

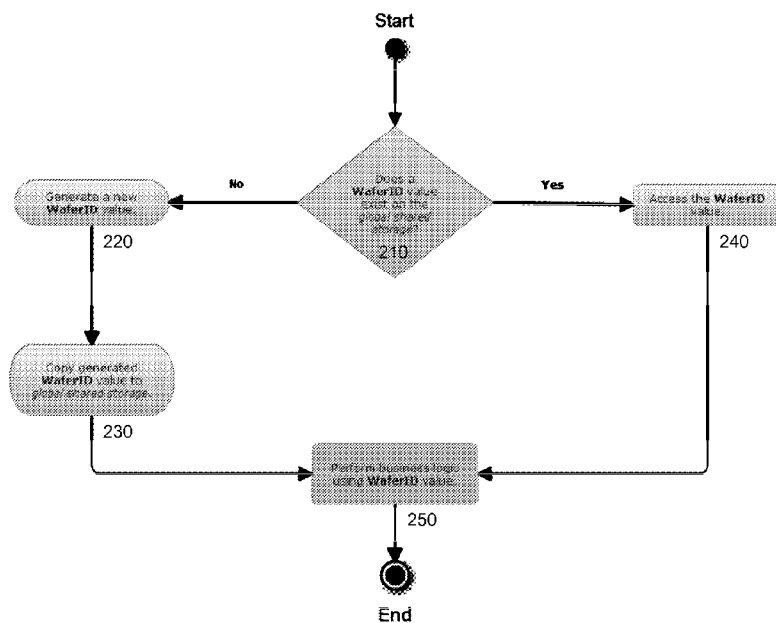


- (51) **International Patent Classification:**
G06F 21/57 (2013.01) *G06F 21/53* (2013.01)
- (21) **International Application Number:**
PCT/US2013/033357
- (22) **International Filing Date:**
21 March 2013 (21.03.2013)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
61/614,475 22 March 2012 (22.03.2012) US
13/831,085 14 March 2013 (14.03.2013) US
- (71) **Applicant (for all designated States except US):** **THE 41ST PARAMETER, INC.** [US/US]; 17851 North 85th Street, Scottsdale, AZ 85255 (US).
- (72) **Inventors; and**
- (71) **Applicants (for US only):** **EISEN, Ori** [US/US]; 6214 E. Hillery Drive, Scottsdale, AZ 85254 (US). **YALOV, Raz** [IL/US]; 14362 N. 98th Place, Scottsdale, AZ 85260 (US).
- (74) **Agents:** **KIM, Elaine** et al.; Wilson Sonsini Goodrich & Rosati, 650 Page Mill Road, Palo Alto, CA 94304-1050 (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, IS, JP, KE, KG, KM, 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, 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, ML, MR, NE, SN, TD, TG).

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

(54) **Title:** METHODS AND SYSTEMS FOR PERSISTENT CROSS-APPLICATION MOBILE DEVICE IDENTIFICATION



(57) **Abstract:** Systems and methods are provided for persistent cross-application mobile device identification. A mobile device may have a plurality of sandboxes in memory containing applications. The mobile device may have a shared storage which may be accessible by applications from different sandboxes. A storage location identifier may be used to access information in shared storage. A universal device identifier may be stored in the shared storage to identify the mobile device and may be accessible by multiple applications and updates to applications. The universal device identifier may be used to track the mobile device for advertising, fraud detection, reputation tracking, or other purposes.



METHODS AND SYSTEMS FOR PERSISTENT CROSS-APPLICATION MOBILE DEVICE IDENTIFICATION

CROSS-REFERENCE

[0001] This application claims the benefit of U.S. Provisional Patent Application Serial No. 61/614,475, filed March 22, 2012, and U.S. Patent Application Serial No. 13/831,085, filed March 14, 2013, each of which is incorporated herein by reference in its entirety.

BACKGROUND OF THE INVENTION

[0002] As the use of networked mobile devices grows, there is a general need for service providers and other third parties to be able to reliably and accurately track the usage patterns of a mobile device. For example, in connection with certain fraud detection methods, it is important to be able to identify the source device used to commit a fraudulent transaction in order to limit future potential fraudulent transactions from the same device. As another example, many advertising and marketing programs must accurately identify the mobile device from which various disparate activities and actions are taken.

[0003] Such systems and processes rely upon the ability to consistently and accurately identify the mobile device utilized for participating in such activities. Typically, in order to track various user activities, an application or a service provider may generate a service-specific identifier for each unique user of the application or service. The application will generally include such service-specific identifier along with each request from the mobile device made to the service in order for the service to accurately identify the originating user or mobile device.

[0004] The mobile device may be capable of storing and executing multiple applications on the same device, including applications that are developed by third parties. Such third parties may be untrusted or even unknown to the user of the mobile device, and the applications generated thereby may be capable of interfering with other applications executing on the mobile device. For this reason, some mobile device operating systems create a "sandbox" environment for each active application by which the memory, storage and other resources made available to one application are isolated from the memory, storage and resources made available to any other application.

[0005] Accordingly, if an application generates and stores a service-specific identifier on an iOS-enabled device, the identifier is stored in the application's "sandbox" environment and no other application on the iOS-enabled device may access or use such identifier. As a result, the service-specific identifier is effective only for use by the specific service that generates it, but is not otherwise effective in uniquely identifying the mobile device itself. Further, each application on the mobile device is required to generate and store its own service-specific identifier, which will differ from the identifier utilized by every other application on the same mobile device. Accordingly, there is no reliable process or system for the mobile device itself to be accurately identified and tracked across a plurality of applications and users on the same mobile device.

[0006] Thus, a need exists to overcome the service-to-service or application-to-application variances in mobile device identification, and thereby provide a persistent cross-application mobile device identification process and system.

SUMMARY OF THE INVENTION

[0007] An aspect of the invention is directed to a method for identifying a mobile device, comprising: determining, with aid of a processor, whether a universal device identifier of the mobile device exists on the mobile device; generating the universal device identifier to identify the mobile device in response to a determination that the universal device identifier does not exist on the mobile device; storing the universal device identifier in a persistent shared storage on the mobile device; retrieving the universal device identifier from the persistent shared storage; and making available the identifier to a plurality of applications installed on the mobile device.

