(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
7 September 2012 (07.09.2012)

WIPO | PCT

(10) International Publication Number
WO 2012/117155 A1

(51) International Patent Classification:
H04L 29/08 (2006.01) *G06F 17/30* (2006.01)
H04L 29/06 (2006.01)

(21) International Application Number:
PCT/FI2012/050169

(22) International Filing Date:
22 February 2012 (22.02.2012)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/447,203 28 February 2011 (28.02.2011) US
13/071,144 24 March 2011 (24.03.2011) US

(71) Applicant *(for all designated States except US)*: **NOKIA CORPORATION** [FI/FI]; Keilalahdentie 4, FI-02150 Espoo (FI).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **SAINIO, Miikka Johannes** [FI/FI]; Jaakkolantie 11 C 23, FI-04250 Kerava (FI). **LAHTIRANTA, Atte** [FI/US]; 26 Sweetwater Avenue, Bedford, MA 01730 (US).

(74) Agents: **NOKIA CORPORATION** et al.; IPR Department, Jussi Jaatinen, Keilalahdentie 4, FI-02150 Espoo (FI).

(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, 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, 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.

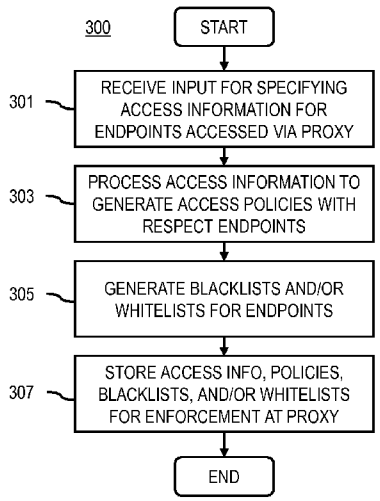
(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE,

[Continued on next page]

(54) Title: METHOD AND APPARATUS FOR PROVIDING A PROXY-BASED ACCESS LIST

(57) Abstract: An approach is provided for a proxy-based access list. A proxy platform receives an input for specifying access information for one or more communication endpoints accessible via a proxy server. The proxy platform processes and/or facilitates a processing of the access information to generate one or more access policies with respect to the one or more communication endpoints. Access to the one or more communication endpoints via the proxy server is provided based, at least in part, on the one or more access policies.

FIG. 3



WO 2012/117155 A1

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))*

METHOD AND APPARATUS FOR PROVIDING A PROXY-BASED ACCESS LIST

BACKGROUND

Wireless (e.g., cellular) service providers and device manufacturers are continually challenged to deliver value and convenience to consumers by, for example, providing compelling network services, applications, and content. In light of an increasingly web-centric culture, one emerging service is the use of wireless devices to access mobile web services. However, limited resources (e.g., bandwidth, processing power, availability of the mobile web server) within the wireless environment can limit access to such web services on mobile devices. Accordingly, service providers and device manufacturers face significant technical challenges to overcome such limitations by enabling efficient and secure access to web services via, for instance, a proxy server.

SOME EXEMPLARY EMBODIMENTS

Therefore, there is a need for an approach for providing a proxy-based access list (e.g., a black list or white list of communication endpoints) to reduce, for instance, risks resulting from access of potentially malicious web services.

According to one embodiment, a method comprises receiving an input for specifying access information for one or more communication endpoints accessible via a proxy server. The method also comprises processing and/or facilitating a processing of the access information to generate one or more access policies with respect to the one or more communication endpoints. Access to the one or more communication endpoints via the proxy server is provided based, at least in part, on the one or more access policies.

According to another embodiment, an apparatus comprises at least one processor, and at least one memory including computer program code, the at least one memory and the computer program code configured to, with the at least one processor, cause, at least in part, the apparatus to receive an input for specifying access information for one or more communication endpoints accessible via a proxy server. The apparatus is also caused to process and/or facilitate a processing of the access information to generate one or more access policies with respect to the one or more communication endpoints. Access to the one or more communication endpoints via the proxy server is provided based, at least in part, on the one or more access policies.

According to another embodiment, a computer-readable storage medium carries one or more sequences of one or more instructions which, when executed by one or more processors, cause, at least in part, an apparatus to receive an input for specifying access information for one or more

communication endpoints accessible via a proxy server. The apparatus is also caused to process and/or facilitate a processing of the access information to generate one or more access policies with respect to the one or more communication endpoints. Access to the one or more communication endpoints via the proxy server is provided based, at least in part, on the one or more access policies.

According to another embodiment, an apparatus comprises means for receiving an input for specifying access information for one or more communication endpoints accessible via a proxy server. The apparatus also comprises means for processing and/or facilitating a processing of the access information to generate one or more access policies with respect to the one or more communication endpoints. Access to the one or more communication endpoints via the proxy server is provided based, at least in part, on the one or more access policies.

In addition, for various example embodiments of the invention, the following is applicable: a method comprising facilitating a processing of and/or processing (1) data and/or (2) information and/or (3) at least one signal, the (1) data and/or (2) information and/or (3) at least one signal based, at least in part, on (including derived at least in part from) any one or any combination of methods (or processes) disclosed in this application as relevant to any embodiment of the invention.

For various example embodiments of the invention, the following is also applicable: a method comprising facilitating access to at least one interface configured to allow access to at least one service, the at least one service configured to perform any one or any combination of network or service provider methods (or processes) disclosed in this application.

For various example embodiments of the invention, the following is also applicable: a method comprising facilitating creating and/or facilitating modifying (1) at least one device user interface element and/or (2) at least one device user interface functionality, the (1) at least one device user interface element and/or (2) at least one device user interface functionality based, at least in part, on data and/or information resulting from one or any combination of methods or processes disclosed in this application as relevant to any embodiment of the invention, and/or at least one signal resulting from one or any combination of methods (or processes) disclosed in this application as relevant to any embodiment of the invention.

For various example embodiments of the invention, the following is also applicable: a method comprising creating and/or modifying (1) at least one device user interface element and/or (2) at least one device user interface functionality, the (1) at least one device user interface element and/or (2) at least one device user interface functionality based at least in part on data and/or information resulting from one or any combination of methods (or processes) disclosed in this application as relevant to any embodiment of the invention, and/or at least one signal resulting

from one or any combination of methods (or processes) disclosed in this application as relevant to any embodiment of the invention.

In various example embodiments, the methods (or processes) can be accomplished on the service provider side or on the mobile device side or in any shared way between service provider and mobile device with actions being performed on both sides.

For various example embodiments, the following is applicable: An apparatus comprising means for performing the method of any of originally filed claims 1-8, 21-28, and 42-44.

Still other aspects, features, and advantages of the invention are readily apparent from the following detailed description, simply by illustrating a number of particular embodiments and implementations, including the best mode contemplated for carrying out the invention. The invention is also capable of other and different embodiments, and its several details can be modified in various obvious respects, all without departing from the spirit and scope of the invention. Accordingly, the drawings and description are to be regarded as illustrative in nature, and not as restrictive.

