMMARY

[0006] Additional features and advantages of the disclosure will be set forth in the description which follows. These and other features of the disclosure will become more fully apparent from the following description and appended claims, or can be learned by the practice of the principles set forth herein.

[0007] In some embodiments, a Find My Device (FMD) mode is enabled on a mobile device and a hardware identifier for the mobile device is associated with a cloud-based account identifier and account credentials. The mobile device may or may not be protected with a local passcode lock. Subsequently, a user can disable the FMD mode through a settings menu (e.g., Settings > Location Settings > Turn Off Find My Device). The FMD mode can be disabled in a number of other ways, including deleting a cloud-based user account from the mobile device (e.g., deleting an iCloud account in a settings menu), resetting settings or data (e.g., Settings > General > Reset), and the like. When the user attempts to change a setting on the mobile device that disables the FMD mode, the user of the mobile device can be challenged for the credentials. The mobile device can disable the FMD mode when valid credentials are provided or remain in FMD mode when invalid credentials are provided. This can prevent a thief or other unauthorized person from disabling the FMD mode on the device.

[0008] In some embodiments, an FMD mode is enabled on a mobile device and a hardware identifier for the mobile device is associated with a cloud-based account identifier and account credentials. Subsequently, the content or settings of the mobile device are erased. After a device is wiped or erased, a reactivation may be required before the device is useable to its full functionality. Erasing the content or settings may, by default, disable the FMD mode on the mobile device. When that mobile device attempts to reactivate, reauthorize, or the like, the user of the mobile device may be challenged for the credentials. The mobile device can be reactivated when valid credentials are provided or denied reactivation when invalid credentials are provided. This can prevent a thief or other unauthorized person from using a wiped device or device that has been otherwise erased.

BRIEF DESCRIPTION OF THE DRAWINGS

[0009] FIG. 1 illustrates a high-level block diagram of a system for remotely authenticating a user of a mobile device with a device locator mode enabled according to some embodiments of the present invention.

5 [0010] FIG. 2 illustrates a system including computing devices in network communication with each other according to some embodiments of the present invention.

[0011] FIG. 3 illustrates a high-level process flow of a method of device locator disable authentication according to some embodiments of the present invention.

10 [0012] FIG. 4 illustrates a high-level process flow of a method of enabling an FMD mode on a mobile device according to some embodiments of the present invention.

[0013] FIG. 5 illustrates a high-level process flow of a method of determining whether to allow an FMD mode on a mobile device to be disabled according to some embodiments of the present invention.

15 [0014] FIG. 6 illustrates a high-level process flow of a method of disabling an FMD mode on a mobile device according to some embodiments of the present invention.

[0015] FIG. 7 illustrates a user interface of an embodiment of setting up and activating a mobile device according to some embodiments of the present invention.

[0016] FIG. 8 illustrates a user interface of an embodiment of providing account credentials according to some embodiments of the present invention.

20 [0017] FIG. 9 illustrates a user interface of an embodiment of enabling an FMD mode on a mobile device according to some embodiments of the present invention.

[0018] FIG. 10 illustrates an embodiment of a user interface that can be used to disable an FMD mode on a mobile device according to some embodiments of the present invention.

25 [0019] FIG. 11 illustrates an embodiment of a user interface that can be used to disable an FMD mode on a mobile device according to some embodiments of the present invention.

[0020] FIG. 12 illustrates an embodiment of location data being presented according to some embodiments of the present invention.

[0021] FIG. 13 illustrates an embodiment of location data being presented according to some embodiments of the present invention.

[0022] FIG. 14 illustrates a computer system that can be used in accordance with embodiments of the present invention.

5

DETAILED DESCRIPTION

[0023] Various embodiments of the disclosure are discussed in detail below. While specific implementations are discussed, it should be understood that this is done for illustration purposes only. A person skilled in the relevant art will recognize that other components and configurations may be used without departing from the spirit and scope of the disclosure.

10 [0024] Various systems exist for remotely locating mobile user devices, remotely sending messages to those devices and/or remotely erasing those devices to preserve sensitive data. US Patent Appl. Nos. 12/434,586 (filed on May 1, 2009 and published as US Pub. No. 2010/0279652), 12/434,582 (filed on May 1, 2009 and published as US Pub. 2010/0279673), and 12/750,600 (filed on March 30, 2010 and published as US Pub. No. 2010/0279675) describe
15 various methods, systems and apparatuses for remotely locating and commanding a mobile device. US Patent App. No. 13/488438, filed on June 4, 2012, describes systems, methods, and apparatuses for remotely initiating a lost mode on a computing device. Each of these applications is hereby incorporated by reference in their entirety for all purposes.

[0025] One problem faced by device locator systems is that thieves or others can disable these
20 systems so that the mobile computing devices can no longer be located, communicated with, and/or remotely erased. Additionally, thieves are getting more sophisticated. Certain embodiments of the present invention address the growing sophistication of thieves and others in the illicit trade of stolen or lost devices. There are numerous ways a device locator mode can be disabled or turned off. For example, an FMD mode can be turned off in a settings menu of the
25 mobile device. This can be especially easy for an unauthorized party to do if a local passcode lock does not protect the device and/or the passcode lock timeout has not occurred. In another example, an FMD mode may be disabled by removing a SIM card from the device. In yet another example, a device may be erased or restored. For example, a mobile device can be restored to factory settings using the mobile device itself or by using a separate user computing
30 device in communication with the mobile device (e.g., iTunes to restore to factory settings on an

iPhone). In still another example, a device may be put into a device firmware update (DFU) mode, which can disable the FMD mode. Another example is that a user account associated with an FMD mode may be deleted from the device (e.g., in the case of commercially available Find My iPhone, a user's Apple ID account can be deleted from the device, thereby disabling Find My iPhone). Other ways of disabling FMD may be possible and for security reasons they will not be described in detail here.

[0026] Passcode locks on mobile devices can temporarily prevent someone from disabling a device locator mode on a mobile device. Some passcode locks suppress all or some of the user interface elements that would allow access to data and/or applications on a mobile device and thus render the device in a useless locked state. Typically, passcodes are stored on a mobile device's memory. When in a locked state, the mobile device has limited functionality and prompts a user for input of a secret code (e.g., a passcode). The user can input the passcode. In response to the user entering the passcode, the mobile device itself (typically without exchanging messages with a remote server computer) determines whether or not the passcode is valid. For example, a processor on the device compares the user-entered passcode to the stored passcode. If the passcode is valid, the mobile device unlocks itself and becomes useable. If the passcode is invalid, the mobile device can remain in a locked state. However, this method too is vulnerable to device resets, device erases, and DFU mode resets because the passcode memory can be overwritten or modified in a manner that circumvents the passcode protection. Therefore, a system that more robustly addresses the growing sophistication of thieves and others is needed.

[0027] A hardware identification can be associated with cloud-based user account credentials. The hardware identifier can be any immutable and/or unchangeable identifier of unique hardware. The cloud-based user account credentials can be any suitable credentials that are stored by and/or verified by a remote server computer in communication with the mobile device. For example, cloud-based user account credentials are verified by a remote server computer by an exchange of messages between a mobile device and server using a network. Cloud-based user account credentials can provide an external verification technique. On the other hand, local passcode locks and the like are verified locally by the device itself. Local passcode locks can be verified without a network connection. Cloud-based authentication uses a network connection, such as the Internet.

[0028] In some embodiments, an FMD mode is activated on a mobile device and a hardware identifier for the mobile device is associated with a cloud-based account identifier and account credentials. Subsequently, the content or settings of the mobile device are erased or reset. Erasing the content or settings may, by default, disable the FMD mode on the mobile device.

5 When that mobile device attempts to reactivate, reauthorize, or the like, the user of the mobile device may be challenged for the credentials. The mobile device can be reactivated when valid credentials are provided or denied reactivation when invalid credentials are provided. This can prevent a thief or other unauthorized person from using a wiped device.

[0029] In some embodiments, an FMD mode is activated on a mobile device and a hardware
10 identifier for the mobile device is associated with a cloud-based account identifier and account credentials. Subsequently, a user can disable the FMD mode through a settings menu. When the user attempts to change a setting on the mobile device that disables the FMD mode, the user of the mobile device may be challenged for the credentials. The mobile device can disable the FMD mode when valid credentials are provided or remain in FMD when invalid credentials are
15 provided. This can prevent a thief or other unauthorized person from disabling the FMD mode on the device.

[0030] FIG. 1 illustrates a high-level block diagram of a system 100 for remotely authenticating a user of a mobile device with a device locator mode enabled according to some embodiments. System 100 includes a mobile device 110 and one or more servers 150. Servers
20 150 can include an activation server 270 for activating a mobile device and a find my device (FMD) server 215 for locating mobile devices. Activation server 270 and FMD server 215 could be implemented as one or more distinct servers and are described in more detail below. Mobile device 110 is shown with a sequence of three sample user interfaces 120, 130, and 140 that could be used in some embodiments. Mobile device 110 has a hardware identifier 115, which is a
25 hardware element that uniquely identifies the mobile device 110. In some embodiments, hardware identifier 115 cannot be changed and/or is not erasable or programmable once set.

[0031] Turning to a simplified example, a mobile device can be activated to enable one or more functionalities. For example, an iPhone® commercially available from Apple may need to be activated in order for it to be useable as a phone. A mobile device can be activated by
30 navigating through various screens, selecting options and/or entering information into the mobile

device. The mobile device can configure on-board settings in accordance with the user input. The mobile device can send messages to, and communicate with, an activation server, which can store information relating to the activation (e.g., opt-ins, opt-outs, cloud-based account information, etc.).

5 **[0032]** In some embodiments, as part of the activation process, the mobile device can transmit a hardware identifier to one or more servers (e.g., the activation server). Device activation may include sending device information, such as a hardware identifier, to a remote server. The hardware identifier, for example, could be a serial number, International Mobile Station Equipment Number (IMEI), electronic serial number (ESN), or other suitable hardware identifier
10 that uniquely identifies the device hardware.

[0033] In some embodiments, a cloud-based user account can be set up on the mobile device. Cloud-based user accounts can have an account identifier and account credentials, such as a password, associated with them for identifying the account and authenticating the user. Account identifiers and account credentials for the cloud-based account are different from locally stored
15 passwords/passcodes in that account credentials are verified using a remote server computer, rather than a processor that is part of the mobile device. Authentication credentials may include an account identifier, a user identifier, a password, and other data that can authenticate the user.

[0034] In some embodiments, the account identifier and/or credentials for the cloud-based account can be stored in a secure memory of the mobile device such that it cannot be accessed by
20 a thief or other unauthorized party. For example, a user name and password can be encrypted and stored such that a cloud-based service is available on the device without the user needing to repeatedly enter in the credentials. This can also provide user access to the various features of the cloud-based user account without the account credentials being available to copy from the mobile device memory.

25 **[0035]** In some embodiments, a device locator mode (or find my device mode) can be enabled by the user as part of the activation process or thereafter. When the mobile device is operating in device locator mode, authorized requesting user devices can receive location information of the mobile device. In some embodiments, the device cannot be located unless device locator mode is enabled.

[0036] When a device locator mode is enabled, messages can be sent to one or more servers (e.g., activation server 270 and/or FMD server 215). Responsive to receipt of a message to enable the device locator mode (or a message indicating that a device locator mode has been enabled on the mobile device), the servers may link the hardware ID of the mobile device to the cloud-based account credentials. In some embodiments, the hardware identifier may be linked to cloud-based user account authentication credentials in an activation record. The activation record can be stored in a database on a remote server. In some embodiments, this linkage can occur automatically when the device locator mode is enabled. In some embodiments, the user may be presented with a prompt that asks whether the user would like to enable the protections provided by linking the hardware ID to the cloud-based account credentials.

[0037] In some embodiments, a user may attempt to disable the device locator mode. This may be done by an authorized user of the device or by an unauthorized user. User interface 120 shows one example of how a device locator mode can be disabled. For example, in the Settings or Location Services menu, a user can toggle off a button 125 to disable the device locator mode. Responsive to toggling button 125, the mobile device can send hardware ID 115 to a server.

[0038] The server can receive hardware ID 115 and determine whether or not hardware ID 115 is associated with a mobile device that had previously enabled a device locator mode. The server can send a challenge, or initiate the sending of a challenge, to mobile device 110. The challenge can include a challenge for the credentials for the cloud-based account previously associated with the particular hardware ID provided by mobile device 110.

[0039] User interface 130 shows one example of how a challenge could be presented to a user for the account credentials in response to a user request to disable a device locator mode. User interface 130 can include one or more fields 135 for a user to enter account credentials. After a user enters credentials, the credentials can be sent to the server for validation. One or more servers can determine whether the account credentials are valid and send a response indicating that the credentials are valid (or invalid).

[0040] If the credentials are valid, the mobile device can disable the device locator mode. In this circumstance, user interface 140 can include a toggle button 145 that indicates that the device locator mode is OFF. If the credentials are invalid, the mobile device can continue to operate in device locator mode. In some embodiments, a prompt can be displayed indicating that

the device is continuing to operate in device locator mode because the proper credentials have not been provided. In some embodiments, a device is made unusable if invalid credentials are provided after a threshold number of attempts. In some embodiments, a device locator mode cannot be disabled without authentication to a remote server.