[0008] A system for identifying a mobile device may be provided in accordance with an aspect of the invention, said system comprising: a memory having (a) a plurality of application sandboxes, an individual sandbox having at least one application therein, and (b) a shared storage; and a processor capable of executing steps defined by the plurality of applications, wherein the applications are capable of accessing information within the shared storage via a storage location identifier, and the applications are not capable of accessing information from other sandboxes.

[0009] Another aspect of the invention is directed to a method of identifying a mobile device, comprising: providing a memory having (a) a plurality of application sandboxes, an individual sandbox having at least one application therein, and (b) a shared storage; providing a processor capable of executing steps defined by the plurality of applications;

permitting the applications to access information within the shared storage via a storage location identifier, while not permitting the applications to access information from other sandboxes, wherein the information within the shared storage accessed by the applications includes a universal device identifier; and performing advertisement tracking of the mobile device using the universal device identifier.

[0010] Other goals and advantages of the invention will be further appreciated and understood when considered in conjunction with the following description and accompanying drawings. While the following description may contain specific details describing particular embodiments of the invention, this should not be construed as limitations to the scope of the invention but rather as an exemplification of preferable embodiments. For each aspect of the invention, many variations are possible as suggested herein that are known to those of ordinary skill in the art. A variety of changes and modifications can be made within the scope of the invention without departing from the spirit thereof.

INCORPORATION BY REFERENCE

[0011] All publications, patents, and patent applications mentioned in this specification are herein incorporated by reference to the same extent as if each individual publication, patent, or patent application was specifically and individually indicated to be incorporated by reference.

BRIEF DESCRIPTION OF THE DRAWINGS

[0012] The novel features of the invention are set forth with particularity in the appended claims. A better understanding of the features and advantages of the present invention will be obtained by reference to the following detailed description that sets forth illustrative embodiments, in which the principles of the invention are utilized, and the accompanying drawings of which:

[0013] Figure 1 illustrates a mobile device system for generating, storing, and using a persistent mobile device identifier that incorporates concepts of the invention.

[0014] Figure 2 illustrates a process for generating, storing, and using a persistent mobile device identifier that incorporates concepts of the invention.

[0015] Figure 3 shows an identification system utilizing persistent device identifiers in accordance with an embodiment of the invention.

DETAILED DESCRIPTION OF THE INVENTION

[0016] While preferable embodiments of the invention have been shown and described herein, it will be obvious to those skilled in the art that such embodiments are provided by way of example only. Numerous variations, changes, and substitutions will now occur to those skilled in the art without departing from the invention. It should be understood that various alternatives to the embodiments of the invention described herein may be employed in practicing the invention.

[0017] The invention provides systems and methods for identifying mobile devices by a persistent cross-application identifier. Various aspects of the invention described herein may be applied to any of the particular applications set forth below. It shall be understood that different aspects of the invention can be appreciated individually, collectively, or in combination with each other.

[0018] It shall be understood that this invention is addressed to mobile device functionality. The mobile devices may include phones such as cellular phones, smartphones (e.g., iPhone, BlackBerry, Android, Treo); tablets (e.g., iPad, Galaxy Tab, Kindle Fire, Surface); a wireless device such as a wireless email device; certain network devices such a tablet; personal digital assistants (PDAs) such as a Palm-based device or Windows CE device; other devices capable of communicating wirelessly with a computer network or other communication network; or any other type of mobile device that may communicate over a network and handle electronic transactions. A mobile device may be handheld. A mobile device may use specialized programs or applications. Any discussion herein of devices may also be applied to any other mobile devices as provided.

[0019] As illustrated in Figure 1, the mobile device 100 may have a processor 110 and a memory 120 that may store an operating system (OS) 125 and a plurality of applications or “apps” 130a, 130b, 130c. The memory may be capable of storing non-transitory computer readable media comprising code, logic, or instructions to perform one or more steps, such as steps of the apps. A processor may be capable of executing the one or more steps defined by the non-transitory computer readable media. The operating system may operate to display a graphical user interface to the user and permit the user to execute one or more apps. Any display known in the art may be used including, but not limited to, a liquid crystal display, a plasma screen, a touchscreen, an LED screen, or an OLED display. The processor may be capable of executing one or more steps of the methods provided herein to identify mobile devices by a persistent cross-application

unique identifier. The applications may be native functionality incorporated into the OS of the mobile device or may be third party applications installed by the manufacturer, carrier network, or user of the mobile device.

[0020] It shall be understood that the memory of the mobile device may include non-removable memory or removable memory. The non-removable memory may consist of RAM, ROM, a hard disk, or other well-known memory storage technologies. The removable memory may consist of Subscriber Identity Module (SIM) cards, which are well known in GSM communication systems, or other well-known memory storage technologies, such as “smart cards.” Applications could be installed and/or implemented in either the removable memory or the non-removable memory. Memory may include volatile and non-volatile memory. Volatile memory may include memory that requires power to retain information. Non-volatile memory may include memory that can retain information, even when it is not powered, such as include read-only memory, flash memory, ferroelectric RAM (F-RAM), most types of magnetic computer storage devices (e.g. hard disks, floppy disks, and magnetic tape), and/or optical discs.

[0021] It shall be understood that the mobile devices may have one or more software applications (apps) 130a, 130b, 130c to carry out instructions. In some instances, one or more of the apps may generate an identifier 140 (e.g., device identifier, WaferID) and store a WaferID in shared storage 150. One or more steps of the application may be implemented by non-transitory and/or tangible computer readable media which may contain instructions, logic, data, or code that may be stored in persistent or temporary memory of the mobile device, or may somehow affect or initiate action by the computer or other device. In some embodiments, only some applications have instructions to generate, store or retrieve a device identifier from a shared storage. In some embodiments, all applications on the mobile device have instructions to generate, store or retrieve a device identifier from a shared storage.