BRIEF DESCRIPTION OF THE DRAWINGS

The embodiments of the invention are illustrated by way of example, and not by way of limitation, in the figures of the accompanying drawings:

FIG. 1 is a diagram of a communication system capable of providing a proxy-based access list, according to one embodiment;

FIG. 2 is a diagram of components of a proxy platform, according to one embodiment;

FIG. 3 is a flowchart of a process for generating proxy-based access policies or lists, according to one embodiment;

FIG. 4 is flowchart of a process for enforcing proxy-based access policies or lists, according to one embodiment;

FIGs. 5A and 5B are diagrams of user interfaces utilized in the processes of FIGs. 1-4, according to various embodiments;

FIG. 6 is a diagram of hardware that can be used to implement an embodiment of the invention;

FIG. 7 is a diagram of a chip set that can be used to implement an embodiment of the invention; and

FIG. 8 is a diagram of a mobile station (e.g., handset) that can be used to implement an embodiment of the invention.

DESCRIPTION OF PREFERRED EMBODIMENT

A method and apparatus for providing proxy-based access lists are disclosed. In the following description, for the purposes of explanation, numerous specific details are set forth in order to provide a thorough understanding of the embodiments of the invention. It is apparent, however, to one skilled in the art that the embodiments of the invention may be practiced without these specific details or with an equivalent arrangement. In other instances, well-known structures and devices are shown in block diagram form in order to avoid unnecessarily obscuring the embodiments of the invention.

Although various embodiments are described with respect to providing proxy-based access lists within a wireless network environment, it is contemplated that the various embodiments of the approach described herein may be used within any type of communication system or network and with any mode of communication available of the network (e.g., data communications, Internet communication, voice communication, text communication, etc). In addition, although the various embodiments are further described with respect to mobile devices, it is contemplated that the various embodiments are applicable to any type of device with network access (e.g., stationary terminals, personal computers, etc.).

FIG. 1 is a diagram of a communication system capable of providing a proxy-based access list, according to one embodiment. As discussed previously, implementing mobile web services within a wireless environment can potentially tax the relatively limited resources (e.g., bandwidth, processing power, memory, etc.) that are available within the environment (e.g., within a mobile device). Moreover, use of such services to access content over the Internet can potentially expose devices to potential risks (e.g., security risks, privacy risks, etc.). For example, the Internet can contain or otherwise provide access to risks such as phishing or other fraudulent attacks, questionable material, as well as to malicious web sites that aim to, for instance, acquire sensitive information from the a user device, crash the browser or device, and/or perform other malicious acts. Similarly, access to other communication endpoints (e.g., telephone numbers, premium text messaging services, chat services, etc.) accessible over a communication network can also be used as vehicles for such malicious purposes.

As a result, devices can be vulnerable to a myriad number of risks present within modern communication networks. Historically, devices can use protective measures such as anti-malware programs, anti-virus programs, and the like, but these traditional solutions can be quite resource intensive to operate, particularly in mobile devices with limited resources. Furthermore, such solutions can be slow to respond to quickly emerging threats.

To address these problems, a system 100 of FIG. 1 introduces a capability to create proxy-based access lists and/or policies for communicating with communication endpoints available via, for instance, a proxy platform 101 (e.g., a proxy server) over a communication network 103. In one embodiment, the system 100 uses crowd-sourced access information to generate the access lists

and/or policies that are then enforced at the proxy platform 101. More specifically, the system 100 enables users (e.g., via user equipment (UEs) 105a-105n, also collectively referred to as UEs 105) to be able to (1) flag or otherwise designate malicious communication endpoints (e.g., websites, phone numbers, text messaging numbers, chat identifiers, user names, etc.), and (2) be protected from the flagged malicious communication endpoints without exposing the client device (e.g., the UE 105) to malicious endpoints.

As shown in FIG. 1, the system 100 includes a proxy browsing architecture which consists of one or more proxy clients 107a-107n (also collectively referred to as proxy clients 107) operating within respective client devices (e.g., UEs 105a-105n). In one embodiment, the proxy clients 107 route at least a portion of the communication traffic from the UEs 105 through the proxy platform 101. In some embodiments, the proxy clients 107 may be a browser application. In addition or alternatively, the proxy clients 107 can be independent processes executing in the UEs 105, or can be incorporated in other applications executing in the UEs 1015.

In one embodiment, the proxy platform 101 receives requests from the proxy clients 107 to route communication traffic to the intended communication endpoints. In addition, the proxy platform 101 can route return communication traffic from the communication endpoints to the any of the proxy clients 107 and/or UEs 105. By way of example, the communication endpoints can include a service platform 109, the services 111a-111m (also collectively referred to as services 111), the content providers 113a-113k (also collectively referred to as content providers 113), or any other component with connectivity to the communication network 103 (e.g., another UE 105). For example, the service platform 109, the service 111, and/or the content providers 113 may provide any number of services (e.g., mapping services, social networking services, media services, content services, etc.) via a web server or other means of communications (e.g., text messaging, voice, instant messaging, chat, etc.). In other words, the communication endpoints represent a terminating point of communications from the proxy clients 107, and an originating point of communications to the proxy clients 107.

In some embodiments, in addition to various embodiments of the access list or policy process described herein, the proxy platform 101 can perform any number of communications related functions for routing and/or processing communication traffic. For example, the proxy platform 101 may compress or otherwise modify content that is to be delivered to the proxy clients 107 based, at least in part, on one or more capabilities or characteristics of the receiving UE 105. For example, in wireless environments, the proxy platform 101 can compress data for more efficient transmission, transform content to reduce the amount of data for transfer, reformat content for display in smaller screens, etc.

In one embodiment, the proxy platform 101 receives access information for generating the access lists and/or access policies using crowd-sourcing (e.g., access information gathered from other

UEs 105 and/or their respective users). For example, through crowd-sourcing the access information, the system 100 can quickly respond to new threats or conditions, and also reduce resource burdens (e.g., operational expense, computation resources, etc.) associated with operating a completely managed system. As used herein, access information includes identification of one or more communication endpoints, the access behavior that has been or is to be associated with the communication endpoint, descriptions of the communication endpoints, characteristics of the communication endpoints, and/or any other information that can indicate potential risks associated with the communication endpoints. For example, the access information may include flags indicating that a particular endpoint (e.g., website) is malicious, spreads malware, infected with one or more viruses, etc.

In one embodiment, the reported access information can be verified by access information received from other users. For example, the system 100 may only use access information that has been reported by multiple UEs 105 or users. In addition, the system 100 enables user to report on the accuracy of previously reported access information. For example, other users relying on the access information can give feedback or a rating of the information.

In one embodiment, the access information and/or access list may be provided by or obtained from third party providers (e.g., the services 111 and/or content providers 113). For example, an organization may maintain a blacklist of fraudulent or otherwise risky communication endpoints. In one embodiment, the proxy platform 101 can use these third party lists or access information as default blacklists. Then, as the proxy platform 101's proxy clients 107 begin generating and reporting their own access information, the proxy platform 101 can customize or replace portions of the default blacklists based, at least in part, on the reported access information.