5 [0041] User interfaces 120, 130, and 140 show one example of how an FMD mode could be disabled. There are numerous other ways that an FMD mode could be disabled, including resetting settings on a device, erasing a device, restoring a device to a previous configuration, and the like. In some embodiments, when a device has been reset/restored/erased, the mobile device can be prohibited from activating until the user is authenticated by a remote server
10 computer. One having skill in the art will recognize that other ways for disabling an FMD mode are possible and contemplated within the scope of the present invention. Some of these other methods are described in more detail below.

I. FIND MY DEVICE SYSTEM

[0042] As illustrated in FIG. 2, an exemplary system includes computing devices in network
15 communication with each other, a mobile user device 205, a Find My Device (FMD) server 215, an activation server 270, and a requesting user device 220. The system illustrated in FIG. 2 can be configured to allow requesting device 220 to locate mobile device 205 when an FMD mode is enabled on mobile device 205.

[0043] As illustrated, FMD server 215 can contain a number of components. The components
20 can include one or more databases for storing data relevant to the operation of FMD server 215, e.g., an account database 225 and a location database 230; and one or more modules or interfaces for interacting with the databases and/or controlling the features provided by the FMD server 215, e.g., an authentication module 235, a request module 240 and a location module 245. Each of these components is discussed in more detail below; however, it should be understood to one
25 skilled in the art that the configuration illustrated is simply one possible configuration and that other configurations, with more or less components, are possible.

[0044] FMD server 215 can include an account database 225 configured to store a user profile for each of a plurality of users. A user's profile can include a variety of information about the user, for example the information can include a user name, password, a list of all computing

devices owned by the user, an identifier for each computing device owned by the user, user specified preferences, contact information, demographic information, etc.

[0045] FMD server 215 can also include an authentication module 235, configured to communicate with account database 225 and authenticate that a user requesting the location of mobile device 205, for example, has permission to make the request. In another example, authentication module 235 can be configured to communicate with account database 225 and authenticate that a user has permission to disable an FMD mode on mobile device 205. In yet another example, authentication module 235 can be configured to communicate with account database 225 and authenticates that a mobile device is permitted to be reset or reactivated. To properly authenticate a user, authentication module 235 can be configured to prompt the user to enter authenticating information, such as a user name and password. The password can be any type of password known to those skilled in the art such as a numeric pin, character password, gesture, etc.

[0046] To confirm that the authentication information received from the requesting user is correct, authentication module 235 can be configured to communicate with account database 225 to confirm that the given user name and password match a user profile in account database 225. If the given user name and password matches a user profile stored in account database 225, the requesting user can be authenticated as having permission to receive location information of mobile device 205, disable an FMD mode on mobile device 205, or reactivate mobile device 205. Although a user name and password are used as an example, one skilled in the art would recognize that any variety of authenticating information can be requested from the user, including personal information or answers to predetermined security questions.

[0047] In some embodiments, requesting device 220 can include a web browser application configured to request access to FMD server 215 via the communication network 210. In some embodiments, authentication module 235 and request module 240, either entirely or partially, can be running on requesting device 220 and the requesting user can access modules 235, 240 from requesting device 220 to create the request.

[0048] FMD server 215 can also include a location module 245 configured to receive location data from mobile device 205 and transmit the location to the requesting user. The location data can include data indicating the location of mobile device 205 as well as the time mobile device

205 was at the location. Once received, location module 245 can be configured to transmit the location data to the requesting user in numerous ways. For example, in some embodiments, the location data can be sent to requesting device 220. Location module 245 can determine whether requesting device 220 is available, and if available, send the location data. If requesting device
5 220 is not available, location module 245 can be configured to store the location data in a location database 230 on FMD server 215 until requesting device 220 is available.

[0049] The location data can be presented to the requesting user in numerous ways. In some embodiments, the location data can be presented to the requesting user on a map that tracks the movement of mobile device 205. FIGS. 12 and 13 are two such examples. In some
10 embodiments, the location data can be presented to the requesting user by giving the street address or GPS coordinate of mobile device 205.

[0050] The location data can also be sent to the requesting user in numerous ways. For example, in some embodiments, the requesting user can log into web interface or application configured to communicate with location module 245 to view the location of the mobile device.
15 In some embodiments, the location data can be e-mailed to the owner of the user device. In some embodiments, the location data can be sent to requesting device 220 via a push notification to immediately update the requesting user of the location of mobile device 205. Although the above examples of sending location data are described, these examples are not meant to be limiting and are just a few possible embodiments. One skilled in the art would recognize that
20 there are numerous ways to send and present data.

[0051] Mobile device 205 can contain a number of components. The components can include one or more databases for storing data relevant to the operation of the device and one or more modules or interfaces for interacting with the databases and/or controlling the features provided by the mobile user device, e.g., a user interface module 255, hardware identifier 260, and Find
25 My Device (FMD) module 265. Each of these components is discussed in more detail below; however, it should be understood to one skilled in the art that the configuration illustrated is simply one possible configuration and that other configurations, with more or less components, are possible.

[0052] Mobile device 205 can include a user interface module 255 configured to manage the user interface on mobile device 205. This can include displaying all user interface elements on the device such as icons, buttons, controls, date, time, notifications, alerts, etc.

[0053] Mobile device 205 can include a hardware identifier that uniquely identifies mobile device 205. Information uniquely identifying the mobile device can include a serial number, a telephone number, a Subscriber Identity Module (SIM) card, a Media Access Control (MAC) address, or an International Mobile Equipment Identity (IMEI). In some embodiments, the information identifying the mobile device can be a unique device identifier (UDID), which can be a hash, e.g., generated using a Secure Hash Algorithm, of hardware identifiers associated with the mobile device. In some embodiments, the unique identifier can be obtained by servers from the mobile device automatically. Thus, data entry errors can be avoided.

[0054] Mobile device 205 can also include an FMD module 265 configured to provide location data to FMD server 215 and/or requesting device 220. For example, in some embodiments, the FMD module 265 can be a daemon running in the background on mobile device 205 and configured to communicate with the operating system to initiate applications and modules running on mobile device 205 as well as control hardware components of mobile device 205.

[0055] In some embodiments, FMD module 265 can be configured to transmit location data to the requesting user. For example, FMD module 265 can be configured to collect location data from a GPS component of mobile device 205 and periodically send the location data to the requesting user. The location data can be any type of data that can identify the location of the mobile device. For example, the location data can be GPS coordinates, a street address, etc. In addition, the location data can include the time that the mobile device was at the specified location. For example, FMD module 265 can be configured to receive the time from an internal clock running on mobile device 205.

[0056] In some embodiments, the FMD module 265 can be configured to send the location data to FMD server 215, which then sends the location data to the requesting user. In some embodiments, FMD module 265 sends the location data to requesting device 220. In some embodiments, the FMD module determines whether requesting device 220 is available to receive the location data, and if so, send the location data to requesting device 220, but if the requesting device is not available, FMD module 265 sends the location data to FMD server 215. In some

embodiments, FMD module 265 sends the location data to a personal account associated with the requesting user, such as the requesting user's e-mail account. Although the above examples of sending location data to a requesting user are described, these are just possible embodiments and are not meant to be limiting. One skilled in the art would recognize that the location information can be sent to the requesting user in numerous other ways.

[0057] Activation server 270 can store information related to the activation process, including the hardware ID. Hardware identifiers and user account information may be stored in an activation record database 275. An entry in activation record database 275 can include a hardware identifier for a mobile device and user credentials for an account of a user of the mobile device. The user credentials can be an account identifier and/or authentication data.

[0058] In some embodiments, activation server 270 and FMD server 215 can be implemented on the same server computer. In some embodiments, activation server 270 and FMD server 215 can be implemented on different server computers and/or can be remote from one another. In some embodiments, activation server 270 and FMD server 215 are operated and maintained by different entities, while in other embodiments they are operated by the same entity. An advantage to the same operating entity controlling both activation server 270 and FMD server 215 is that information can be more easily shared between the servers and the system can be more secure.

II. FIND MY DEVICE METHODS

[0059] Various methods are described below. One having skill in the art will recognize that the following methods are exemplary in nature and that various modifications can be made without departing from the scope of the present invention. One or more steps may not be shown for clarity and the order of one or more steps can be modified. Some of the modifications in order are specifically described, while other modifications to the order of the process will be apparent to one having skill in the art.

[0060] FIG. 3 illustrates a high-level process flow of a method 300 of device locator disable authentication according to some embodiments of the present invention. Method 300 can be used to prevent an unauthorized third party from disabling an FMD mode of a mobile device

(e.g., mobile device 110 in FIG. 1 or 205 in FIG. 2). Method 300 can also be used to permit a rightful possessor of a mobile device to turn off an FMD mode on the device as needed.

[0061] At block 310, a user can activate a mobile device with an activation server. In some embodiments, a mobile device needs to be activated before it can be used and/or used to its full functionality. For example, a mobile device may need to be activated to be used as a mobile phone or as a wireless Internet device. In some embodiments, the mobile device is not useable or certain features are not available until the mobile device is activated. Activating the device can initialize one or more settings on the device or on a remote server in communication with the mobile device. Sometimes – for example, after a device has been restored to factory settings – a device may have to be reactivated before it can be used and/or used to its full functionality.

[0062] In some embodiments, a setup assistant software module facilitates the set up process and provides various user interfaces to guide a user through the activation process. In some embodiments, the activation process includes user interfaces for the user to select a country, select a WiFi network, set up email, opt into location services, opt into or out of various other services, or the like. In some embodiments, the activation process includes prompting the user for cloud-based user account credentials, such as a user name and a password. In some embodiments, the user may be prompted to create a cloud-based user account, while in others the user can enter account credentials for an account that has been previously created.

[0063] In some embodiments, the activation process might occur with limited or no user input (e.g., with limited or no prompting from setup assistant software). For example, a software backup of a mobile device may have been created. In some embodiments, when a software backup is used to restore or initialize a device, one or more of the user interfaces prompting the user for user input may be omitted and the software backup may be used instead. For example, a user might upgrade to a new device. The mobile device may be initialized from a backup. In another example, a user might restore a device from a backup.

[0064] In some embodiments, the software backup is stored in the cloud (e.g., an iCloud account backup). In some embodiments, the software backup can be stored on a separate computing device (e.g., a personal computer). For example, a backup created in the syncing process with a software program can be stored on a separate computing device (e.g., iTunes on a

computer). The backup can be used to restore factory settings on a mobile device in communication with the separate computing device.

[0065] At block 320, an FMD mode can be enabled on the device. In some embodiments, enabling of the FMD mode can occur as part of the activation process. For example, the activation process can include a user interface for enabling an FMD mode on the mobile device. In some embodiments, FMD mode can be enabled at a later time (e.g., after the activation process is completed). For example, a setting menu can be provided for a user to turn on an FMD mode on the mobile device. In some embodiments, if an FMD mode was enabled on the backup used to restore or initialize the device, then an FMD can be enabled when the device is restored or initialized. For example, a mobile device may have had the FMD mode enabled when a backup of that device was created. When the device backup is used to initialize or restore a device, FMD mode can be enabled based on the backup.

[0066] When the FMD mode is enabled on a mobile device, a server can associate a device hardware identifier of the mobile device with the cloud-based user account credentials. The associated hardware identifier and user account credentials can be stored in a database in communication with the server.

[0067] At block 330, the mobile device or a server can determine whether or not there has been an attempt to disable an FMD mode on the mobile device. For example, a user of the device may attempt to disable an FMD mode using various provided user interfaces on the mobile device (e.g., disabling FMD mode in a settings menu). In another example, the mobile device may have been erased or restored to factory settings, for example, and a server can recognize this as an implicit attempt to disable FMD mode. In some embodiments, if there has not been an attempt to disable FMD mode on the device, the mobile device remains in the FMD mode.

[0068] In some embodiments, before the software running on the separate computing device will permit the restore/erase, the software program may determine whether the mobile device has an FMD mode enabled. If an FMD mode is enabled, the user may be challenged for account credentials as described herein. In some embodiments, when a mobile device in DFU mode is connected to a syncing software on a separate computing device, the syncing software (e.g., iTunes) can challenge a user for the user account credentials (e.g., Apple ID and password).

[0069] At block 340, when it is determined that there was an attempt to disable the FMD mode on the device, a challenge can be sent to a mobile device by a server computer and can be presented to the user. In some embodiments, the challenge is for the cloud-based user account identifier, password, and/or other user account credentials. For example, the user can be
5 challenged for credentials associated with an FMD account, for example. Other cloud-based accounts can be used. The challenge and response can be received and entered, respectively, into either or both of the mobile device or/and the separate user computing device. For example, the display on the mobile device may present the user with the challenge, and the user can enter a challenge response into the device with a user input element. The challenge response can be sent
10 to a server in communication with the mobile device. For example, the response can be sent to the server computer that issued the challenge.

[0070] At block 350, the challenge response can be evaluated to determine whether the response is valid. In some embodiments, a server computer in communication with the mobile device evaluated whether the challenge response is valid. For example, the server can look up
15 the account credentials associated with the hardware identifier for the mobile device. The server can compare the user-entered challenge response with the stored account credentials and determine if there is a match.