[0022] As illustrated in Figure 1, one or more of the applications installed on the mobile device may be restricted in its operations to a “sandbox” environment. A sandbox 135a, 135b 135c is a secure memory space on the mobile device in which such applications 130a, 130b, 130c are confined and prevented from accessing certain data 137a, 137b, 137c and resources. For example, some sandbox restrictions may prevent an application from accessing certain system resources and data such as critical system files. Applications may be capable of accessing data and resources within the same sandbox as

the application. In some instances, applications are not capable of accessing data and resources in other sandboxes. Optionally, only one application is provided per sandbox. In other instances, multiple applications may be provided within the same sandbox if the applications are created, distributed, and/or operated by the same party. Alternatively, multiple applications may be provided within the same sandbox even they are not created, distributed and/or operated by the same party. As further example, some sandbox restrictions may prevent an application from accessing the data or resources created and used by another application on the same mobile device. For example, an application 130a in a first sandbox 135a may only be able to access data and resources 137a within the same sandbox, and may not be able to access data or resources 137b, 137c in other sandboxes 135b, 135c.

[0023] Confinement to a sandbox prevents applications from carrying out potentially dangerous or malicious operations on the mobile device. In some cases, the mobile device OS 125 may manage the sandbox and determine the resources that an application is prevented from accessing. For example, the Apple iOS operating system (used, for example, on Apple iPhone mobile phones, Apple iPad tablets and other mobile devices) isolates each application of the mobile device, including its respective data and preferences information, from other applications. The iOS operating system installs each application in its own application-specific storage directory and restricts the application from saving or accessing any application data that is stored external to the application-specific storage directory.

[0024] In accordance with the invention, as illustrated in Figure 1, the mobile device may include a global, persistent shared storage 150 accessible by one or more applications 130a, 130b, 130c on the mobile device. In some instances, any of the applications may be able to access the shared storage, regardless of which sandbox within which they reside. The shared storage provides applications with data and information storage that is external to the application's sandbox environment on the mobile device. The shared storage may be implemented using removable or non-removable non-transitory memory on the mobile device. In some embodiments, the shared storage is made available to two or more applications on the same mobile device such that each of the applications may have permission to read data from and write data to the same memory location within the shared storage (i.e., "share" the memory). Accordingly, the shared storage provides a space for two or more applications to share data or information between the applications

without violating the application's sandbox environment restriction on storing or accessing data from outside the application-specific storage directory.

[0025] The shared storage 150 may provide one or more of the following persistence characteristics for the information stored in the shared storage: (i) the information persists across a reboot or restart of the mobile device, (ii) the information persists across applications, (iii) the information persists across updated versions of applications, and/or (iv) the information persists across updated versions of the mobile device OS. It shall be understood that the shared storage may provide more than one of the persistence characteristics set forth above and may provide other persistence characteristics. The shared storage may be provided in non-volatile memory, such as ROM or any others described herein.

[0026] In accordance with the invention, the use of the shared storage 150 is controlled by a shared storage manager (SSM) 155. The SSM provides an interface and exposes the functionality necessary for applications, firmware or the mobile device OS 125 to interact with the shared storage. Accordingly, the SSM controls one or more applications' 130a, 130b, 130c access to the shared storage. In some embodiments, the mobile device OS may implement the SSM directly. For example, the Apple iOS system includes "pasteboard" functionality that can be used by applications to persistently store and share certain types of data for use by the application or between applications. In some embodiments, the SSM may restrict the types of information or data that may be stored in or retrieved from the shared storage. For example, the SSM may prevent executable code from being stored in the shared storage in order to restrict applications from performing potentially harmful activities that could interfere with the functionality of another application on the mobile device. As another example, the SSM may permit only text strings to be stored to and retrieved from the shared storage.

[0027] The SSM 155 provides access to specific information of the shared storage 150 by the use of a storage location identifier. One or more applications may retrieve shared data or information by requesting access from the SSM to the data or information at a specific shared storage location. In some embodiments, the storage location identifier may be an alphanumeric key that maps to a value located at a specific storage location and that identifies a specific piece of information. Any application may be able to access the information located at a specific storage location by use of the storage location identifier, regardless of the sandbox to which the application belongs. For example, an

application (e.g., App1) 130a may utilize the SSM to store application preferences data at the shared storage location identified by the key "Application1.Preferences" (which may function as the storage location identifier). Subsequently, a different application (e.g., App2) 130b may retrieve the preferences data of App1 by requesting from the SSM the data located at the shared storage location identified by the key "Application1.Preferences". Thus, applications may be able to access the same data or resources stored in a shared storage, via the storage location identifier, regardless of whether the applications are in the same or different sandboxes.

[0028] It shall be understood that the storage location identifier key may be any alphanumeric string and that each unique key shall map to a discrete piece of data or information stored in the shared storage. In some instances, the storage location identifier may have any other form that may uniquely identify or index the information in the shared storage.

[0029] Another aspect of the invention is directed to generating a persistent, universal device identifier (UDID) for a mobile device 100, referred to herein as a "WaferID" 140. Embodiments of the invention generate and maintain a WaferID for every mobile device. The WaferID uniquely identifies a mobile device in the context of an online service, a mobile device application, or other third party services. The WaferID is an identifier generated on the mobile device and can be separate from any system identifier that is pre-loaded by the mobile device OS, the mobile device manufacturer, or a network carrier. In some embodiments, only a single unique WaferID is generated for the mobile device. One or more applications and/or services may make use of the WaferID in identifying the device. In some embodiments, more than one WaferID may be generated for the mobile device such that a subset of applications and services on the mobile device can make use of the same WaferID in order to uniquely identify the mobile device.

[0030] The WaferID may be an alphanumeric string of any length and that is unique within the context of use for every mobile device. The WaferID may have any other form that may permit the unique identification of the mobile device. The WaferID is intended to be persistent and can typically survive a change in the carrier network, operating system, user and other variables associated with a mobile device. In some instances, the WaferID is only deleted upon request of a user or application. In some embodiments, the WaferID is generated by a process on the mobile device. It shall be understood that a variety of methods are known for generating an alphanumeric string that is unique for a

mobile device. For example, the WaferID may be generated by any of a number of known algorithms for generating a random or pseudo-random string. In some embodiments, the algorithm may be seeded with a date or time to produce a unique WaferID.