The proxy platform 101 can then use the crowd-sourced information to generate and/or determine policies to apply when receiving requests to access communication endpoints via the proxy platform 101. In one embodiment, the access policies may provide rules for the proxy platform 101 to determine whether grant, deny, or restrict access to one or more communication endpoints. In one embodiment, the system 100 can present a notification to a requesting proxy client 107 regarding the access information and/or policies associated with a particular communication endpoint. For example, if the communication endpoint appears on a blacklist, the proxy platform 101 may present a prompt to ask whether the requesting proxy client 107 would like to override the blacklist or corresponding access policy.

By way of example, the UE 105 is any type of mobile terminal, fixed terminal, or portable terminal including a mobile handset, station, unit, device, multimedia computer, multimedia tablet, Internet node, communicator, desktop computer, laptop computer, notebook computer, netbook computer, tablet computer, personal communication system (PCS) device, personal navigation device, personal digital assistants (PDAs), audio/video player, digital camera/camcorder,

positioning device, television receiver, radio broadcast receiver, electronic book device, game device, or any combination thereof, including the accessories and peripherals of these devices, or any combination thereof. It is also contemplated that the UE 105 can support any type of interface to the user (such as "wearable" circuitry, etc.).

Additionally, the communication network 103 of system 100 includes one or more networks such as a data network (not shown), a wireless network (not shown), a telephony network (not shown), or any combination thereof. It is contemplated that the data network may be any local area network (LAN), metropolitan area network (MAN), wide area network (WAN), a public data network (e.g., the Internet), short range wireless network, or any other suitable packet-switched network, such as a commercially owned, proprietary packet-switched network, e.g., a proprietary cable or fiber-optic network, and the like, or any combination thereof. In addition, the wireless network may be, for example, a cellular network and may employ various technologies including enhanced data rates for global evolution (EDGE), general packet radio service (GPRS), global system for mobile communications (GSM), Internet protocol multimedia subsystem (IMS), universal mobile telecommunications system (UMTS), etc., as well as any other suitable wireless medium, e.g., worldwide interoperability for microwave access (WiMAX), Long Term Evolution (LTE) networks, code division multiple access (CDMA), wideband code division multiple access (WCDMA), wireless fidelity (WiFi), wireless LAN (WLAN), Bluetooth®, Internet Protocol (IP) data casting, satellite, mobile ad-hoc network (MANET), and the like, or any combination thereof.

Communication is facilitated between the UE 105 and the proxy platform 101 via the communication network 103 using well known, new or still developing protocols. In this context, a protocol includes a set of rules defining how the network nodes within the communication network 103 interact with each other based on information sent over the communication links. The protocols are effective at different layers of operation within each node, from generating and receiving physical signals of various types, to selecting a link for transferring those signals, to the format of information indicated by those signals, to identifying which software application executing on a computer system sends or receives the information. The conceptually different layers of protocols for exchanging information over a network are described in the Open Systems Interconnection (OSI) Reference Model.

Communications between the network nodes are typically effected by exchanging discrete packets of data. Each packet typically comprises (1) header information associated with a particular protocol, and (2) payload information that follows the header information and contains information that may be processed independently of that particular protocol. In some protocols, the packet includes (3) trailer information following the payload and indicating the end of the payload information. The header includes information such as the source of the packet, its destination, the length of the payload, and other properties used by the protocol. Often, the data

in the payload for the particular protocol includes a header and payload for a different protocol associated with a different, higher layer of the OSI Reference Model. The header for a particular protocol typically indicates a type for the next protocol contained in its payload. The higher layer protocol is said to be encapsulated in the lower layer protocol. The headers included in a packet traversing multiple heterogeneous networks, such as the Internet, typically include a physical (layer 1) header, a data-link (layer 2) header, an internetwork (layer 3) header and a transport (layer 4) header, and various application headers (layer 5, layer 6 and layer 7) as defined by the OSI Reference Model.

In one embodiment, the proxy clients 107 and the proxy platform 101 interact according to a client-server model. It is noted that the client-server model of computer process interaction is widely known and used. According to the client-server model, a client process sends a message including a request to a server process, and the server process responds by providing a service. The server process may also return a message with a response to the client process. Often the client process and server process execute on different computer devices, called hosts, and communicate via a network using one or more protocols for network communications. The term "server" is conventionally used to refer to the process that provides the service, or the host computer on which the process operates. Similarly, the term "client" is conventionally used to refer to the process that makes the request, or the host computer on which the process operates. As used herein, the terms "client" and "server" refer to the processes, rather than the host computers, unless otherwise clear from the context. In addition, the process performed by a server can be broken up to run as multiple processes on multiple hosts (sometimes called tiers) for reasons that include reliability, scalability, and redundancy, among others.

FIG. 2 is a diagram of components of a proxy platform, according to one embodiment. By way of example, the proxy platform 101 includes one or more components for providing proxy-based access lists. It is contemplated that the functions of these components may be combined in one or more components or performed by other components of equivalent functionality. In this embodiment, the proxy platform 101 includes a control logic 201, an access information collector 203, an access information/policies/lists database 205, an access policy/list generator 207, a communication router 209, an enforcement module 211, a notification module 213, and a social networking module 215.

More specifically, the control logic 201 executes at least one algorithm for performing one or more functions of the proxy platform 101. For example, the control logic 201 interacts with the access information collector 203 to receive or otherwise determine access information from, for instance, the UEs 105. As previously described, access information includes information that provides, at least in part, indications of whether access to one or more communications points are to granted, denied, or otherwise restricted. For example, access information may include flags indicating whether a particular communication endpoint (e.g., a website, a phone number, a test

messaging number, etc.) is associated with malicious, fraudulent, or other potential risks. In addition or alternatively, access information may include user experience that indicates one or more communication endpoints are free or substantially free from known threats. By way of example, the access information collector 203 may store all or a portion of the collected access information in the access information/policies/lists database 205.

The access information collector 203 can then interact with the access policy/list generator 207 to process the collected access information for generating one or more access policies or lists. For example, for communication endpoints that are specified in the access information, the access policy/list generator 207 can determine access recommendations such as whether a particular communication endpoint is malicious and then determine an appropriate access policy. For example, if a communication endpoint meets criteria (e.g., reported as malicious by more than a predetermined number of users, reported as free from threats by more than a predetermined number of users, demonstrated to have caused harm to a proxy client 107 or UE 105, etc.), then a corresponding access policy is applied (e.g., deny access to a communication endpoint, provide warnings before allowing access, etc.). These policies can be stored, at least in part, in the access information/policies/lists database 205.

In addition or alternatively, the access policy/list generator 207 can generate access lists (e.g., blacklists to deny access, whitelists to enable access, gray lists to warn before determining access) with respect to the communication endpoints. For example, the access policy/list generator 207 may create or compile a blacklist of endpoints that pose threat level above a threshold value. Entry in the blacklist of a communication endpoint can result in denial of access to that endpoint. Similarly, the access policy/list generator 207 can generate whitelists of endpoints that have been reported to pose a no threat or a threat level below threshold level. Entry in the whitelist of a communication endpoint can, for instance, enable communication with the endpoint without restriction from the proxy platform 101. In another embodiment, the access policy/list generator 207 can generate gray lists to cover communication endpoints that may have at least some of level of potential threat. Entry in the gray list of a communication endpoint can, for instance, result in presentation notification of potential threats to enable the user to make a final access decision with respect to a particular endpoint. In one embodiment, the access policy/list generator 207 can store the access lists in the access information/policies/lists database 205.