[0071] If the challenge response does not include valid user account credentials, then the device remains in FMD mode (block 355). In some embodiments, if the challenge response does
20 not include valid user account credentials, the device may be prohibited from certain functionalities (e.g., the device may be denied full activation). If the challenge response is invalid, then activation may be prohibited and/or the mobile device may remain in an FMD mode. In some embodiments, the server sends instructions denying activation or prohibiting an FMD mode change.

[0072] If the challenge response is valid, then FMD mode can be disabled on the device (block 360). In some embodiments, the server transmits a message indicating that the challenge response was valid and that FMD mode can be disabled. In some, embodiments, the server transmits an instruction to disable FMD on the device.

[0073] FIG. 4 illustrates a high-level process flow of a method 400 of enabling an FMD mode
30 on a mobile device according to some embodiments of the present invention. A mobile device

can perform method 400 during or after the activation process. At block 410, an FMD mode of a mobile device can be enabled. In some embodiments, enabling the FMD mode can occur by a user selecting a setting. In some embodiments, enabling FMD mode can occur as part of a restore/initialization process.

5 **[0074]** Responsive to the enablement of the FMD mode on the mobile device, at block 420, the mobile device may initiate communication with a server. As part of the communications, at block 430, the mobile device may transmit a hardware identifier or another identifier that uniquely identifies the hardware of the mobile device to a remote server computer. In some embodiments, a hardware identifier is transmitted from the mobile device to the server computer.

10 In some embodiments, information linked to a unique identifier of the mobile device is transmitted from the mobile device to the server computer.

[0075] At block 440, the user may be prompted for FMD account credentials (e.g., an account ID and/or account password data associated with an account). In some embodiments, the account is an account that provides an FMD service. In some embodiments, the account is a

15 general account that provides various cloud computing services and the like. That is, although the figures illustrate an FMD account, one having skill in the art will recognize that other cloud-based account and credentials can be used without departing from the scope of the invention. In some embodiments, if the user does not have an account, the use may be prompted to create an account.

20 **[0076]** Regardless of whether the user has a previously created account ID and password or whether the user created a new account ID and password, at block 450, the mobile device receives input of the account credentials (e.g., account ID and/or the password). For example, the user may enter in the account credentials using a user input element on the mobile device.

[0077] In some embodiments, blocks 440 and 450 can be omitted and/or be performed earlier

25 in the process flow. For example, a user might provide an FMD account ID and password before enabling an FMD mode on the device.

[0078] At block 460, the mobile device transmits the account credentials to a remote server computer. As discussed herein, the remote server computer can link or associate the device identifier with the account ID and/or password. Linked hardware identifiers and account

credentials can be stored on the server computer or in another system. Later, the linked hardware identifiers and account credentials can be used to determine whether or not the FMD mode on the mobile device can be disabled and/or whether a mobile device is permitted to activate/reactivate.

5 **[0079]** FIG. 5 illustrates a high-level process flow of a method 500 of determining whether to allow a mobile device to activate/reactivate according to some embodiments of the present invention. Method 500 can be performed by a server in communication with mobile device (e.g., activation server, FMD server, or the like). At block 510, a remote server computer can receive a device identifier from a mobile device during an activation or set up process.

10 **[0080]** At block 520, the server computer can determine whether the device identifier is associated with a cloud-based user account (e.g., an FMD account). For example, the server computer can initiate query on an[??] account database and/or an activation record database. In some embodiments, block 520 can include determining whether a mobile device associated with the hardware ID has been activated before or whether the device is being activated for the first
15 time. In some embodiments, when a device is reset (e.g., restored to factory settings), the reset device may be required to go through the activation (reactivation) process again. In the reactivation process, a remote server can receive the device information and determine that the device was previously activated and that FMD mode was enabled for the device.

20 **[0081]** If the server determines that the device identifier is associated with an account, at block 525, the server can transmit a challenge to the device. In some embodiments, the challenge is for account credentials, such as an account identifier and/or an account password. The server can then receive a challenge response at block 530. For example, a user of the mobile device may enter a challenge response on the mobile device and the mobile device can transmit it to the server.

25 **[0082]** At block 535, the server can determine whether the challenge response is valid. In some embodiments, if the challenge response is valid (e.g., the response matches authentication credentials stored on the server), then the mobile device can be reactivated (block 540). In some embodiments, if an invalid challenge response is received, the mobile device activation can be denied (block 545). In some embodiments, if the challenge response is invalid, the mobile
30 device user may be challenged again. In some embodiments, there is a threshold maximum

number of times that an incorrect challenge response can be provided before reactivation is denied and/or the device functionality is limited. After a threshold maximum of invalid challenge responses, the server may deny reactivation (545).

5 [0083] If the server determines that the device identifier is not associated with an account, at block 550, the device can be activated. That is, since the hardware ID was not previously associated with an FMD account, the device can be activated as normal. This could be, for example, because the device is being activated for the first time or because the device was not previously associated with a FMD account. In some embodiments, the step of activation may occur in a different order than shown in FIG. 5. For example, activation can occur after storing
10 linked information (570) or at another suitable time.

[0084] At block 555, the server can receive an account identifier from the mobile device. The account identifier can be any user could-based user account. In some embodiments, the account is an account that provides an FMD service. For example, the account can be an FMD account, and the identifier can be a FMD account user name. Other cloud-based account are suitable. In
15 some embodiments, the account is a general account that provides various cloud computing services and the like.

[0085] At block 560, an account password or other authentication data can be received at the server. Authentication data can include a PIN, password, biometric identification data, or similar authentication. Multi-factor authentication can be used (e.g, two or three factor authentication).

20 [0086] At block 565, the server computer can link the device hardware identifier with the account identifier and/or account password. Linking the device hardware identifier with the account identifier and/or account password on a server before a device is lost, stolen, or misplaced can be beneficial because it provides an external technique for authenticating the device. That is, user authentication can still occur, using the hardware identifier, even if the
25 device has been erased/reset. Furthermore, user authentication can still occur even if a local passcode lock is not used or is circumvented. For example, if a hardware identifier is not associated with an account identifier and/or account password before the device falls into the hands of an unauthorized third party, the unauthorized user may simply turn off FMD mode or erase/reset the device. In this case, there may be limited recourse to prevent the unauthorized

user from disabling the FMD mode or resetting/erasing the device. This can make the device hard to locate and recover.

[0087] At block 570, the linked information can be stored to a database in communication with the server for later use in authenticating a user attempting to disable an FMD mode on a device.

5 For example, the server can link the hardware identifier, the cloud-based account, and/or the authentication data and store it in a database.

[0088] FIG. 6 illustrates a high-level process flow of a method 600 of disabling an FMD mode on a mobile device according to some embodiments of the present invention. Method 600 can be performed by a mobile device and/or a server in communication with the mobile device.

10 [0089] At block 610, an instruction is received to disable an FMD mode. In some embodiments, the instruction may be received as a user input from a user operating the mobile device (e.g., toggling an option in a device settings menu, such as Settings > Location Services > Find My Device ON/OFF) or other computing device in communication with the mobile device (e.g., iTunes sync). Content and settings may be reset or erased, for example, using a settings
15 menu user interface (e.g., Settings > General > Reset All Data, Erase all settings, Erase All Content, or the like). In some embodiments, the instruction may be the resetting, restoring, or erasing of a mobile device. For example, restoring a mobile device to factory settings can be considered an instruction to disable the FMD mode.

[0090] In some embodiments, mobile device erase or reset can be disabled until an FMD mode
20 of the device is disabled. That is, the user can be prevented from erasing/resetting a device while the FMD mode is enabled on the device. For example, the "Reset All Settings" and/or "Erase All Content and Settings" options in FIG. 11 may be disabled. In this circumstance, the user may be presented with a prompt that indicates that FMD mode must be turned off before the user is allowed to reset or erase the device. In some embodiments, the user interface may present a
25 shortcut to the appropriate settings menu such that the user can easily disable an FMD mode after being properly authenticated.

[0091] At block 620, a user of the mobile device is challenged for account credentials that are associated with the hardware identifier of the mobile device. The challenge can be generated by a server computer and transmitted to the mobile device. In some embodiments, the mobile

device displays the challenge and accepts a user input challenge response. In some embodiments, a separate computing device in communication with the mobile device displays the challenge and accepts a user input challenge response.

[0092] At block 630, the server computer determines whether the account credentials are valid.

5 For example, the server computer can query a database or another server computer to determine whether the user-provided challenge response is valid (e.g., whether the challenge response matches the account credentials in the database).

[0093] At block 640, if the challenge response was valid, the server can break the link between the hardware identifier and the user account. This step is optional, as some embodiments may

10 maintain the association between the hardware identifier and the user account. In some circumstances an owner of a mobile device may desire to sell or otherwise transfer possession or ownership of the mobile device. In this scenario, it is desirable to break the link between the unique hardware identifier of the mobile device and the user account. That is, the new owner of the device presumably will not know the account credentials of the previous owner and may
15 want to associate new account credentials with the mobile device.

[0094] To accomplish this, in some embodiments, the old user deletes personal data before sale. Responsive to the user input to erase personal data, the mobile device may prompt for a user account identifier and/or a user account password. This challenge can be received from a remote server computer in communication with the mobile device via an Internet connection. If
20 a valid response is provided and the user is authenticated, personal content and settings can be erased locally on the mobile device and the link in between the user account can be broken.

[0095] In some embodiments, the old user of the mobile device may not delete personal data before sale. For example, the old user / seller may forget to delete data and/or break the link between the user account and the hardware identifier. In this circumstance, the new user may be
25 prevented from activating the device or disabling FMD mode on the device if the link between the old user account and the mobile device identifier (e.g., the new user does not know the challenge response). In this circumstance, various methods can be used to differentiate between an unauthorized person (e.g., a thief) and an authorized user/owner. In some embodiments, the old user can log into an app (e.g., a find my device app) or web interface (e.g., a find my device
30 web interface) and provide account credentials to break the link between the hardware identifier

and the user account. In one embodiment, the old user can otherwise be authenticated in order to break the association between the hardware identifier and the user account (e.g., by calling a customer support telephone number associated with the find my device service and providing proof of identity).

5 [0096] At block 650, an instruction to disable the FMD mode is generated. In some embodiments, this instruction can be generated by a server computer and is received by the mobile device. The mobile device may disable the FMD mode on the device in response to receiving/generating the instruction. In some embodiments, the server computer can transmit a message to the mobile device indicating that valid credentials were provided, and responsive to
10 this message, the mobile device can generate an instruction to disable the FMD mode.

[0097] At block 660, if the challenge response is not valid, the server computer can determine whether a threshold maximum number of authentication attempts have been made unsuccessfully. If less than a threshold maximum unsuccessful attempts have been made, the process flow can return to block 620. If the threshold maximum unsuccessful attempts have
15 been made, the device may be prohibited from disabling the FMD mode on the device (block 670). In some embodiments, a message indicating that a threshold maximum has been reached can be displayed (block 680). In some embodiments, the message can indicate that FMD cannot be disabled for a threshold period of time or until a predetermined event occurs.

III. SAMPLE USER INTERFACES

20 [0098] FIG. 7 illustrates a user interface of an exemplary embodiment of setting up and activating a mobile device. As illustrated, the mobile device can be set up as a new device 710, restored from a cloud backup 720, or restored from a locally stored backup 730. This is an example of a user interface that could be used as part of an activation or setup process.

[0099] FIG. 8 illustrates a user interface of an exemplary embodiment of providing account
25 credentials. As illustrated, a user interface may be presented such that a user can enter a user account identifier 810 and a user account password 820. This is an example of a user interface that could be used as part of an activation or setup process. In some embodiments, after a user enters user input into fields 810 and 820, an account profile can be created on the mobile device to provide account services on the mobile device. In some embodiments, this account profile can

be later disabled or deactivated, for example as illustrated in FIG. 10. In some embodiments, the user account credentials could be provided after the activation and set up process is completed.

[0100] FIG. 9 illustrates a user interface of an exemplary embodiment of enabling an FMD mode on a mobile device. As illustrated, a user interface may be presented such that a user can choose enable an FMD mode (910) or not enable the FMD mode (920). This is an example of a user interface that could be used as part of an activation or setup process. In some embodiments, the enabling of the FMD mode can be done after the activation and set up process is completed. In some embodiments, responsive to the enabling of the FMD mode, a server computer associates a hardware identifier with user account credentials, as has been described herein.

[0101] FIG. 10 illustrates a user interface of an exemplary embodiment of a user interface that can be used to disable an FMD mode on a mobile device. In one example, an FMD mode can be disabled by toggling a button 1010 from ON to OFF, or the like. In another example, an FMD mode can be disabled by deleting or deactivating the user account from the mobile device by selecting a button 1020 that deletes or deactivates the user account. In some embodiments, responsive to toggling button 1010 or actuating button 1020, an instruction to disable the FMD mode can be generated and transmitted to a server.

[0102] FIG. 11 illustrates a user interface of an exemplary embodiment of a user interface that can be used to disable an FMD mode on a mobile device. In one example, an FMD mode can be disabled by actuating button 1110 to reset all settings. In another example, an FMD mode can be disabled by actuating a button 1120 to erase all content and settings. In some embodiments, responsive to actuating button 1110 or button 1120, an instruction to disable the FMD mode can be generated and transmitted to a server.