[0031] The WaferID 140 for a mobile device may be stored in shared storage 150 of the mobile device. The WaferID may be a data or resource stored in the shared storage. The WaferID may be accessible via a storage location identifier. Thus, one or multiple applications may access the WaferID via the storage location identifier. This may occur if the applications are in the same sandbox, or in multiple sandboxes. Thus, multiple applications that may have been created, distributed, or operated by different applications may make use of the same WaferID, which may function as the device ID. This may be useful when multiple applications want to share information about the device.

[0032] Thus, one or more applications on the same mobile device may share the same WaferID through the use of the shared storage. In some embodiments, any application on the mobile device may request access to the WaferID associated with the mobile device. One or more applications of the same mobile device may share data in the shared storage of the mobile device, which may or may not be associated with the WaferID.

[0033] Figure 2 provides an example of a process for generating, storing, and using a persistent mobile device identifier (e.g., WaferID). An application of a mobile device may request access to a WaferID of the mobile device. A determination may be made whether a WaferID value exists in the shared storage 210. In some instances, a WaferID may be a universal device identifier (UDID), and a determination may be made whether a universal device identifier of a mobile device exists on the mobile device. As illustrated in Figure 2, if no WaferID exists in the shared storage, a new WaferID is generated and associated with the mobile device 220. In some embodiments, the first application requesting a WaferID will trigger the generation of a new WaferID on the mobile device. In some embodiments, the WaferID may be generated by the mobile device OS automatically upon initialization of the mobile device for the first time. In some embodiments, the WaferID may be generated by a firmware process associated with a component of the mobile device.

[0034] As further illustrated in Figure 2, the generated WaferID is stored in the shared storage. In accordance with the invention, the WaferID is stored the shared storage 230 using a storage location identifier known by the one or more applications that will share

the WaferID. In some embodiments, the WaferID may be stored in a generally-known location, such as through the use of a well-advertised key as the storage location identifier. In some embodiments, the WaferID may be stored in shared storage using a non-obvious key as the storage location identifier, such as through the use of a key that is not publicly advertised. An application that knows the respective key may retrieve the WaferID from the shared storage location mapped to such key. In some instances, multiple applications may know the respective key, regardless of where in memory (e.g., which sandbox) the applications reside.

[0035] In some embodiments, the method and system disclosed herein may be associated with an application programming interface (API) or with a software development kit (SDK) that allows third parties to easily incorporate the functionality for generating, storing and using the WaferID. In other embodiments, the invention may be associated with the mobile device OS or with firmware associated with components of the mobile device.

[0036] If a WaferID already does exist in shared storage 240 the WaferID value is accessed. A storage location identifier may be used to access the WaferID.

[0037] As indicated in Figure 2, the cross-application WaferID disclosed in this invention may be used in connection with business logic in order to identify a mobile device across applications, user contexts, and discrete user requests 250.

[0038] In some aspects of the invention, the WaferID may be used to maintain a record of activities connected to a specific mobile device. In one embodiment, the WaferID may be used for analytics purposes in connection with monitoring advertisement activities. It shall be understood that any known process in the art for providing in-application advertisements on a mobile device may be enhanced to use the WaferID. The use of the WaferID in connection with providing advertisements may allow an advertiser to understand usage patterns of the mobile device user across applications. For example, an advertiser may be able to track which advertisements are displayed to a specific mobile device regardless of which application is activated at the time the advertisement is displayed. The data from mobile device exposure to advertisements may be used to generate reports and for other analytics purposes.

[0039] In some embodiments, the WaferID may be used in connection with fraud detection and prevention methodologies. For example, a fraud detection and prevention

system may identify a potential attacker or threat based on the WaferID associated with such attacker's device.

[0040] It may be advantageous for the WaferID to be accessible by multiple applications of a mobile device. For example, one or more entity may wish to share advertising or fraud information. In some instances, one or more applications may wish to access the same advertising or fraud information, regardless of whether they belong to the same entity or different entities. Reputational information may be carried across information. Reputational information may include bad reputation for a user or device (e.g., if likely involved in fraud), or good reputation for a user or device (e.g., if the user or device has a history without any problems). A persistent WaferID may permit multiple applications to access the unique device identifier, which may permit information about the device to be tracked across the different applications. Other data may be stored on the shared storage and be accessible by various applications. Such other data may or may not also be useful for advertisement, fraud, or reputation purposes.

[0041] Any of the steps described herein may occur with aid of a processor. The processor may be a processor of the mobile device.

[0042] Figure 3 shows an identification system utilizing persistent device identifiers in accordance with an embodiment of the invention. One or more mobile devices 310a, 310b, 310c may be communicating over a network 330 with one or more server or storage device 340a, 340b. Any depiction of a single server may apply to multiple servers and/or databases. The servers and/or databases may be separate devices or may be integrated into a single device. The server and/or databases may belong to the same entity or different entities. The mobile devices may have one or more applications thereon, which may communicate with respective servers and/or databases.

[0043] An identification system may include a single device or a plurality of devices 310a, 310b, 310c. In some embodiments, a user may interact with a mobile device. In some instances a user of the system may interact with the system over a network. The user may utilize one or more applications on the mobile device. The user may download applications to the mobile device.

[0044] One or more devices 310a, 310b, 310c may be provided within the system. As previously described, a mobile device may have a display. The display may permit a visual display of information. The display may include a display of a browser and/or application. A viewable area of a canvas on the display may be a viewport. The display

may be provided on a screen, such as an LCD screen, LED screen, OLED screen, CRT screen, plasma screen, touchscreen, e-ink screen or any other type of display device. The devices may also include displays of audio information. The display may show a user interface. A user of the system may interact with the device through a user interface. A user may interact via a user interactive device which may include but is not limited to a keypad, touchscreen, keyboard, mouse, trackball, touchpad, joystick, microphone, camera, motion sensor, IR sensor, heat sensor, electrical sensor, or any other user interactive device. A user may be able to operate and/or interact with an application via the display and/or user interactive device.

[0045] In some embodiments, a plurality of devices may be provided in a system. For example, two or more, 10 or more, 100 or more, 1,000 or more, 10,000 or more, 50,000 or more, 100,000 or more, 500,000 or more, 1,000,000 or more, 5,000,000 or more, 10,000,000 or more, 50,000,000 or more, 100,000,000 or more, or 1,000,000,000 or more devices may be provided. In some embodiments, a pre-selected group of devices may be provided. Devices may be accessing a software or application on one or more server 340a, 340b. Devices may be displaying a browser with content provided through the server. Devices may be capable of operating one or a plurality of applications simultaneously. Devices may be capable of interacting with servers for different entities simultaneously. Devices may be capable of interacting with external devices relating to different applications simultaneously.