In another embodiment, the access policy/list generator 207 can retrieve or otherwise obtain premade access lists or policies from a third party source (e.g., the services 111, the content providers 113, the service platform 109, etc.). As previously noted, the third party lists or policies may be used when access information is incomplete or unavailable. For example, the third party access lists or policies can apply to communication endpoints that have not yet been visited by the proxy clients 107 or the UEs 105.

Once the access policies or lists are available, the communication router 209 begins monitoring communication requests and other traffic through the proxy platform 101 to determine whether the requests or traffic relate any previously stored policies or lists. If any policies or lists are applicable, the communication router 209 interacts with the enforcement module 211 to grant, deny, or restrict access to the one or more communication endpoints based, at least in part, on the policies or lists. Based on the applicable access policies or lists, the enforcement module 211 can interact with the notification module 213 to present notifications to the user regarding any access information, policy, or list that might apply to the user's request to access one or more communication endpoints.

In another embodiment, the enforcement module 211 can also interact with the social networking module 215 to filter the access information, policies, or lists based, at least in part, on one or more social networks associated with a user who is requesting access to one or more communication endpoints. In this way, a user can limit the crowd-sourced access information to information collected from social network contacts that may have more trusted relationships with the user. In this way, the access policies and lists can be more specifically tailored for a particular user without the user having, for instance, to manually override any determined policies or lists.

FIG. 3 is a flowchart of a process for generating proxy-based access policies or lists, according to one embodiment. In one embodiment, the proxy platform 101 performs the process 300 and is implemented in, for instance, a chip set including a processor and a memory as shown FIG. 7. In step 301, the proxy platform 101 receives an input for specifying access information for one or more communication endpoints accessible via a proxy server. By way of example, the input is received from one or more of the proxy clients 107, one or more other devices or UEs 105, one or more third-party sources (e.g., the service platform 109, the service 111, and/or the content providers 113).

Next, the proxy platform 101 processes and/or facilitates a processing of the access information to generate one or more access policies with respect to the one or more communication endpoints, wherein access to the one or more communication endpoints via the proxy server is provided based, at least in part, on the one or more access policies (step 303). In one embodiment, the proxy platform 101 also causes, at least in part, a generation of one or more access lists, including, at least in part, blacklists, one or more whitelists, one or more gray lists, or a combination thereof regarding the one or more communication endpoints.

In one embodiment, the proxy platform 101 can generate the one or more access policies based, at least in part, on the one or more access lists (step 305). In other words, the one or more access policies can apply rules for enforcing the one or more access lists at the proxy platform 101. The access information, access policies, and/or access lists can then be stored (e.g., in the access

information/policies/lists database 205) for later use (e.g., enforcement) at the proxy platform 101.

FIG. 4 is flowchart of a process for enforcing proxy-based access policies or lists, according to one embodiment. In one embodiment, the proxy platform 101 performs the process 400 and is implemented in, for instance, a chip set including a processor and a memory as shown FIG. 7. The example of FIG. 4 assumes that the process 300 of FIG. 3 has been completed to generate one or more access policies or access lists for enforcement at the proxy platform 101.

In step 401, the proxy platform 101 receives a request for access to at least one of the one or more communication endpoints via the proxy server. By way of example, the request is received from one or more proxy clients 107 served by the proxy platform 101. In this example, at least a portion of the communication traffic between the one or more proxy clients 107 and one or more communication endpoints is routed through the proxy platform 101. Accordingly, the request can be indicated by a proxy clients 107, for instance, entering a web address, dialing a phone number, texting to a phone number, initiating a chat session, etc. with respect to a communication endpoint. In this case, the communication endpoint is any communication device (e.g., server, device, component, etc.) with connectivity to the proxy platform 101 and/or the communication network 103.

Next, the proxy platform determines whether there is any access information, access policies, access lists (e.g., blacklists, whitelists, gray lists, etc.), or the like associated with one or more communication endpoints referenced in the communication request (step 403). If there is any such information, the proxy platform 101 determines to present a notification message based, at least in part, on the request, the one or more access policies, the access information, or a combination thereof (step 405). By way of example, the notification may provide information regarding the type of access information, policies, lists, etc. that relate to the intended communication endpoints. For example, the notification the may inform the user that the communication endpoint has been reported to be malicious. In one embodiment, the notification information may also include related metadata (e.g., how many users have reported the access information, how recently has the access information been reported, and the like).

In step 407, the proxy platform 101 determines whether there is social networking information associated with a user of a device from which the request was received. If yes, the proxy platform 101 determines social networking information associated with the requesting device and/or a user of the device (step 409). For example, the proxy platform 101 may query user profile information to make the determination. In another example, the user or associated UE 105 may report the availability of social networking information.

In one embodiment, the proxy platform 101 then processes and/or facilitates a processing of the social networking information to filter at least a portion of the access information, the one or more access policies, or a combination thereof associated with one or more social networks of the user (step 411). For example, the proxy platform 101 may filter out access information, policies, lists, etc. that are not derived or collected from one or more social networking contacts of the user. It is contemplated that the proxy platform 101 may apply any criteria or rule for filtering based, on social networking information (e.g., filter information other than information collected from at least friends of friends, filter out information provided by specific users or devices, weigh information from social networking contacts more heavily, etc.).

In step 413, the proxy platform 101 then processes and/or facilitates a processing of the access request and the one or more access policies/lists to determine whether to grant, deny, or restrict the access to the at least one of the one or more communication endpoints. In this way, the proxy platform 101 can enforce policies to reduce potential threat exposure to the proxy clients 107 without having to transmit potentially risky information to the requesting device.

FIGs. 5A and 5B are diagrams of user interfaces utilized in the processes of FIGs. 1-4, according to various embodiments. FIG. 5A shows a user interface 501 that depicts a browser directed to a website, "http://malicious.com". In this example, the website is accessed at a proxy client 107 via the proxy platform 101. Moreover, the proxy platform 101 has no previously reported access information, access policies, access lists, etc. that would restrict access to the site. Accordingly, the requested site is served to the proxy client 107 without restriction. However, the user visiting the site observes that the site includes potential security risks and selects an option 503 to flag the site as potentially malicious. The UI 501 also provides an option 505 to rate the site or to provide more details regarding why the site has been flagged as malicious.

In one embodiment, the selections of the options 503 and 505 represent access information associated with the site (e.g., the communication endpoint) that is then reported to the proxy platform 101. The proxy platform 101 uses this access information to generate access policies or lists with respect the site (e.g., place the site on a blacklist or gray list).

FIG. 5B depicts a user interface 521 that is generated by the proxy platform 101 when enforcing the policy generated as described with respect to FIG. 5A. In this case, the same or another proxy client 107 attempts to access the website, "http://malicious.com", via the proxy platform 101. The proxy platform 101 determines that the site has been placed on a blacklist and notifies the user accordingly. As shown, the UI 521 presents a notification that the site that the user is trying to access has been flagged as malicious. In addition, the proxy platform 101 informs the user that the site has been flagged by 15 different users. The additional information can provide the user with information regarding the reliability of the crowd-sourced access information. In other words, it more likely that the access information is more trustworthy or reliable if a greater

number of users report the same access information. The UI 521 then gives the user an option to either continue to the site or abort the request. In this way, the proxy platform 101 enables the user to learn of potential threats posed by a communication endpoint before the user's device is exposed to the threat (e.g., before the user attempts to download the website data).