[0103] One having skill in the art will recognize that there are many other possibilities for user interfaces to activate a mobile device, enable an FDM mode, and disable an FMD mode on a mobile device. The examples shown are merely exemplary and not limiting.

[0104] FIG. 12 illustrates a user interface of an exemplary embodiment of location data being presented on a request user device. As illustrated, the location data 1205 can be presented as a dot over a map to illustrate the location of the lost, stolen, or misplaced device. Further, an info box 1210 can be presented with the dot that displays the time the location data was collected. As

illustrated, the lost device was determined to be at the identified location one minute prior to the location data being presented.

[0105] FIG. 13 illustrates a user interface of an exemplary embodiment of location data being presented on a requesting user device. As illustrated multiple location data points 1305, 1310, 1315 and 1320 can be displayed as dots on a map to illustrate the movement of the lost device. The location data points can be connected by a line to display the path of the lost device and the dots can be different colors to signify which location data point is the most recent. For example, all previous location data points can be illustrated in one color, such as green, while the most current data location point can be illustrated in a different color, such as red. Further, the each location data point can be configured to display an information box 1325 associated with the location data point that identifies the time at which the device was at the given location data point. As illustrated, the mobile device was at location data point 1315 at approximately 15 minutes prior at 11:30 am.

IV. SAMPLE COMPUTER SYSTEM

[0106] With reference to FIG. 14, an exemplary system 1400 includes a general-purpose computing device 1400, including a processing unit (CPU or processor) 1420 and a system bus 1410 that couples various system components including the system memory 1430 such as read only memory (ROM) 1440 and random access memory (RAM) 1450 to the processor 1420. The system 1400 can include a cache 1422 of high speed memory connected directly with, in close proximity to, or integrated as part of the processor 1420. The system 1400 copies data from the memory 1430 and/or the storage device 1460 to the cache 1422 for quick access by the processor 1420. In this way, the cache 1422 provides a performance boost that avoids processor 1420 delays while waiting for data. These and other modules can control or be configured to control the processor 1420 to perform various actions. Other system memory 1430 may be available for use as well. The memory 1430 can include multiple different types of memory with different performance characteristics. It can be appreciated that the disclosure may operate on a computing device 1400 with more than one processor 1420 or on a group or cluster of computing devices networked together to provide greater processing capability. The processor 1420 can include any general purpose processor and a hardware module or software module, such as module 1 1462, module 2 1464, and module 3 1466 stored in storage device 1460, configured to

control the processor 1420 as well as a special-purpose processor where software instructions are incorporated into the actual processor design. The processor 1420 may essentially be a completely self-contained computing system, containing multiple cores or processors, a bus, memory controller, cache, etc. A multi-core processor may be symmetric or asymmetric.

5 [0107] The system bus 1410 may be any of several types of bus structures including a memory bus or memory controller, a peripheral bus, and a local bus using any of a variety of bus architectures. A basic input/output (BIOS) stored in ROM 1440 or the like, may provide the basic routine that helps to transfer information between elements within the computing device 1400, such as during start-up. The computing device 1400 further includes storage devices 1460
10 such as a hard disk drive, a magnetic disk drive, an optical disk drive, tape drive or the like. The storage device 1460 can include software modules 1462, 1464, and 1466 for controlling the processor 1420. Other hardware or software modules are contemplated. The storage device 1460 is connected to the system bus 1410 by a drive interface. The drives and the associated computer-readable storage media provide nonvolatile storage of computer-readable instructions,
15 data structures, program modules and other data for the computing device 1400. In one aspect, a hardware module that performs a particular function includes the software component stored in a non-transitory computer-readable medium in connection with the necessary hardware components, such as the processor 1420, bus 1410, output device 1470, and so forth, to carry out the function. The basic components are known to those of skill in the art and appropriate
20 variations are contemplated depending on the type of device, such as whether the device 1400 is a small, handheld computing device, a desktop computer, or a computer server.

[0108] Although the exemplary embodiment described herein employs a storage device 1460, it should be appreciated by those skilled in the art that other types of computer-readable media which can store data that are accessible by a computer, such as magnetic cassettes, flash memory
25 cards, digital versatile disks, cartridges, random access memories (RAMs) 1450, read-only memory (ROM) 1440, a cable or wireless signal containing a bit stream and the like, may also be used in the exemplary operating environment. Non-transitory computer-readable storage media expressly exclude media such as energy, carrier signals, electromagnetic waves, and signals per se.

[0109] To enable user interaction with the computing device 1400, an input device 1490 represents any number of input mechanisms, such as a microphone for speech, a touch-sensitive screen for gesture or graphical input, keyboard, mouse, motion input, speech and so forth. An output device 1470 can also be one or more of a number of output mechanisms known to those of skill in the art. In some instances, multimodal systems enable a user to provide multiple types of input to communicate with the computing device 1400. The communications interface 1480 generally governs and manages the user input and system output. There is no restriction on operating on any particular hardware arrangement and therefore the basic features here may easily be substituted for improved hardware or firmware arrangements as they are developed.

[0110] For clarity of explanation, the illustrative system embodiment is presented as including individual functional blocks including functional blocks labeled as a "processor" or processor 1420. The functions these blocks represent may be provided through the use of either shared or dedicated hardware, including, but not limited to, hardware capable of executing software and hardware, such as a processor 1420, that is purpose-built to operate as an equivalent to software executing on a general purpose processor. For example the functions of one or more processors presented in FIG. 14 may be provided by a single shared processor or multiple processors. (Use of the term "processor" should not be construed to refer exclusively to hardware capable of executing software.) Illustrative embodiments may include microprocessor and/or digital signal processor (DSP) hardware, read-only memory (ROM) 1440 for storing software performing the operations discussed below, and random access memory (RAM) 1450 for storing results. Very large scale integration (VLSI) hardware embodiments, as well as custom VLSI circuitry in combination with a general purpose DSP circuit, may also be provided.

[0111] The logical operations of the various embodiments are implemented as: (1) a sequence of computer implemented steps, operations, or procedures running on a programmable circuit within a general use computer, (2) a sequence of computer implemented steps, operations, or procedures running on a specific-use programmable circuit; and/or (3) interconnected machine modules or program engines within the programmable circuits. The system 1400 shown in FIG. 14 can practice all or part of the recited methods, can be a part of the recited systems, and/or can operate according to instructions in the recited non-transitory computer-readable storage media. Such logical operations can be implemented as modules configured to control the processor 1420

to perform particular functions according to the programming of the module. For example, FIG. 14 illustrates three modules Mod1 1462, Mod2 1464 and Mod3 1466, which are modules configured to control the processor 1420. These modules may be stored on the storage device 1460 and loaded into RAM 1450 or memory 1430 at runtime or may be stored as would be

5 [0112] The present disclosure recognizes that the use of such personal information data in the present technology can be used to the benefit of users. For example, the personal information data can be used to better understand user behavior, facilitate and measure the effectiveness of advertisements, applications, and delivered content. Accordingly, use of such personal information data enables calculated control of the delivered content. For example, the system
10 can reduce the number of times a user receives a given ad or other content and can thereby select and deliver content that is more meaningful to users. Such changes in system behavior improve the user experience. Further, other uses for personal information data that benefit the user are also contemplated by the present disclosure.

[0113] The present disclosure further contemplates that the entities responsible for the
15 collection, analysis, disclosure, transfer, storage, or other use of such personal information data should implement and consistently use privacy policies and practices that are generally recognized as meeting or exceeding industry or governmental requirements for maintaining personal information data private and secure. For example, personal information from users should be collected for legitimate and reasonable uses of the entity and not shared or sold outside
20 of those legitimate uses. Further, such collection should occur only after the informed consent of the users. Additionally, such entities would take any needed steps for safeguarding and securing access to such personal information data and ensuring that others with access to the personal information data adhere to their privacy and security policies and procedures. Further, such entities can subject themselves to evaluation by third parties to certify their adherence to widely
25 accepted privacy policies and practices.

[0114] Despite the foregoing, the present disclosure also contemplates embodiments in which users selectively block the use of, or access to, personal information data. That is, the present disclosure contemplates that hardware and/or software elements can be provided to prevent or block access to such personal information data. For example, in the case of advertisement
30 delivery services, the present technology can be configured to allow users to select to “opt in” or

“opt out” of participation in the collection of personal information data during registration for services. In another example, users can select not to provide location information for advertisement delivery services. In yet another example, users can configure their devices or user terminals to prevent storage or use of cookies and other mechanisms from which personal information data can be discerned. The present disclosure also contemplates that other methods or technologies may exist for blocking access to their personal information data.

[0115] Therefore, although the present disclosure broadly covers use of personal information data to implement one or more various disclosed embodiments, the present disclosure also contemplates that the various embodiments can also be implemented without the need for accessing such personal information data. That is, the various embodiments of the present technology are not rendered inoperable due to the lack of all or a portion of such personal information data. For example, content can be selected and delivered to users by inferring preferences based on non-personal information data or a bare minimum amount of personal information, such as the content being requested by the device associated with a user, other non-personal information available to the content delivery services, or publicly available information.

[0116] Embodiments within the scope of the present disclosure may also include tangible and/or non-transitory computer-readable storage media for carrying or having computer-executable instructions or data structures stored thereon. Such non-transitory computer-readable storage media can be any available media that can be accessed by a general purpose or special purpose computer, including the functional design of any special purpose processor as discussed above. By way of example, and not limitation, such non-transitory computer-readable media can include RAM, ROM, EEPROM, CD-ROM or other optical disk storage, magnetic disk storage or other magnetic storage devices, or any other medium which can be used to carry or store desired program code means in the form of computer-executable instructions, data structures, or processor chip design. When information is transferred or provided over a network or another communications connection (either hardwired, wireless, or combination thereof) to a computer, the computer properly views the connection as a computer-readable medium. Thus, any such connection is properly termed a computer-readable medium. Combinations of the above should also be included within the scope of the computer-readable media.

[0117] Computer-executable instructions include, for example, instructions and data which cause a general purpose computer, special purpose computer, or special purpose processing device to perform a certain function or group of functions. Computer-executable instructions also include program modules that are executed by computers in stand-alone or network environments. Generally, program modules include routines, programs, components, data structures, objects, and the functions inherent in the design of special-purpose processors, etc. that performs particular tasks or implement particular abstract data types. Computer-executable instructions, associated data structures, and program modules represent examples of the program code means for executing steps of the methods disclosed herein. The particular sequence of such executable instructions or associated data structures represents examples of corresponding acts for implementing the functions described in such steps.

[0118] Those of skill in the art will appreciate that other embodiments of the disclosure may be practiced in network computing environments with many types of computer system configurations, including personal computers, hand-held devices, multi-processor systems, microprocessor-based or programmable consumer electronics, network PCs, minicomputers, mainframe computers, and the like. Embodiments may also be practiced in distributed computing environments where tasks are performed by local and remote processing devices that are linked (either by hardwired links, wireless links, or by a combination thereof) through a communications network. In a distributed computing environment, program modules may be located in both local and remote memory storage devices.

[0119] The various embodiments described above are provided by way of illustration only and should not be construed to limit the scope of the disclosure. Those skilled in the art will readily recognize various modifications and changes that may be made to the principles described herein without following the example embodiments and applications illustrated and described herein, and without departing from the spirit and scope of the disclosure.

[0120] It is understood that the examples and embodiments described herein are for illustrative purposes only and that various modifications or changes in light thereof will be suggested to persons skilled in the art and are to be included within the spirit and purview of this application and scope of the appended claims.

WHAT IS CLAIMED IS:

- 1 1. A method comprising:
2 activating a mobile device with a server, wherein activating the mobile device
3 includes transmitting a hardware identifier from the mobile device to the server;
4 associating, by the mobile device, a cloud-based user account with the mobile
5 device, wherein associating the user account with the mobile device includes transmitting user
6 account information to the server, the user account information including a user account
7 identifier and user authentication data;
8 enabling, by the mobile device, a device locator mode on the mobile device,
9 wherein the device locator mode enables the mobile device to be located by a requesting user
10 device;
11 after the device locator mode has been enabled, receiving, by the mobile device, a
12 user input on the mobile device to disable the device locator mode;
13 presenting, by the mobile device, a challenge to a user of the mobile device for
14 user authentication data; and
15 receiving, via a user interface of the mobile device, a challenge response from the
16 user; and
17 disabling the device locator mode when the challenge response is valid.
- 1 2. The method of claim 1 further comprising:
2 remaining in device locator mode when the challenge response is invalid.
- 1 3. The method of claim 1, wherein the enabling by the mobile device is in
2 response to a command from the server.
- 1 4. The method of claim 1, wherein receiving the user input on the mobile
2 device to disable the device locator mode includes one of the following:
3 a user input to delete a profile for the user account that is stored on the mobile
4 device;
5 a user input to restore default device settings; and
6 a user input to erase device content and settings.

1 5. The method of claim 2, further comprising:
2 after the device locator mode has been enabled, erasing all user-erasable content
3 on the mobile device;
4 reactivating the mobile device with the server, wherein reactivating of the mobile
5 device includes transmitting the hardware identifier from the mobile device to the server;
6 denying reactivation of the mobile device unless valid user authentication data is
7 received by the mobile device.

1 6. The method of claim 5, wherein erasing all user-erasable content on the
2 mobile device includes entering a device firmware update mode.