[0046] The network 330 may be a local area network (LAN) or wide area network (WAN) such as the Internet. The network may be a personal area network, a telecommunications network such as a telephone network, cell phone network, mobile network, a wireless network, a data-providing network, or any other type of network. The communications may utilize wireless technology, such as Bluetooth or RTM technology. Alternatively, various communication methods may be utilized, such as a dial-up wired connection with a modem, a direct link such as TI, ISDN, or cable line. In some embodiments, a wireless connection may be using exemplary wireless networks such as cellular, satellite, or pager networks, GPRS, or a local data transport system such as Ethernet or token ring over a LAN. In some embodiments, the system may communicate wirelessly using infrared communication components.

[0047] One, two or more servers 340a, 340b may be provided in accordance with an embodiment of the invention. A server may include a memory and/or a processor. The

server may or may not be at a location that is remote to the devices. The server may communicate with the devices over a network. In some instances, a cloud computing infrastructure may be provided. Any functions described herein may be carried out using a cloud computing infrastructure, such as distributed processing and memory functions. In alternate embodiments, peer to peer architectures may be utilized by the system.

[0048] The server may store data relating to a website or application to be displayed on a browser on a user's device. The server may store data or access data relating to an application. The server may be operated by a service that may aggregate and/or analyze information about one or more devices. A server may provide content to the devices via the network. The server may receive information about the devices. In some instances, two-way communication may be provided between the devices and the server.

[0049] The devices 310a, 310b, 310c may have corresponding universal device identifiers (UDIDs) 320a, 320b, 320c. In some embodiments, the universal device identifier for each device may be unique to that device. In some embodiments, universal device identifiers may be a unique string of numbers associated with a device that can let developers of apps track their apps. Or when passed between apps, UDIDs allow ad networks, for example, to build a profile noting user habits and preferences associated with that device, which allows them to more carefully target their ads. A device may have a single universal device identifier. Alternatively, the device may have multiple universal device identifiers. The device identifiers may be accessible by one or more applications of the devices. The device identifiers may be accessible by multiple applications of the devices, even if the applications belong to different sandboxes.

[0050] When communicating with one or more server 340a, 340b that may relate to various applications of the devices, the universal device identifiers 320a, 320b, 320c of the devices 310a, 310b, 310c may be shared. The one or more server may track the universal device identifiers. The one or more servers may access databases and/or memory that may include information relating to the devices associated with the universal device identifiers. Such information may be accessed by servers associated with one or more applications of the device. For example, a first server 340a may relate to a first application of a device 310a and a second server 340b may relate to a second application of the device. A universal device identifier 320a of the device may be accessible by the first and second applications of the device. The universal device identifier may be conveyed to the related servers. In some instances, relevant information about the device

to be accessed by the applications may be stored locally on the device. Alternatively, some or all of the information may be stored off-board (e.g., on the servers).

[0051] In some instances, one or more external devices, such as servers may access information relating to the universal device identifier. For example, external servers may have information stored about a mobile device based on its universal device identifier. In some instances, a plurality of servers related to different applications may have access to information about the mobile device based on its universal identifier. The plurality of servers may each keep their own records about the mobile device or may access the same data repository about the mobile device. The plurality of servers, which may relate to different applications, may share information about the mobile device, or may keep their own records about the mobile device. The servers may be operated by an entity that operates an application of the mobile device. Alternatively, they may be operated by different entities.

[0052] A universal device identifier may service as an index or key through which records about the mobile device may be accessed. This may be useful for keeping track of the mobile device for advertisement, fraud, and/or reputation purposes as described herein.

[0053] It should be understood from the foregoing that, while particular implementations have been illustrated and described, various modifications can be made thereto and are contemplated herein. It is also not intended that the invention be limited by the specific examples provided within the specification. While the invention has been described with reference to the aforementioned specification, the descriptions and illustrations of the preferable embodiments herein are not meant to be construed in a limiting sense. Furthermore, it shall be understood that all aspects of the invention are not limited to the specific depictions, configurations or relative proportions set forth herein which depend upon a variety of conditions and variables. Various modifications in form and detail of the embodiments of the invention will be apparent to a person skilled in the art. It is therefore contemplated that the invention shall also cover any such modifications, variations and equivalents.

CLAIMS

WHAT IS CLAIMED IS:

1. A method for identifying a mobile device, comprising:
 - determining, with aid of a processor, whether a universal device identifier of the mobile device exists on the mobile device;
 - generating the universal device identifier to identify the mobile device in response to a determination that the universal device identifier does not on the mobile device;
 - storing the universal device identifier in a persistent shared storage on the mobile device;
 - retrieving the universal device identifier from the persistent shared storage;and
 - making available the identifier to a plurality of applications installed on the mobile device.
2. The method of claim 1, wherein the plurality of applications installed on the mobile devices belong to different sandboxes in a memory of the device.
3. The method of claim 1, further comprising performing business logic using the universal device identifier.
4. The method of claim 1, further comprising creating a storage location identifier providing access to the universal device identifier in the persistent shared storage.
5. The method of claim 4, wherein retrieving the universal device identifier occurs via the storage location identifier.
6. The method of claim 1, wherein the universal device identifier is an alphanumeric string.
7. The method of claim 3, further comprising performing advertisement tracking of the mobile device using the universal device identifier.
8. The method of claim 3, further comprising sharing information between the plurality of applications installed on the mobile device, with aid of the universal device identifier.