The processes described herein for providing a proxy-based access list may be advantageously implemented via software, hardware, firmware or a combination of software and/or firmware and/or hardware. For example, the processes described herein, may be advantageously implemented via processor(s), Digital Signal Processing (DSP) chip, an Application Specific Integrated Circuit (ASIC), Field Programmable Gate Arrays (FPGAs), etc. Such exemplary hardware for performing the described functions is detailed below.

FIG. 6 illustrates a computer system 600 upon which an embodiment of the invention may be implemented. Although computer system 600 is depicted with respect to a particular device or equipment, it is contemplated that other devices or equipment (e.g., network elements, servers, etc.) within FIG. 6 can deploy the illustrated hardware and components of system 600. Computer system 600 is programmed (e.g., via computer program code or instructions) to provide a proxy-based access list as described herein and includes a communication mechanism such as a bus 610 for passing information between other internal and external components of the computer system 600. Information (also called data) is represented as a physical expression of a measurable phenomenon, typically electric voltages, but including, in other embodiments, such phenomena as magnetic, electromagnetic, pressure, chemical, biological, molecular, atomic, sub-atomic and quantum interactions. For example, north and south magnetic fields, or a zero and non-zero electric voltage, represent two states (0, 1) of a binary digit (bit). Other phenomena can represent digits of a higher base. A superposition of multiple simultaneous quantum states before measurement represents a quantum bit (qubit). A sequence of one or more digits constitutes digital data that is used to represent a number or code for a character. In some embodiments, information called analog data is represented by a near continuum of measurable values within a particular range. Computer system 600, or a portion thereof, constitutes a means for performing one or more steps of providing a proxy-based access list.

A bus 610 includes one or more parallel conductors of information so that information is transferred quickly among devices coupled to the bus 610. One or more processors 602 for processing information are coupled with the bus 610.

A processor (or multiple processors) 602 performs a set of operations on information as specified by computer program code related to providing a proxy-based access list. The computer program code is a set of instructions or statements providing instructions for the operation of the processor and/or the computer system to perform specified functions. The code, for example, may be written in a computer programming language that is compiled into a native instruction set of the

processor. The code may also be written directly using the native instruction set (e.g., machine language). The set of operations include bringing information in from the bus 610 and placing information on the bus 610. The set of operations also typically include comparing two or more units of information, shifting positions of units of information, and combining two or more units of information, such as by addition or multiplication or logical operations like OR, exclusive OR (XOR), and AND. Each operation of the set of operations that can be performed by the processor is represented to the processor by information called instructions, such as an operation code of one or more digits. A sequence of operations to be executed by the processor 602, such as a sequence of operation codes, constitute processor instructions, also called computer system instructions or, simply, computer instructions. Processors may be implemented as mechanical, electrical, magnetic, optical, chemical or quantum components, among others, alone or in combination.

Computer system 600 also includes a memory 604 coupled to bus 610. The memory 604, such as a random access memory (RAM) or any other dynamic storage device, stores information including processor instructions for providing a proxy-based access list. Dynamic memory allows information stored therein to be changed by the computer system 600. RAM allows a unit of information stored at a location called a memory address to be stored and retrieved independently of information at neighboring addresses. The memory 604 is also used by the processor 602 to store temporary values during execution of processor instructions. The computer system 600 also includes a read only memory (ROM) 606 or any other static storage device coupled to the bus 610 for storing static information, including instructions, that is not changed by the computer system 600. Some memory is composed of volatile storage that loses the information stored thereon when power is lost. Also coupled to bus 610 is a non-volatile (persistent) storage device 608, such as a magnetic disk, optical disk or flash card, for storing information, including instructions, that persists even when the computer system 600 is turned off or otherwise loses power.

Information, including instructions for providing a proxy-based access list, is provided to the bus 610 for use by the processor from an external input device 612, such as a keyboard containing alphanumeric keys operated by a human user, or a sensor. A sensor detects conditions in its vicinity and transforms those detections into physical expression compatible with the measurable phenomenon used to represent information in computer system 600. Other external devices coupled to bus 610, used primarily for interacting with humans, include a display device 614, such as a cathode ray tube (CRT), a liquid crystal display (LCD), a light emitting diode (LED) display, an organic LED (OLED) display, a plasma screen, or a printer for presenting text or images, and a pointing device 616, such as a mouse, a trackball, cursor direction keys, or a motion sensor, for controlling a position of a small cursor image presented on the display 614 and issuing commands associated with graphical elements presented on the display 614. In some embodiments, for example, in embodiments in which the computer system 600 performs all functions automatically

without human input, one or more of external input device 612, display device 614 and pointing device 616 is omitted.

In the illustrated embodiment, special purpose hardware, such as an application specific integrated circuit (ASIC) 620, is coupled to bus 610. The special purpose hardware is configured to perform operations not performed by processor 602 quickly enough for special purposes. Examples of ASICs include graphics accelerator cards for generating images for display 614, cryptographic boards for encrypting and decrypting messages sent over a network, speech recognition, and interfaces to special external devices, such as robotic arms and medical scanning equipment that repeatedly perform some complex sequence of operations that are more efficiently implemented in hardware.

Computer system 600 also includes one or more instances of a communications interface 670 coupled to bus 610. Communication interface 670 provides a one-way or two-way communication coupling to a variety of external devices that operate with their own processors, such as printers, scanners and external disks. In general the coupling is with a network link 678 that is connected to a local network 680 to which a variety of external devices with their own processors are connected. For example, communication interface 670 may be a parallel port or a serial port or a universal serial bus (USB) port on a personal computer. In some embodiments, communications interface 670 is an integrated services digital network (ISDN) card or a digital subscriber line (DSL) card or a telephone modem that provides an information communication connection to a corresponding type of telephone line. In some embodiments, a communication interface 670 is a cable modem that converts signals on bus 610 into signals for a communication connection over a coaxial cable or into optical signals for a communication connection over a fiber optic cable. As another example, communications interface 670 may be a local area network (LAN) card to provide a data communication connection to a compatible LAN, such as Ethernet. Wireless links may also be implemented. For wireless links, the communications interface 670 sends or receives or both sends and receives electrical, acoustic or electromagnetic signals, including infrared and optical signals, that carry information streams, such as digital data. For example, in wireless handheld devices, such as mobile telephones like cell phones, the communications interface 670 includes a radio band electromagnetic transmitter and receiver called a radio transceiver. In certain embodiments, the communications interface 670 enables connection to the communication network 103 for providing a proxy-based access list to the UE 105.

The term “computer-readable medium” as used herein refers to any medium that participates in providing information to processor 602, including instructions for execution. Such a medium may take many forms, including, but not limited to computer-readable storage medium (e.g., non-volatile media, volatile media), and transmission media. Non-transitory media, such as non-volatile media, include, for example, optical or magnetic disks, such as storage device 608.