1 7. The method of claim 5, wherein the hardware identifier is not user-
2 erasable.

1 8. The method of claim 5, the mobile device has limited functionality until
2 the mobile device is activated.

1 9. A non-transitory computer-readable medium comprising code that, when
2 executed by a processor, causes a device to perform a method including:
3 activating a mobile device with a server, wherein activating the mobile device
4 includes transmitting a hardware identifier from the mobile device to the server;
5 associating a cloud-based user account with the mobile device;
6 enabling a device locator mode on the mobile device, wherein the device locator
7 mode enables the mobile device to be located by a requesting user device;
8 after the device locator mode has been enabled, receiving a user input on the
9 mobile device to disable the device locator mode;
10 presenting a challenge to a user of the mobile device for user authentication data;
11 and
12 receiving a challenge response from the user; and
13 disabling the device locator mode when the challenge response is valid.

1 10. The computer-readable medium of claim 9 further comprising:
2 remaining in device locator mode when the challenge response is invalid.

1 11. The computer-readable medium of claim 9, wherein the enabling by the
2 mobile device is in response to a command from the server.

1 12. The computer-readable medium of claim 9, wherein associating the user
2 account with the mobile device includes transmitting user account information to the server and
3 the user account information includes a user account identifier and user authentication data.

1 13. A method comprising:
2 receiving, by a server, a hardware identifier for a mobile device and cloud-based
3 user account identifier from the mobile device, wherein the user account identifier is associated
4 with user authentication data;
5 associating, by the server, the hardware identifier with the user account identifier;
6 storing, in a database coupled to the server, the associated hardware identifier and
7 user account identifier;
8 after a device locator mode has been enabled on the mobile device, receiving, by
9 the server, the hardware identifier from the mobile device;
10 determining, with the server, whether the hardware identifier has been previously
11 associated with the user account identifier; and
12 when the hardware identifier has been previously associated with the user account
13 identifier, initiating, by the server, a challenge to the mobile device, wherein the challenge
14 includes a request for the user authentication data;
15 transmitting, with the server, an instruction to disable the device locator mode to
16 the mobile device, when a challenge response is valid, wherein the challenge response is input by
17 a user of the mobile device.

1 14. The method of claim 13, further comprising:
2 transmitting, with the server, an instruction to remain in the device locator mode
3 to the mobile device, when the challenge response is invalid.

1 15. The method of claim 13, further comprising:
2 transmitting, with the server, an instruction to deny reactivation of the mobile
3 device to the mobile device, when the challenge response is invalid.

1 16. The method of claim 13 further comprising:
2 after a device locator mode has been enabled, receiving, by the server, a request to
3 disable the device locator mode.

1 17. A non-transitory computer-readable medium comprising code that, when
2 executed by a processor, causes a device to perform a method including:
3 receiving a hardware identifier for a mobile device and a cloud-based user
4 account identifier, wherein the user account identifier is associated with user authentication data;
5 associating the hardware identifier with the user account identifier;
6 storing the associated hardware identifier and user account identifier;
7 after a device locator mode has been enabled on the mobile device, receiving the
8 hardware identifier from the mobile device;
9 determining whether the hardware identifier has been previously associated with
10 the user account identifier;
11 when the hardware identifier has been previously associated with the user account
12 identifier, initiating a challenge to a user including a request for the user authentication data; and
13 generating an instruction to disable the device locator mode to the mobile device,
14 when a challenge response is valid, wherein the challenge response is input by a user of the
15 mobile device.

1 18. The computer-readable medium of claim 17, the method further
2 comprising:
3 generating an instruction to remain in the device locator mode to the mobile
4 device, when the challenge response is invalid.

1 19. The computer-readable medium of claim 17, the method further
2 comprising:
3 generating an instruction to deny reactivation of the mobile device to the mobile
4 device, when the challenge response is invalid.

1 20. The computer-readable medium of claim 17, the method further
2 comprising:
3 after a device locator mode has been enabled, receiving a request to disable the
4 device locator mode.

1/14

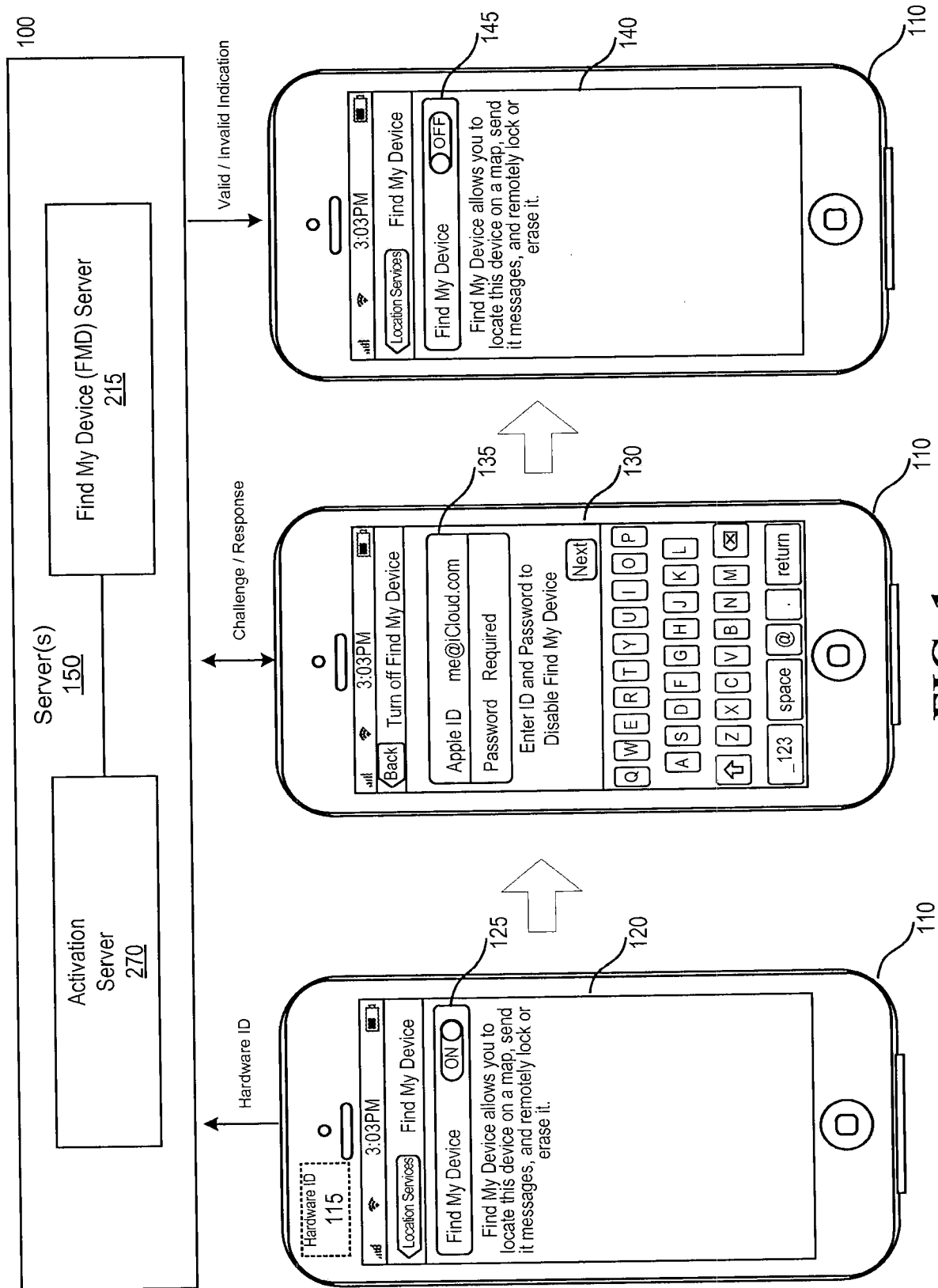


FIG. 1

2/14

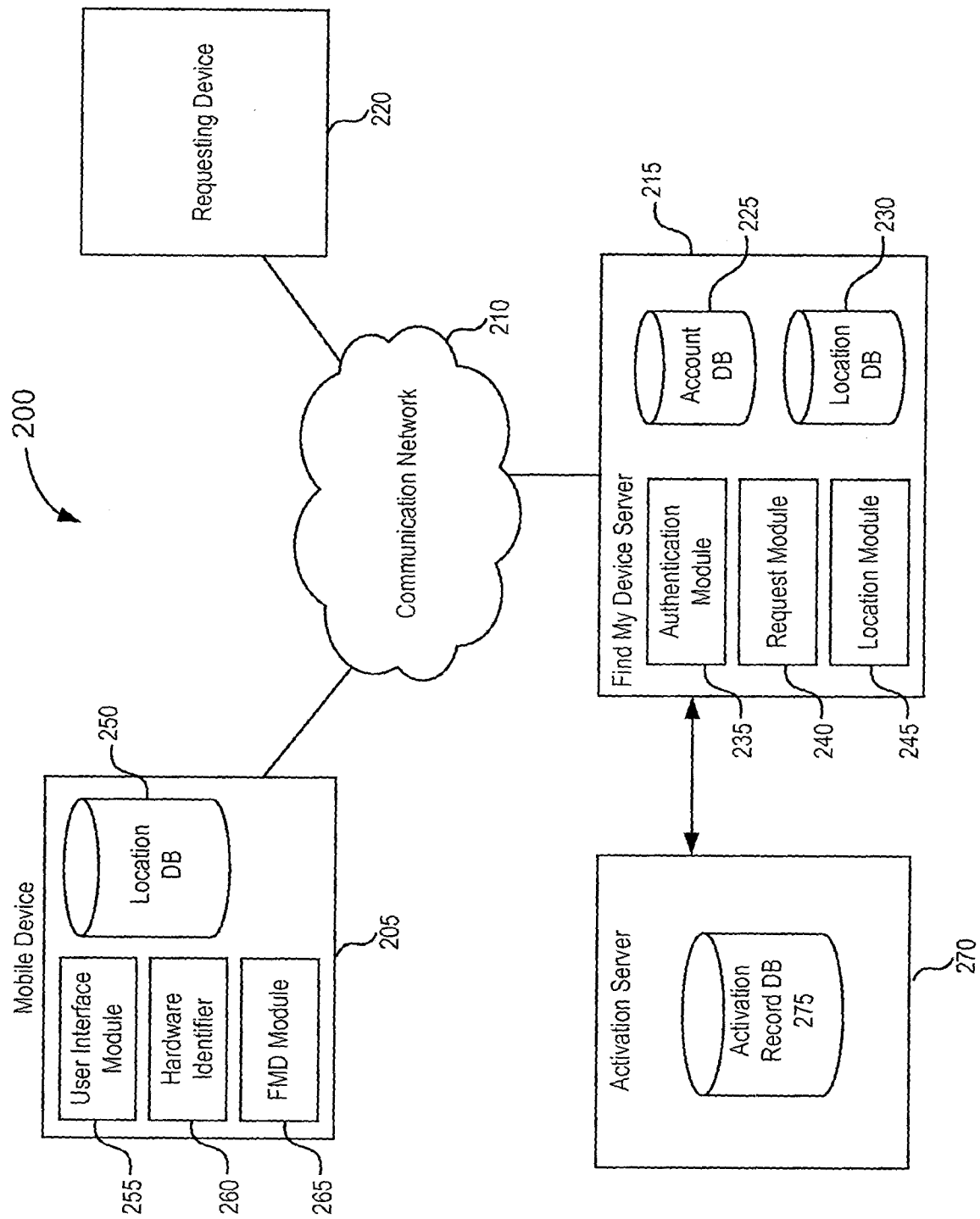
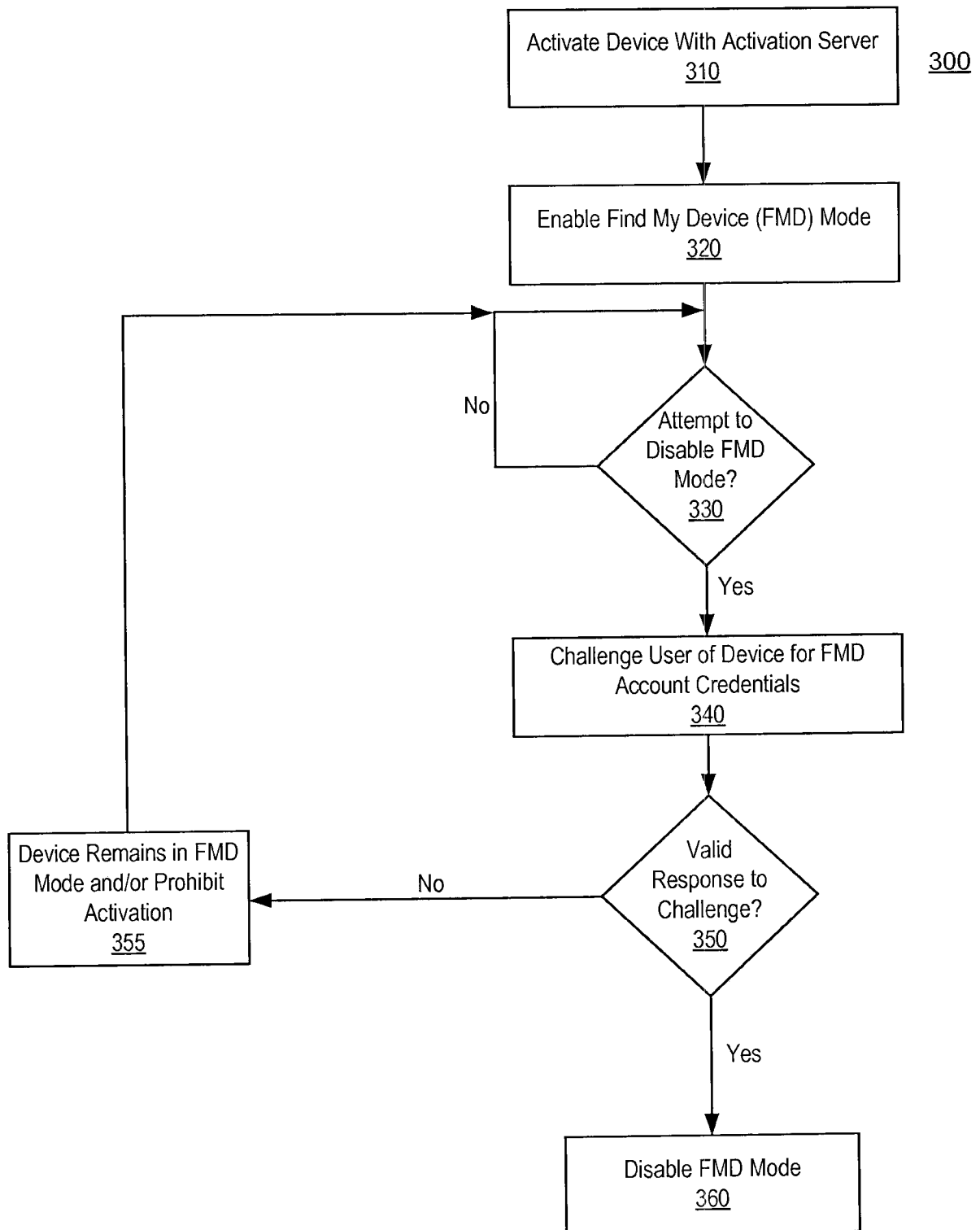
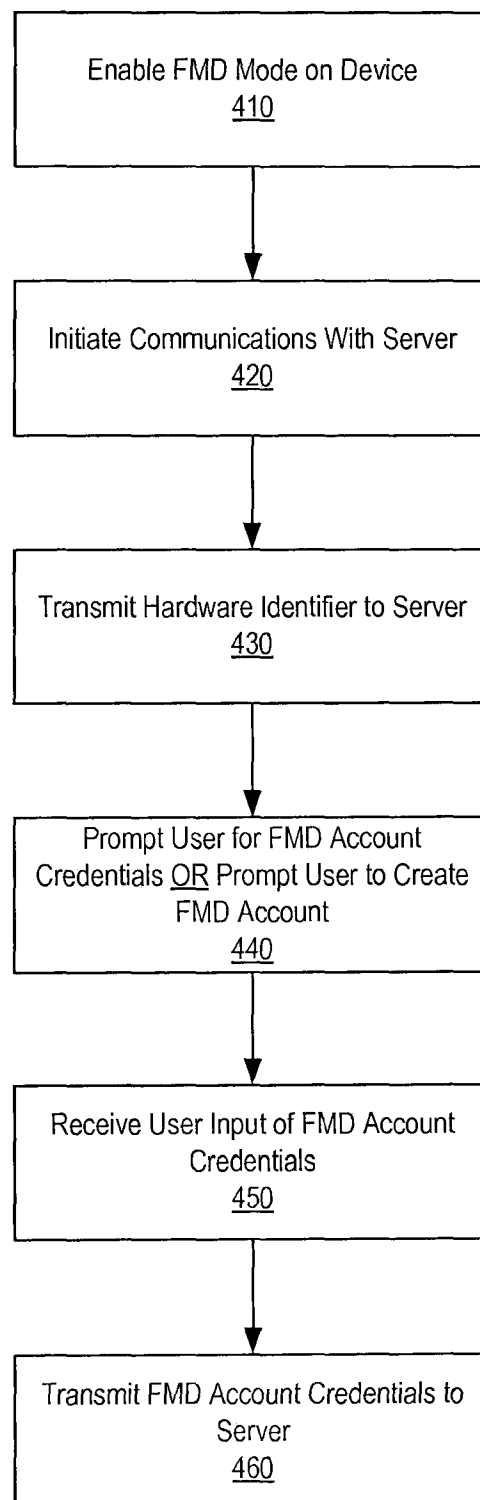