9. A system for identifying a mobile device, comprising:
a memory having (a) a plurality of application sandboxes, an individual sandbox having at least one application therein, and (b) a shared storage; and
a processor capable of executing steps defined by the plurality of applications,
wherein the applications are capable of accessing information within the shared storage via a storage location identifier, and the applications are not capable of accessing information from other sandboxes.
10. The system of claim 9, further comprising a shared storage manager controlling the applications' access to the shared storage.
11. The system of claim 10, wherein the shared storage manager controls access with aid of the storage location identifier that uniquely identifies the location in the shared storage of data accessible by the applications.
12. The system of claim 11, wherein the storage location identifier is an alphanumeric string.
13. The system of claim 9, wherein an individual sandbox of said plurality is a secure memory space on the mobile device in which an associated application is confined and prevented from accessing data and resources in other sandboxes.
14. The system of claim 9, further comprising an operating system that manages the sandboxes and determines resources that the applications are prevented from accessing.
15. The system of claim 9, wherein the shared storage includes a universal device identifier identifying the mobile device and accessible by applications from a plurality of sandboxes.
16. The system of claim 15, wherein the universal device identifier is accessible via the storage location identifier for the universal device identifier.
17. The system of claim 15, wherein the universal device identifier is an alphanumeric string unique to the device.
18. The system of claim 17, wherein the universal device identifier incorporates the time of creation of the universal device identifier.

19. A method of identifying a mobile device, comprising:
providing a memory having (a) a plurality of application sandboxes, an individual sandbox having at least one application therein, and (b) a shared storage;
providing a processor capable of executing steps defined by the plurality of applications;
permitting the applications to access information within the shared storage via a storage location identifier, while not permitting the applications to access information from other sandboxes, wherein the information within the shared storage accessed by the applications includes a universal device identifier; and
performing advertisement tracking of the mobile device using the universal device identifier.
20. The method of claim 19, wherein performing advertising tracking includes following usage patterns of the mobile device across applications.