Volatile media include, for example, dynamic memory 604. Transmission media include, for example, twisted pair cables, coaxial cables, copper wire, fiber optic cables, and carrier waves that travel through space without wires or cables, such as acoustic waves and electromagnetic waves, including radio, optical and infrared waves. Signals include man-made transient variations in amplitude, frequency, phase, polarization or other physical properties transmitted through the transmission media. Common forms of computer-readable media include, for example, a floppy disk, a flexible disk, hard disk, magnetic tape, any other magnetic medium, a CD-ROM, CDRW, DVD, any other optical medium, punch cards, paper tape, optical mark sheets, any other physical medium with patterns of holes or other optically recognizable indicia, a RAM, a PROM, an EPROM, a FLASH-EPROM, an EEPROM, a flash memory, any other memory chip or cartridge, a carrier wave, or any other medium from which a computer can read. The term computer-readable storage medium is used herein to refer to any computer-readable medium except transmission media.

Logic encoded in one or more tangible media includes one or both of processor instructions on a computer-readable storage media and special purpose hardware, such as ASIC 620.

Network link 678 typically provides information communication using transmission media through one or more networks to other devices that use or process the information. For example, network link 678 may provide a connection through local network 680 to a host computer 682 or to equipment 684 operated by an Internet Service Provider (ISP). ISP equipment 684 in turn provides data communication services through the public, world-wide packet-switching communication network of networks now commonly referred to as the Internet 690.

A computer called a server host 692 connected to the Internet hosts a process that provides a service in response to information received over the Internet. For example, server host 692 hosts a process that provides information representing video data for presentation at display 614. It is contemplated that the components of system 600 can be deployed in various configurations within other computer systems, e.g., host 682 and server 692.

At least some embodiments of the invention are related to the use of computer system 600 for implementing some or all of the techniques described herein. According to one embodiment of the invention, those techniques are performed by computer system 600 in response to processor 602 executing one or more sequences of one or more processor instructions contained in memory 604. Such instructions, also called computer instructions, software and program code, may be read into memory 604 from another computer-readable medium such as storage device 608 or network link 678. Execution of the sequences of instructions contained in memory 604 causes processor 602 to perform one or more of the method steps described herein. In alternative embodiments, hardware, such as ASIC 620, may be used in place of or in combination with

software to implement the invention. Thus, embodiments of the invention are not limited to any specific combination of hardware and software, unless otherwise explicitly stated herein.

The signals transmitted over network link 678 and other networks through communications interface 670, carry information to and from computer system 600. Computer system 600 can send and receive information, including program code, through the networks 680, 690 among others, through network link 678 and communications interface 670. In an example using the Internet 690, a server host 692 transmits program code for a particular application, requested by a message sent from computer 600, through Internet 690, ISP equipment 684, local network 680 and communications interface 670. The received code may be executed by processor 602 as it is received, or may be stored in memory 604 or in storage device 608 or any other non-volatile storage for later execution, or both. In this manner, computer system 600 may obtain application program code in the form of signals on a carrier wave.

Various forms of computer readable media may be involved in carrying one or more sequence of instructions or data or both to processor 602 for execution. For example, instructions and data may initially be carried on a magnetic disk of a remote computer such as host 682. The remote computer loads the instructions and data into its dynamic memory and sends the instructions and data over a telephone line using a modem. A modem local to the computer system 600 receives the instructions and data on a telephone line and uses an infra-red transmitter to convert the instructions and data to a signal on an infra-red carrier wave serving as the network link 678. An infrared detector serving as communications interface 670 receives the instructions and data carried in the infrared signal and places information representing the instructions and data onto bus 610. Bus 610 carries the information to memory 604 from which processor 602 retrieves and executes the instructions using some of the data sent with the instructions. The instructions and data received in memory 604 may optionally be stored on storage device 608, either before or after execution by the processor 602.

FIG. 7 illustrates a chip set or chip 700 upon which an embodiment of the invention may be implemented. Chip set 700 is programmed to provide a proxy-based access list as described herein and includes, for instance, the processor and memory components described with respect to FIG. 6 incorporated in one or more physical packages (e.g., chips). By way of example, a physical package includes an arrangement of one or more materials, components, and/or wires on a structural assembly (e.g., a baseboard) to provide one or more characteristics such as physical strength, conservation of size, and/or limitation of electrical interaction. It is contemplated that in certain embodiments the chip set 700 can be implemented in a single chip. It is further contemplated that in certain embodiments the chip set or chip 700 can be implemented as a single "system on a chip." It is further contemplated that in certain embodiments a separate ASIC would not be used, for example, and that all relevant functions as disclosed herein would be performed by a processor or processors. Chip set or chip 700, or a portion thereof, constitutes a

means for performing one or more steps of providing user interface navigation information associated with the availability of functions. Chip set or chip 700, or a portion thereof, constitutes a means for performing one or more steps of providing a proxy-based access list.

In one embodiment, the chip set or chip 700 includes a communication mechanism such as a bus 701 for passing information among the components of the chip set 700. A processor 703 has connectivity to the bus 701 to execute instructions and process information stored in, for example, a memory 705. The processor 703 may include one or more processing cores with each core configured to perform independently. A multi-core processor enables multiprocessing within a single physical package. Examples of a multi-core processor include two, four, eight, or greater numbers of processing cores. Alternatively or in addition, the processor 703 may include one or more microprocessors configured in tandem via the bus 701 to enable independent execution of instructions, pipelining, and multithreading. The processor 703 may also be accompanied with one or more specialized components to perform certain processing functions and tasks such as one or more digital signal processors (DSP) 707, or one or more application-specific integrated circuits (ASIC) 709. A DSP 707 typically is configured to process real-world signals (e.g., sound) in real time independently of the processor 703. Similarly, an ASIC 709 can be configured to performed specialized functions not easily performed by a more general purpose processor. Other specialized components to aid in performing the inventive functions described herein may include one or more field programmable gate arrays (FPGA) (not shown), one or more controllers (not shown), or one or more other special-purpose computer chips.

In one embodiment, the chip set or chip 700 includes merely one or more processors and some software and/or firmware supporting and/or relating to and/or for the one or more processors.

The processor 703 and accompanying components have connectivity to the memory 705 via the bus 701. The memory 705 includes both dynamic memory (e.g., RAM, magnetic disk, writable optical disk, etc.) and static memory (e.g., ROM, CD-ROM, etc.) for storing executable instructions that when executed perform the inventive steps described herein to provide a proxy-based access list. The memory 705 also stores the data associated with or generated by the execution of the inventive steps.