FIG. 2

3/14

**FIG. 3**

4/14

400**FIG. 4**

500

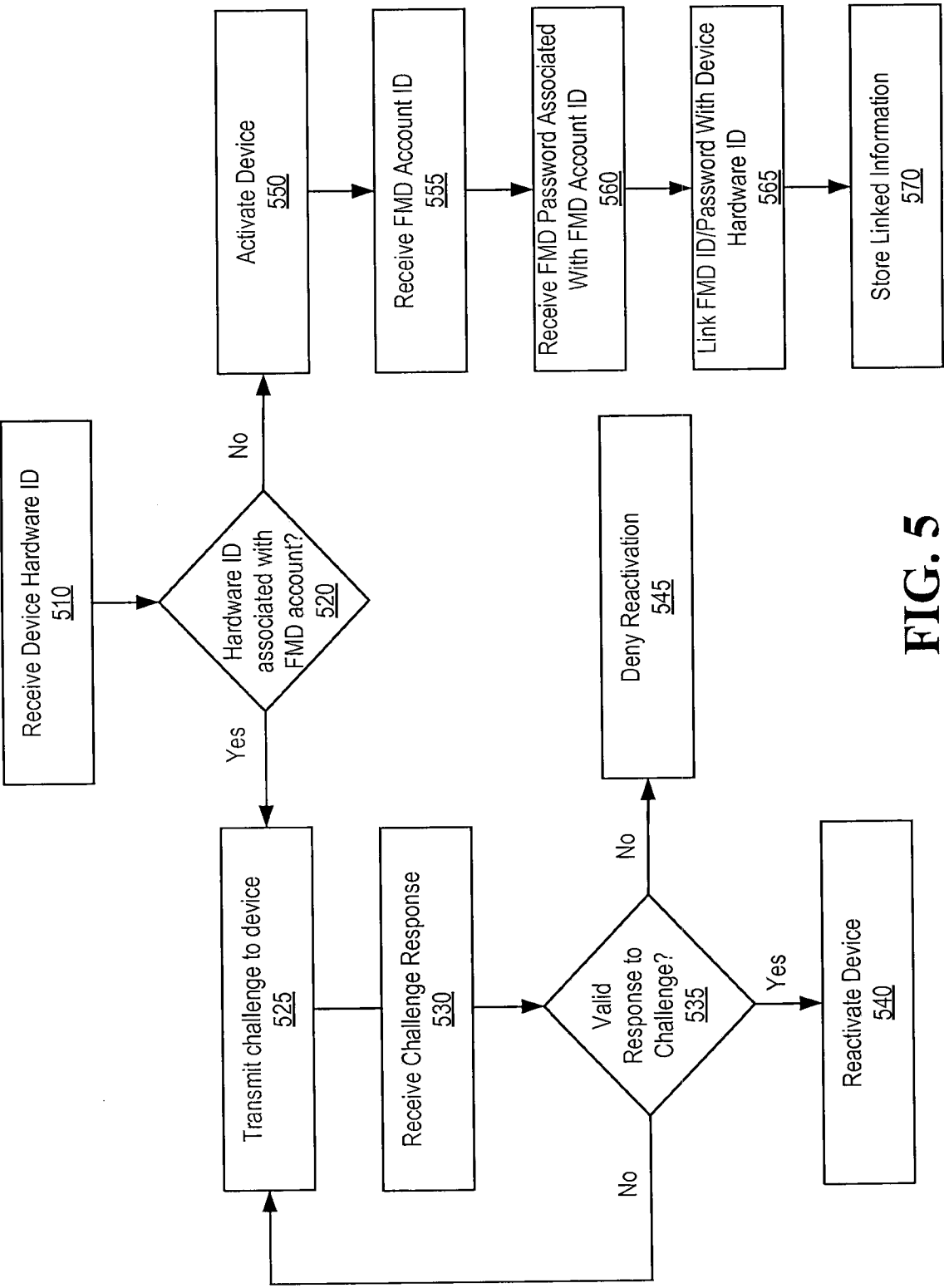
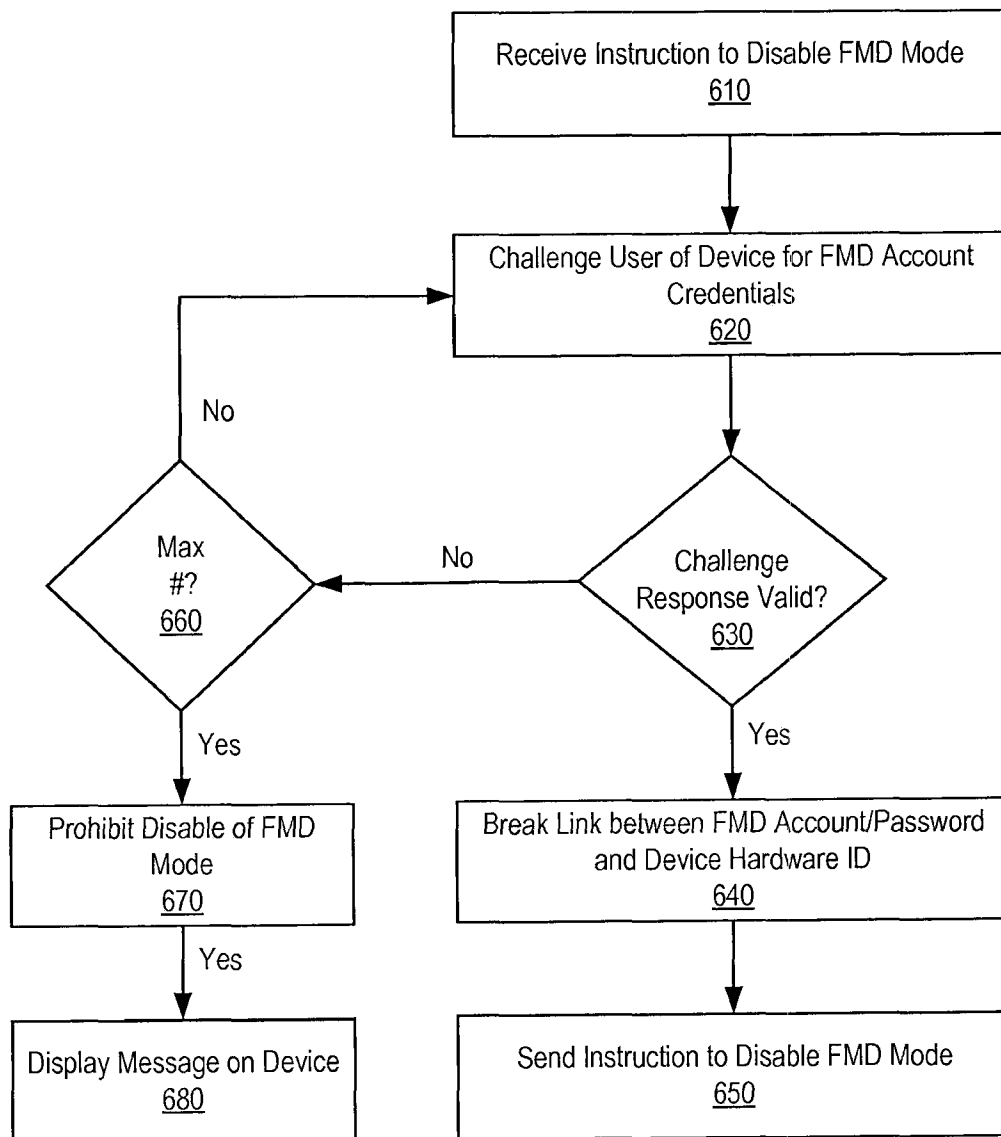
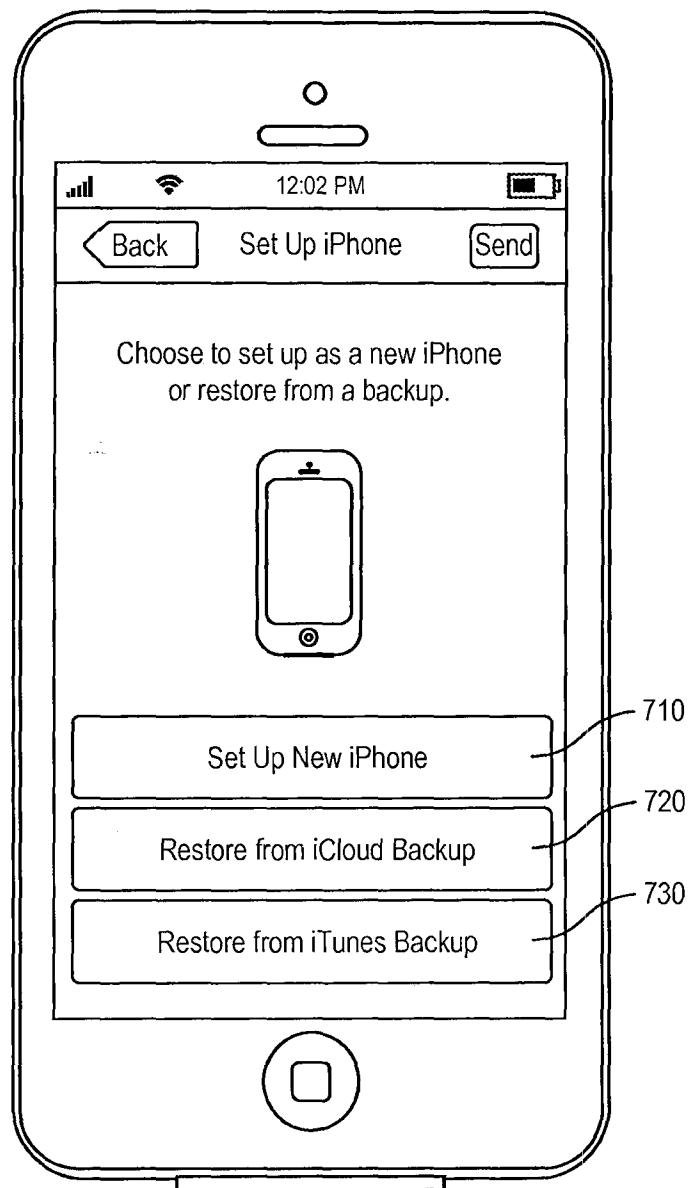