1 / 3
Mobile Device

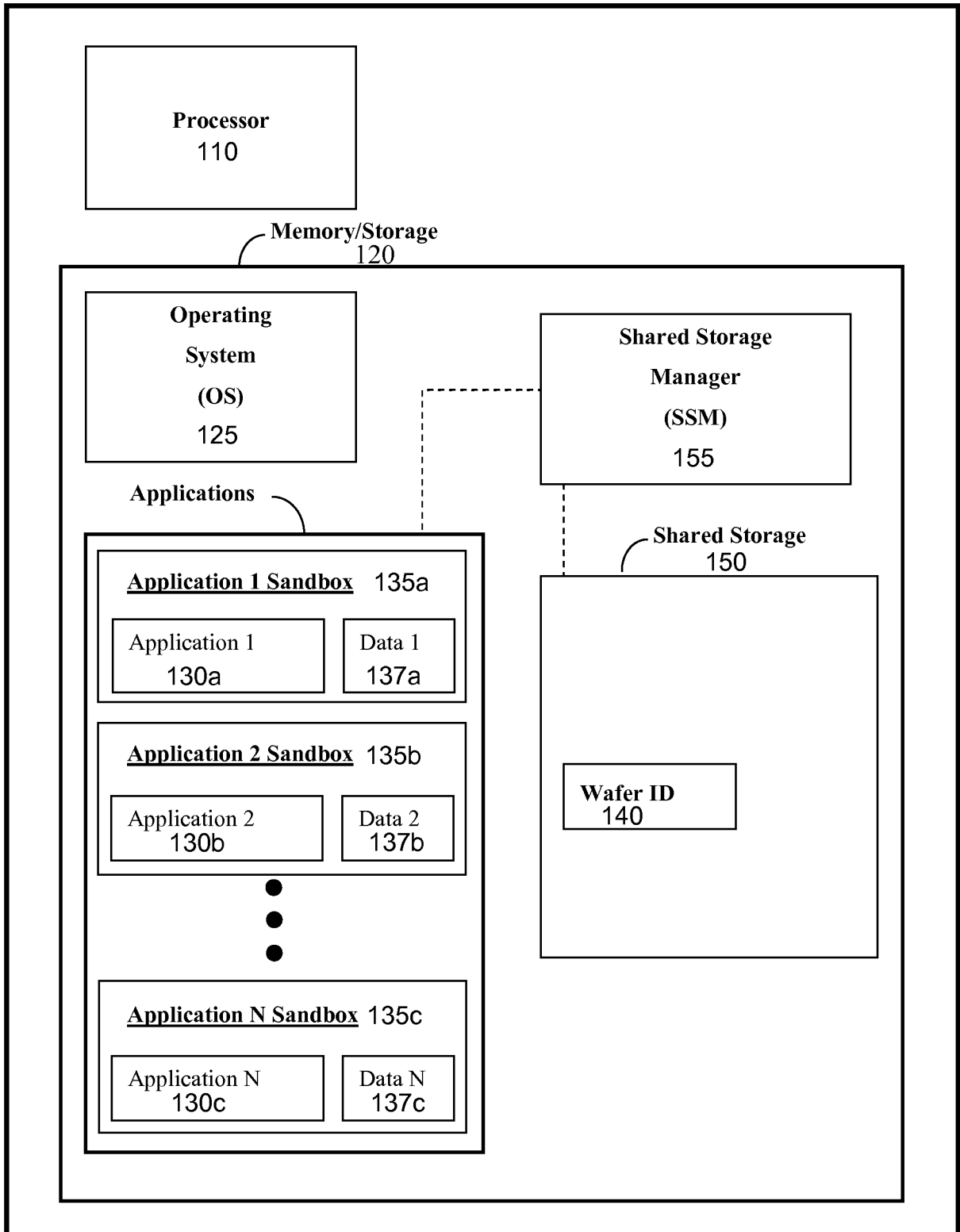


FIGURE 1

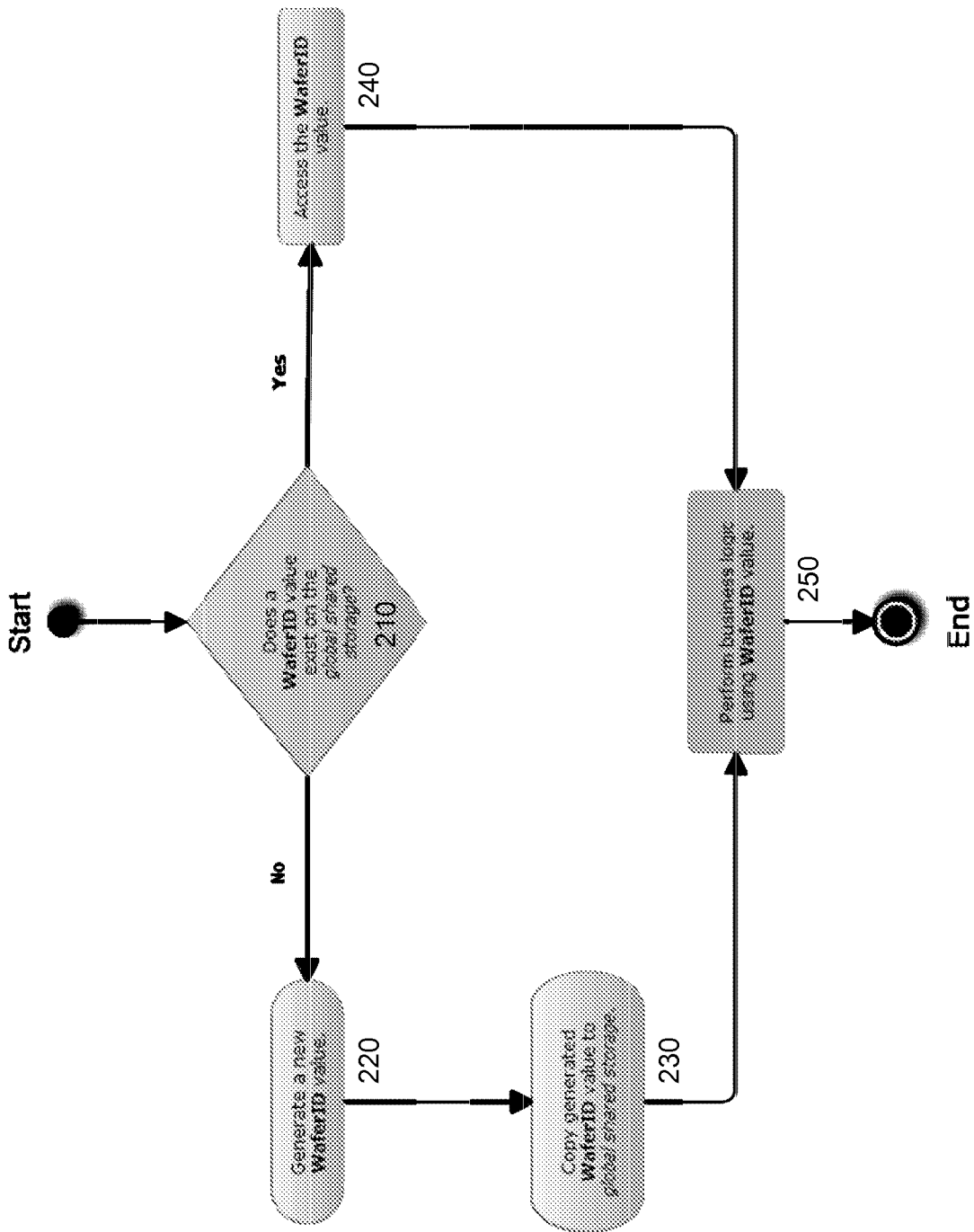


FIGURE 2

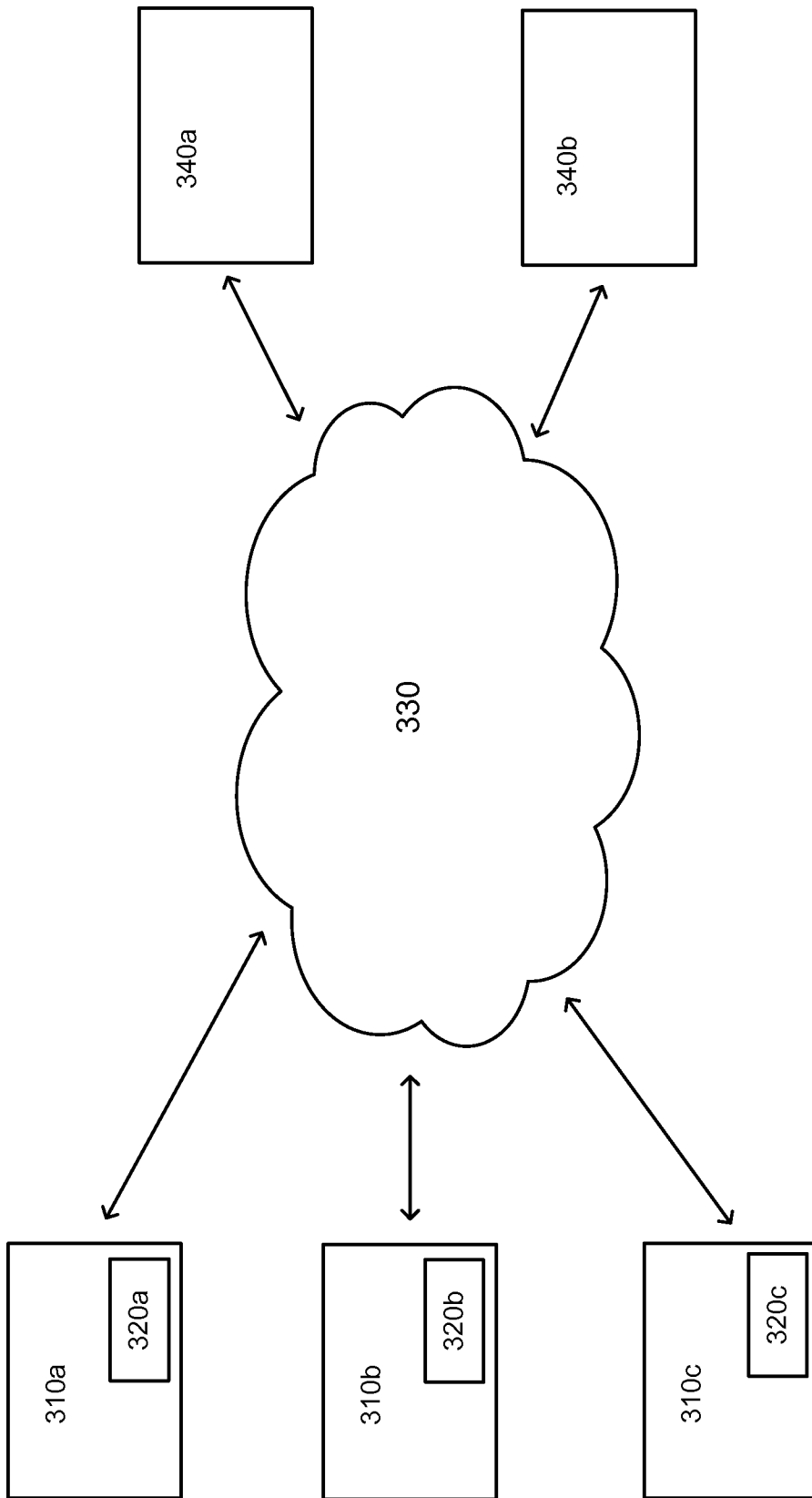


FIGURE 3

A. CLASSIFICATION OF SUBJECT MATTER**G06F 21/57(2013.01)i, G06F 21/53(2013.01)i**

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 21/57; H04Q 7/38; G06F 9/445; H04H 60/65; G06F 17/30; G06Q 30/00; H04N 7/26; G06F 7/04; G06F 21/53

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

Korean utility models and applications for utility models

Japanese utility models and applications for utility models

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

eKOMPASS(KIPO internal) & Keywords:mobile, application, identification, universal device identifier, sandbox

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|-----------|--|-----------------------|
| X | US 7908645 B2 (THOMAS EMMANUAL VARGHESE et al.) 15 March 2011 See column 2, line 45; column 3, lines 17-19; column 5, lines 65-67; column 6, lines 14-17; column 9, lines 4-5; column 12, lines 3-4; column 16, lines 56-58; column 25, lines 54-56, 61-63, 67; column 26, lines 1-3; column 28, lines 20-21; and figs. 1-6, 13A-13B, 14. | 1,3,6,8 |
| A | | 2,4-5,7,9-20 |
| A | US 2011-0288932 A1 (EDWARD MARKS et al.) 24 November 2011 See paragraphs [0004], [0007], [0015], [0047], [0050], [0064]; [0087]; and figs. 1, 3, 5. | 1,3,6,8 |
| A | EP 1209935 A1 (TELEFONAKTIEBOLAGET L M ERICSSON (PUBL)) 29 May 2002 See paragraphs [0001], [0030]-[0033]; and figs. 5, 8. | 1-20 |
| A | EP 1703382 A1 (SUN MICROSYSTEMS, INC.) 20 September 2006 See paragraphs [0001]-[0038]; and figs. 1-3. | 1-20 |
| A | EP 2154891 A1 (RESEARCH IN MOTION LIMITED) 17 February 2010 See paragraphs [0001]-[0006]; and fig. 4. | 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 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

09 July 2013 (09.07.2013)

Date of mailing of the international search report

10 July 2013 (10.07.2013)

Name and mailing address of the ISA/KR


 Korean Intellectual Property Office
 189 Cheongsa-ro, Seo-gu, Daejeon Metropolitan City,