FIG. 8 is a diagram of exemplary components of a mobile terminal (e.g., handset) for communications, which is capable of operating in the system of FIG. 1, according to one embodiment. In some embodiments, mobile terminal 801, or a portion thereof, constitutes a means for performing one or more steps of providing a proxy-based access list. Generally, a radio receiver is often defined in terms of front-end and back-end characteristics. The front-end of the receiver encompasses all of the Radio Frequency (RF) circuitry whereas the back-end encompasses all of the base-band processing circuitry. As used in this application, the term "circuitry" refers to both: (1) hardware-only implementations (such as implementations in only

analog and/or digital circuitry), and (2) to combinations of circuitry and software (and/or firmware) (such as, if applicable to the particular context, to a combination of processor(s), including digital signal processor(s), software, and memory(ies) that work together to cause an apparatus, such as a mobile phone or server, to perform various functions). This definition of "circuitry" applies to all uses of this term in this application, including in any claims. As a further example, as used in this application and if applicable to the particular context, the term "circuitry" would also cover an implementation of merely a processor (or multiple processors) and its (or their) accompanying software/or firmware. The term "circuitry" would also cover if applicable to the particular context, for example, a baseband integrated circuit or applications processor integrated circuit in a mobile phone or a similar integrated circuit in a cellular network device or other network devices.

Pertinent internal components of the telephone include a Main Control Unit (MCU) 803, a Digital Signal Processor (DSP) 805, and a receiver/transmitter unit including a microphone gain control unit and a speaker gain control unit. A main display unit 807 provides a display to the user in support of various applications and mobile terminal functions that perform or support the steps of providing a proxy-based access list. The display 807 includes display circuitry configured to display at least a portion of a user interface of the mobile terminal (e.g., mobile telephone). Additionally, the display 807 and display circuitry are configured to facilitate user control of at least some functions of the mobile terminal. An audio function circuitry 809 includes a microphone 811 and microphone amplifier that amplifies the speech signal output from the microphone 811. The amplified speech signal output from the microphone 811 is fed to a coder/decoder (CODEC) 813.

A radio section 815 amplifies power and converts frequency in order to communicate with a base station, which is included in a mobile communication system, via antenna 817. The power amplifier (PA) 819 and the transmitter/modulation circuitry are operationally responsive to the MCU 803, with an output from the PA 819 coupled to the duplexer 821 or circulator or antenna switch, as known in the art. The PA 819 also couples to a battery interface and power control unit 820.

In use, a user of mobile terminal 801 speaks into the microphone 811 and his or her voice along with any detected background noise is converted into an analog voltage. The analog voltage is then converted into a digital signal through the Analog to Digital Converter (ADC) 823. The control unit 803 routes the digital signal into the DSP 805 for processing therein, such as speech encoding, channel encoding, encrypting, and interleaving. In one embodiment, the processed voice signals are encoded, by units not separately shown, using a cellular transmission protocol such as enhanced data rates for global evolution (EDGE), general packet radio service (GPRS), global system for mobile communications (GSM), Internet protocol multimedia subsystem (IMS), universal mobile telecommunications system (UMTS), etc., as well as any other suitable wireless

medium, e.g., microwave access (WiMAX), Long Term Evolution (LTE) networks, code division multiple access (CDMA), wideband code division multiple access (WCDMA), wireless fidelity (WiFi), satellite, and the like, or any combination thereof.

The encoded signals are then routed to an equalizer 825 for compensation of any frequency-dependent impairments that occur during transmission though the air such as phase and amplitude distortion. After equalizing the bit stream, the modulator 827 combines the signal with a RF signal generated in the RF interface 829. The modulator 827 generates a sine wave by way of frequency or phase modulation. In order to prepare the signal for transmission, an up-converter 831 combines the sine wave output from the modulator 827 with another sine wave generated by a synthesizer 833 to achieve the desired frequency of transmission. The signal is then sent through a PA 819 to increase the signal to an appropriate power level. In practical systems, the PA 819 acts as a variable gain amplifier whose gain is controlled by the DSP 805 from information received from a network base station. The signal is then filtered within the duplexer 821 and optionally sent to an antenna coupler 835 to match impedances to provide maximum power transfer. Finally, the signal is transmitted via antenna 817 to a local base station. An automatic gain control (AGC) can be supplied to control the gain of the final stages of the receiver. The signals may be forwarded from there to a remote telephone which may be another cellular telephone, any other mobile phone or a land-line connected to a Public Switched Telephone Network (PSTN), or other telephony networks.

Voice signals transmitted to the mobile terminal 801 are received via antenna 817 and immediately amplified by a low noise amplifier (LNA) 837. A down-converter 839 lowers the carrier frequency while the demodulator 841 strips away the RF leaving only a digital bit stream. The signal then goes through the equalizer 825 and is processed by the DSP 805. A Digital to Analog Converter (DAC) 843 converts the signal and the resulting output is transmitted to the user through the speaker 845, all under control of a Main Control Unit (MCU) 803 which can be implemented as a Central Processing Unit (CPU) (not shown).

The MCU 803 receives various signals including input signals from the keyboard 847. The keyboard 847 and/or the MCU 803 in combination with other user input components (e.g., the microphone 811) comprise a user interface circuitry for managing user input. The MCU 803 runs a user interface software to facilitate user control of at least some functions of the mobile terminal 801 to provide a proxy-based access list. The MCU 803 also delivers a display command and a switch command to the display 807 and to the speech output switching controller, respectively. Further, the MCU 803 exchanges information with the DSP 805 and can access an optionally incorporated SIM card 849 and a memory 851. In addition, the MCU 803 executes various control functions required of the terminal. The DSP 805 may, depending upon the implementation, perform any of a variety of conventional digital processing functions on the voice signals. Additionally, DSP 805 determines the background noise level of the local environment

from the signals detected by microphone 811 and sets the gain of microphone 811 to a level selected to compensate for the natural tendency of the user of the mobile terminal 801.

The CODEC 813 includes the ADC 823 and DAC 843. The memory 851 stores various data including call incoming tone data and is capable of storing other data including music data received via, e.g., the global Internet. The software module could reside in RAM memory, flash memory, registers, or any other form of writable storage medium known in the art. The memory device 851 may be, but not limited to, a single memory, CD, DVD, ROM, RAM, EEPROM, optical storage, magnetic disk storage, flash memory storage, or any other non-volatile storage medium capable of storing digital data.

An optionally incorporated SIM card 849 carries, for instance, important information, such as the cellular phone number, the carrier supplying service, subscription details, and security information. The SIM card 849 serves primarily to identify the mobile terminal 801 on a radio network. The card 849 also contains a memory for storing a personal telephone number registry, text messages, and user specific mobile terminal settings.

While the invention has been described in connection with a number of embodiments and implementations, the invention is not so limited but covers various obvious modifications and equivalent arrangements, which fall within the purview of the appended claims. Although features of the invention are expressed in certain combinations among the claims, it is contemplated that these features can be arranged in any combination and order.

CLAIMS

WHAT IS CLAIMED IS:

1. A method comprising facilitating a processing of and/or processing (1) data and/or (2) information and/or (3) at least one signal, the (1) data and/or (2) information and/or (3) at least one signal based, at least in part, on the following:

an input for specifying access information for one or more communication endpoints accessible via a proxy server; and

a processing of the access information to generate one or more access policies with respect to the one or more communication endpoints,

wherein access to the one or more communication endpoints via the proxy server is provided based, at least in part, on the one or more access policies.

2. A method of claim 1, wherein the input is received from, at least in part, one or more client devices of the proxy server, one or more other devices, one or more third-party sources, or a combination thereof.