FIG. 5

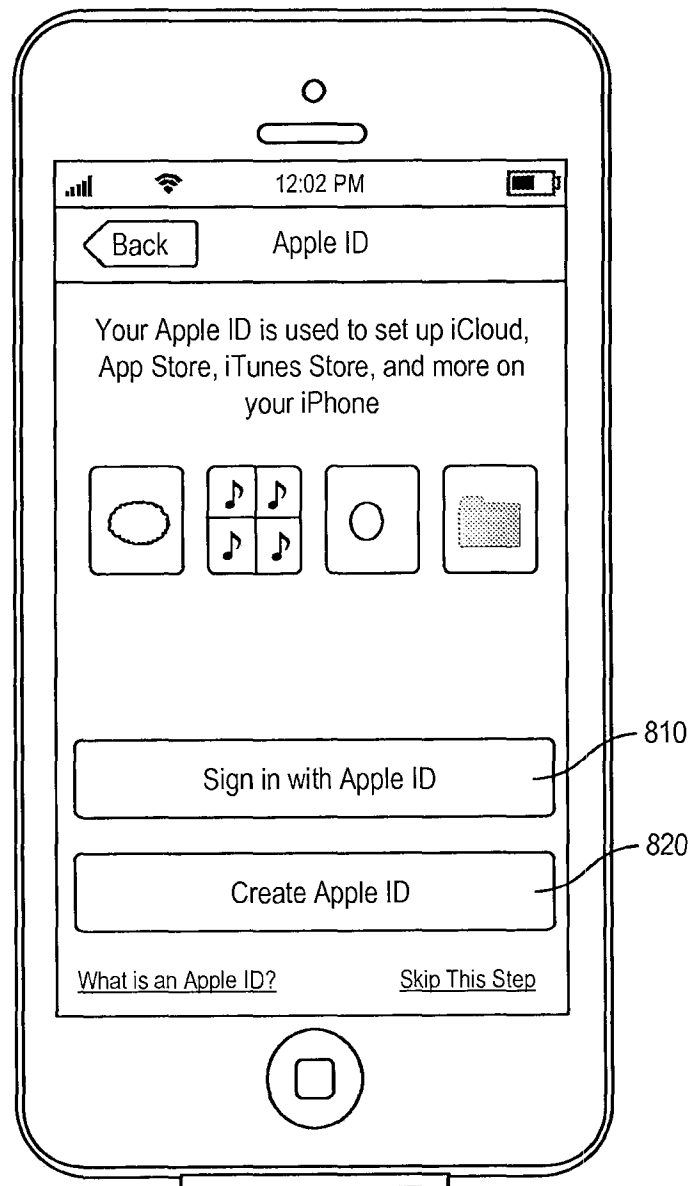
6/14

600**FIG. 6**

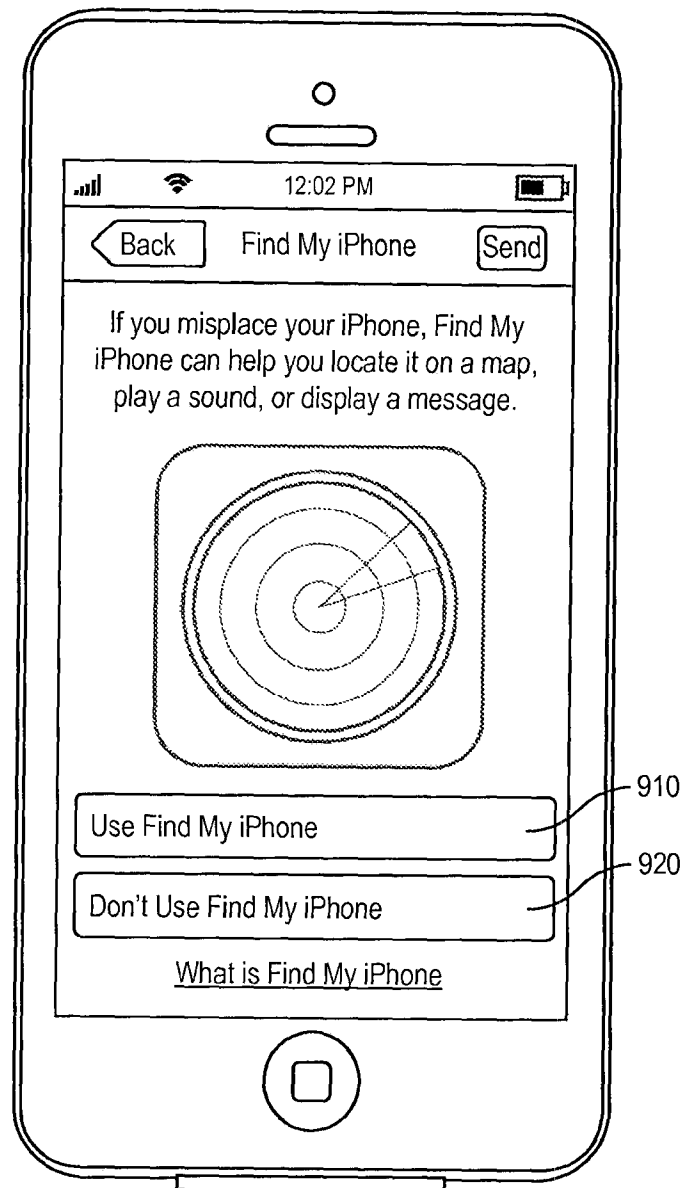
7/14

**FIG. 7**

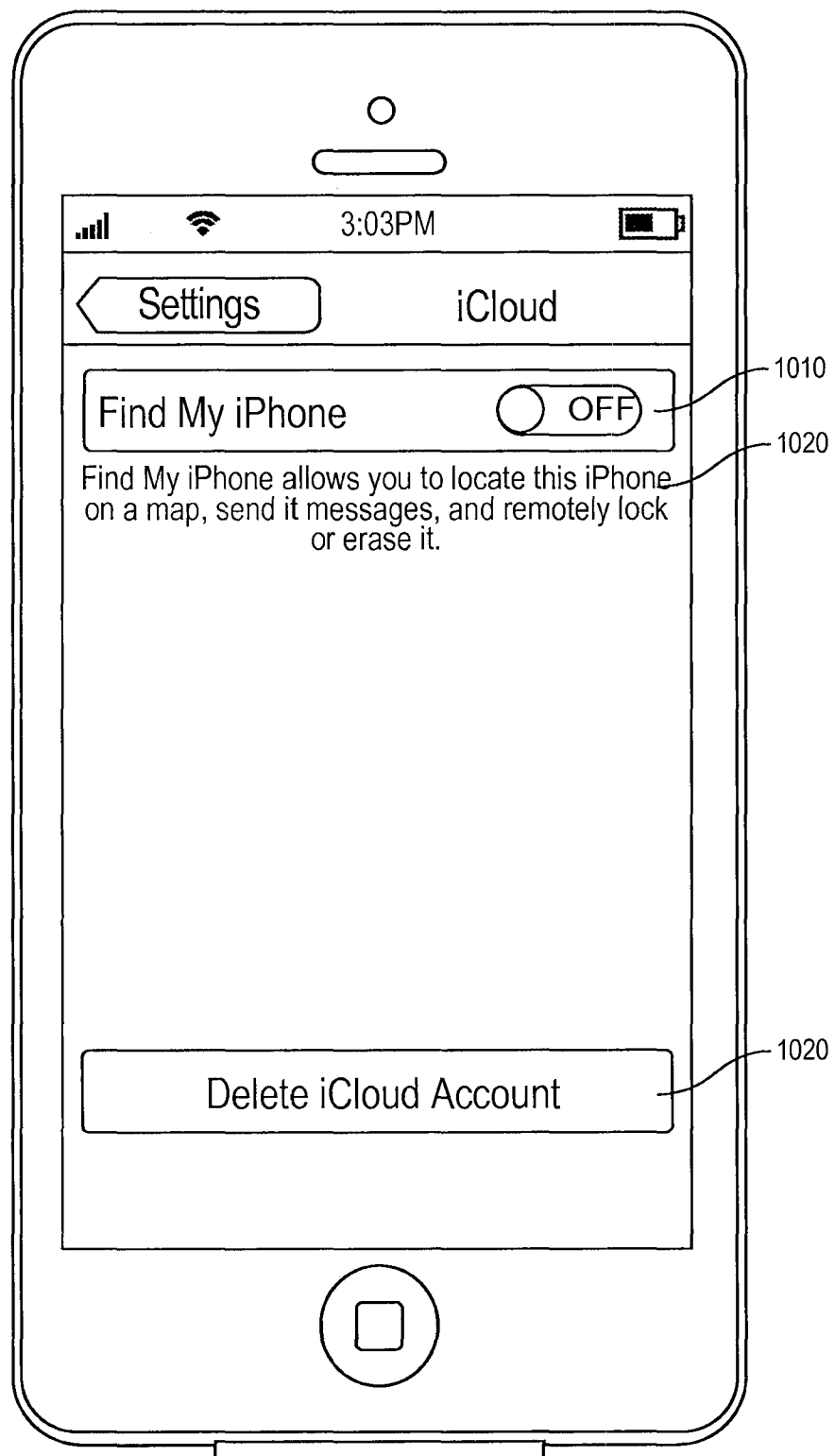
8/14

**FIG. 8**

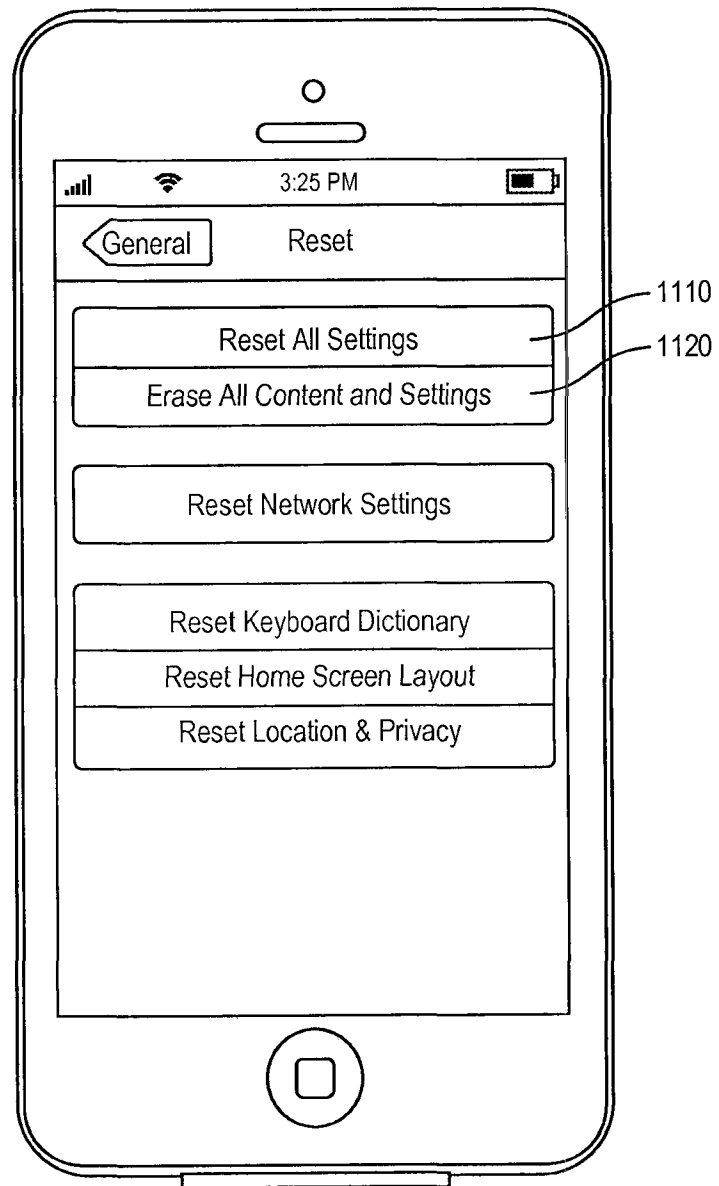
9/14

**FIG. 9**

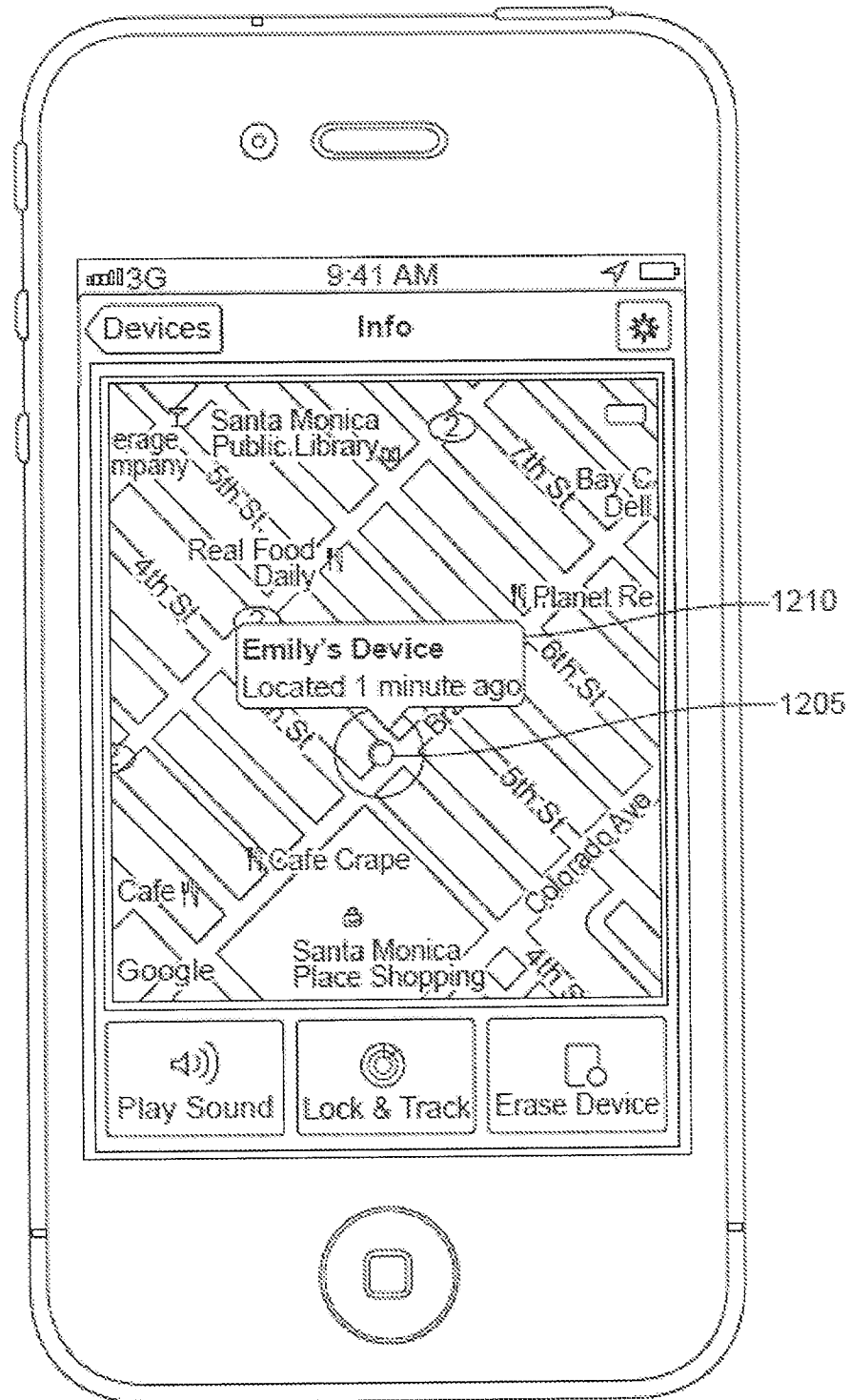
10/14

**FIG. 10**

11/14

**FIG. 11**

12/14

**FIG. 12**

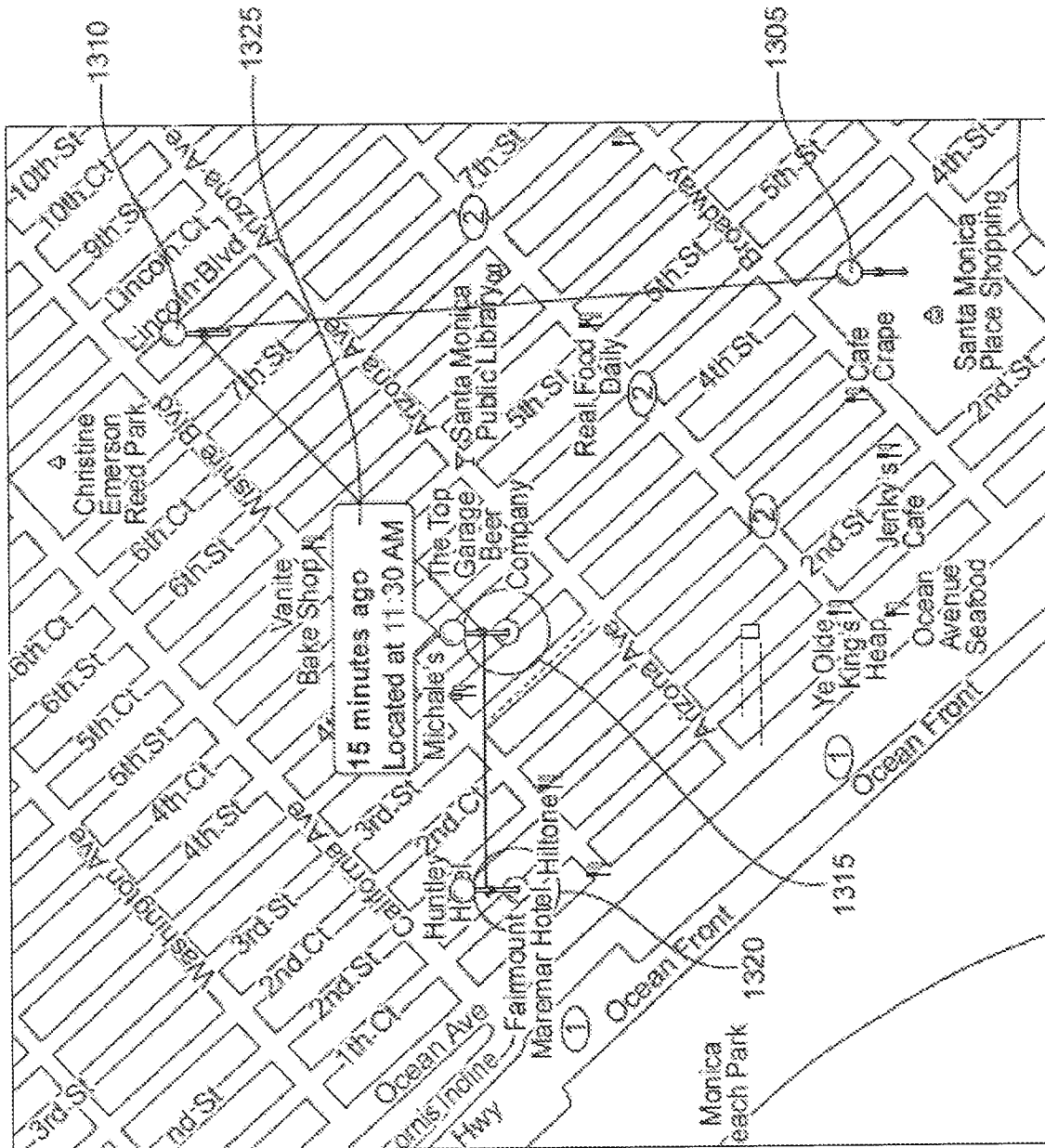


FIG. 13

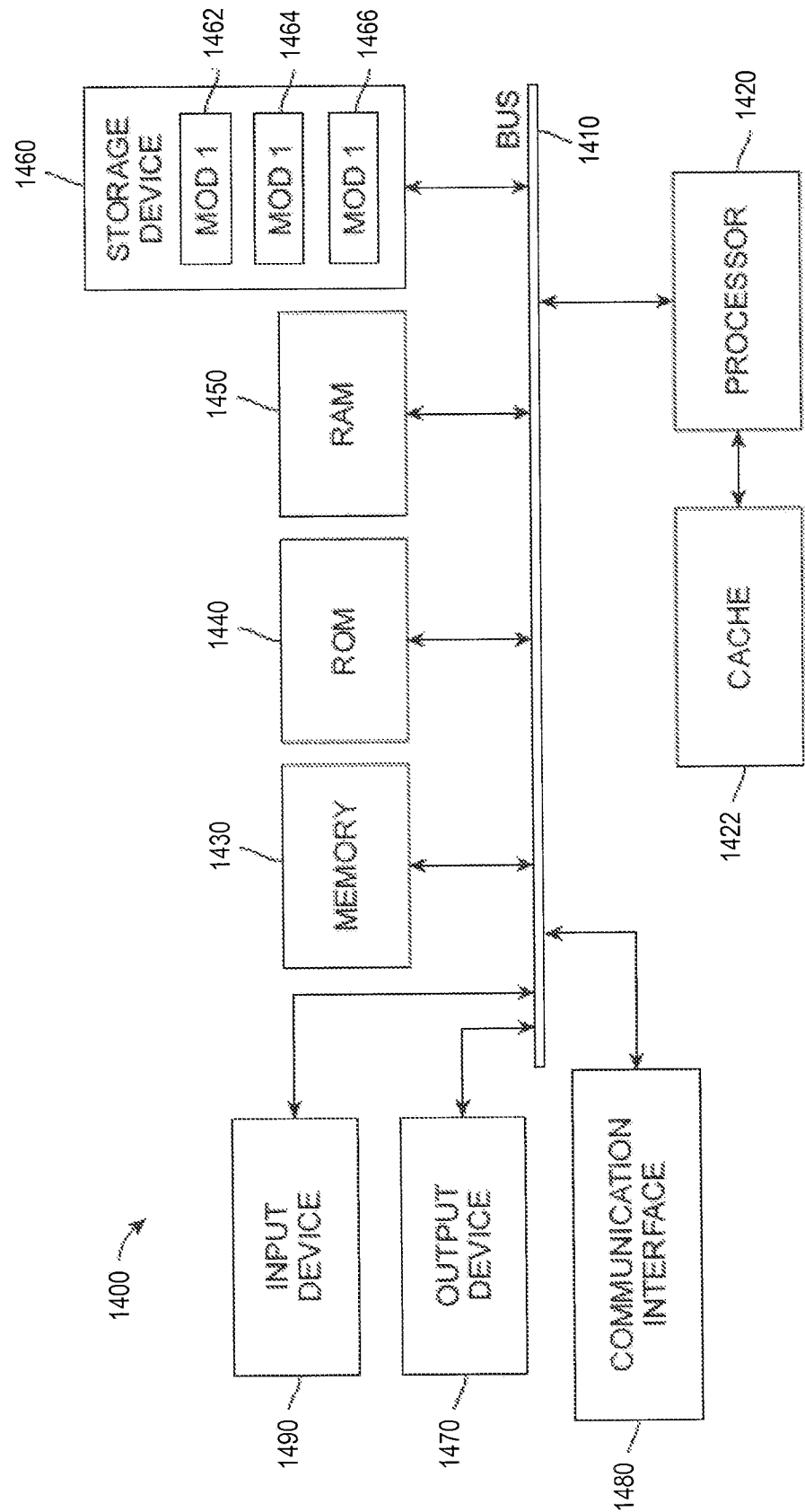


FIG. 14

INTERNATIONAL SEARCH REPORT

International application No

PCT/US2014/040275

A. CLASSIFICATION OF SUBJECT MATTER

INV. G06F9/445 G06F21/88
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F H04W

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, WPI Data, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2013/072774 A2 (YOUGETITBACK LTD [IE]; FITZGERALD WILLIAM [IE]; LYNN WILLIAM [IE]; BER) 23 May 2013 (2013-05-23) paragraph [0024] - paragraph [0028] paragraph [0061] - paragraph [0064] paragraph [0073] paragraph [0079] - paragraph [0086] paragraph [0090] - paragraph [0091] paragraph [0114] paragraph [0128] figures 1,6,8-10 -----	1-20
X	US 8 370 168 B1 (JENKINS JONATHAN A [US] ET AL) 5 February 2013 (2013-02-05) column 1, line 56 - column 2, line 38 column 4, line 28 - column 5, line 3 column 6, line 49 - column 7, line 19 column 10, line 34 - line 67 figures 1,3,5A,6A-6B -----	1-20



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

5 September 2014

Date of mailing of the international search report

15/09/2014

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Milasinovic, Goran

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/US2014/040275

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2013072774	A2	23-05-2013	CA 2855917 A1 23-05-2013
			EP 2780900 A2 24-09-2014
			WO 2013072774 A2 23-05-2013

US 8370168	B1	05-02-2013	NONE