 302-701, Republic of Korea

Facsimile No. +82-42-472-7140

Authorized officer

BYUN Sung Cheal

Telephone No. +82-42-481-8262



INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/US2013/033357

| Patent document cited in search report | Publication date | Patent family member(s) | Publication date |
|--|------------------|-------------------------|------------------|
| US 7908645 B2 | 15/03/2011 | AU 2006-242555 A1 | 09/11/2006 |
| | | CA 2606326 A1 | 09/11/2006 |
| | | CN 101375546 A | 25/02/2009 |
| | | CN 101375546 B | 26/09/2012 |
| | | EP 1875653 A2 | 09/01/2008 |
| | | JP 04954979 B2 | 23/03/2012 |
| | | JP 2008-544339 A | 04/12/2008 |
| | | US 2006-0282660 A1 | 14/12/2006 |
| | | WO 2006-118968 A2 | 09/11/2006 |
| | | WO 2006-118968 A3 | 02/10/2008 |
| US 2011-0288932 A1 | 24/11/2011 | WO 2011-146917 A2 | 24/11/2011 |
| | | WO 2011-146917 A3 | 12/04/2012 |
| EP 1209935 A1 | 29/05/2002 | AT 306799 T | 15/10/2005 |
| | | AU 1699402 A | 03/06/2002 |
| | | AU 2002-16994 A1 | 03/06/2002 |
| | | AU 782981 B2 | 15/09/2005 |
| | | AU 9339401 A | 30/05/2002 |
| | | CA 2363667 A1 | 24/05/2002 |
| | | CA 2363667 C | 12/04/2011 |
| | | CN 1174576 C0 | 03/11/2004 |
| | | CN 1357986 A0 | 10/07/2002 |
| | | DE 60023155 D1 | 17/11/2005 |
| | | DE 60023155 T2 | 06/07/2006 |
| | | EP 1209935 B1 | 12/10/2005 |
| | | ES 2251347 T3 | 01/05/2006 |
| | | JP 04004275 B2 | 07/11/2007 |
| | | JP 2002-247654 A | 30/08/2002 |
| | | WO 02-43424 A1 | 30/05/2002 |
| EP 1703382 A1 | 20/09/2006 | US 2006-0212537 A1 | 21/09/2006 |
| | | US 2011-0177803 A1 | 21/07/2011 |
| | | US 7941656 B2 | 10/05/2011 |
| | | US 8225082 B2 | 17/07/2012 |
| EP 2154891 A1 | 17/02/2010 | AU 2009-202651 A1 | 25/02/2010 |
| | | AU 2009-202651 B2 | 07/04/2011 |
| | | CA 2674119 A1 | 11/02/2010 |
| | | CN 101651685 A | 17/02/2010 |
| | | EP 2154891 B1 | 20/03/2013 |
| | | JP 05047238 B2 | 10/10/2012 |
| | | JP 2010-044758 A | 25/02/2010 |
| | | KR 10-1172571 B1 | 08/08/2012 |
| | | KR 10-2010-0019962 A | 19/02/2010 |
| | | MX 2009007276 A | 01/03/2010 |
| | | SG 159440 A1 | 30/03/2010 |
| | | TW 201007470 A | 16/02/2010 |