3. A method of any of claims 1-2, wherein the (1) data and/or (2) information and/or (3) at least one signal are further based, at least in part, on the following:

a request for access to at least one of the one or more communication endpoints via the proxy server; and

a processing of the request and the one or more access policies to determine whether to grant, deny, or restrict the access to the at least one of the one or more communication endpoints.

4. A method of claim 3, wherein the (1) data and/or (2) information and/or (3) at least one signal are further based, at least in part, on the following:

a notification message based, at least in part, on the request, the one or more access policies, the access information, or a combination thereof.

5. A method of claim 4, wherein the notification message specifies, at least in part, a number of users reporting the access information, a date of the access information, one or more flags, or a combination thereof.

6. A method of any of claims 3-5, wherein the (1) data and/or (2) information and/or (3) at least one signal are further based, at least in part, on the following:

social networking information associated with a user of a device from which the request was received; and

a processing of the social networking information to filter at least a portion of the access information, the one or more access policies, or a combination thereof associated with one or more social networks of the user.

7. A method of any of claims 1-6, wherein the access information includes, at least in part, one or more reports regarding risk information, objectionable information, or a combination thereof associated with the one or more communication endpoints.

8. A method of any of claims 1-7, wherein the (1) data and/or (2) information and/or (3) at least one signal are further based, at least in part, on the following:

a generation of one or more blacklists, one or more whitelists, or a combination thereof regarding the one or more communication endpoints,

wherein the one or more access policies are based, at least in part, on the one or more blacklists, the one or more whitelists, or a combination thereof.

9. An apparatus comprising:

at least one processor; and

at least one memory including computer program code for one or more programs,

the at least one memory and the computer program code configured to, with the at least one processor, cause the apparatus to perform at least the following,

receive an input for specifying access information for one or more communication endpoints accessible via a proxy server; and

process and/or facilitate a processing of the access information to generate one or more access policies with respect to the one or more communication endpoints,

wherein access to the one or more communication endpoints via the proxy server is provided based, at least in part, on the one or more access policies.

10. An apparatus of claim 9, wherein the input is received from, at least in part, one or more client devices of the proxy server, one or more other devices, one or more third-party sources, or a combination thereof.

11. An apparatus of any of claims 9-10, wherein the apparatus is further caused to:

receive a request for access to at least one of the one or more communication endpoints via the proxy server; and

process and/or facilitate a processing of the request and the one or more access policies to determine whether to grant, deny, or restrict the access to the at least one of the one or more communication endpoints.

12. An apparatus of claim 11, wherein the apparatus is further caused to:

determine to present a notification message based, at least in part, on the request, the one or more access policies, the access information, or a combination thereof.

13. An apparatus of claim 12, wherein the notification message specifies, at least in part, a number of users reporting the access information, a date of the access information, one or more flags, or a combination thereof.

14. An apparatus of any of claims 11-13, wherein the apparatus is further caused to:

determine social networking information associated with a user of a device from which the request was received; and

process and/or facilitate a processing of the social networking information to filter at least a portion of the access information, the one or more access policies, or a combination thereof associated with one or more social networks of the user.

15. An apparatus of any of claims 9-14, wherein the access information includes, at least in part, one or more reports regarding risk information, objectionable information, or a combination thereof associated with the one or more communication endpoints.

16. An apparatus of any of claims 9-15, wherein the apparatus is further caused to:

cause, at least in part, a generation of one or more blacklists, one or more whitelists, or a combination thereof regarding the one or more communication endpoints,

wherein the one or more access policies are based, at least in part, on the one or more blacklists, the one or more whitelists, or a combination thereof.

17. A computer-readable storage medium carrying one or more sequences of one or more instructions which, when executed by one or more processors, cause an apparatus to at least perform the following steps:

receiving an input for specifying access information for one or more communication endpoints accessible via a proxy server; and

processing and/or facilitating a processing of the access information to generate one or more access policies with respect to the one or more communication endpoints,

wherein access to the one or more communication endpoints via the proxy server is provided based, at least in part, on the one or more access policies.

18. A computer-readable storage medium of claim 17, wherein the input is received from, at least in part, one or more client devices of the proxy server, one or more other devices, one or more third-party sources, or a combination thereof.

19. A computer-readable storage medium of any of claims 17-18, wherein the apparatus is caused to further perform:

receiving a request for access to at least one of the one or more communication endpoints via the proxy server; and

processing and/or facilitating a processing of the request and the one or more access policies to determine whether to grant, deny, or restrict the access to the at least one of the one or more communication endpoints.

20. A computer-readable storage medium of claim 19, wherein the apparatus is caused to further perform:

determining to present a notification message based, at least in part, on the request, the one or more access policies, the access information, or a combination thereof.

21. A method comprising:

receiving an input for specifying access information for one or more communication endpoints accessible via a proxy server; and

processing and/or facilitating a processing of the access information to generate one or more access policies with respect to the one or more communication endpoints,

wherein access to the one or more communication endpoints via the proxy server is provided based, at least in part, on the one or more access policies.

22. A method of claim 21, wherein the input is received from, at least in part, one or more client devices of the proxy server, one or more other devices, one or more third-party sources, or a combination thereof.

23. A method of any of claims 21-22, further comprising:

receiving a request for access to at least one of the one or more communication endpoints via the proxy server; and

processing and/or facilitating a processing of the request and the one or more access policies to determine whether to grant, deny, or restrict the access to the at least one of the one or more communication endpoints.

24. A method of claim 23, further comprising:

determining to present a notification message based, at least in part, on the request, the one or more access policies, the access information, or a combination thereof.

25. A method of claim 24, wherein the notification message specifies, at least in part, a number of users reporting the access information, a date of the access information, one or more flags, or a combination thereof.

26. A method of any of claims 23-25, further comprising:

determining social networking information associated with a user of a device from which the request was received; and

processing and/or facilitating a processing of the social networking information to filter at least a portion of the access information, the one or more access policies, or a combination thereof associated with one or more social networks of the user.

27. A method of any of claims 21-26, wherein the access information includes, at least in part, one or more reports regarding risk information, objectionable information, or a combination thereof associated with the one or more communication endpoints.

28. A method of any of claims 21-27, further comprising:

causing, at least in part, a generation of one or more blacklists, one or more whitelists, or a combination thereof regarding the one or more communication endpoints,

wherein the one or more access policies are based, at least in part, on the one or more blacklists, the one or more whitelists, or a combination thereof.

29. An apparatus comprising:

at least one processor; and

at least one memory including computer program code for one or more programs,

the at least one memory and the computer program code configured to, with the at least one processor, cause the apparatus to perform at least the following,

receive an input for specifying access information for one or more communication endpoints accessible via a proxy server; and

process and/or facilitate a processing of the access information to generate one or more access policies with respect to the one or more communication endpoints,

wherein access to the one or more communication endpoints via the proxy server is provided based, at least in part, on the one or more access policies.

30. An apparatus of claim 29, wherein the input is received from, at least in part, one or more client devices of the proxy server, one or more other devices, one or more third-party sources, or a combination thereof.

31. An apparatus of any of claims 29-30, wherein the apparatus is further caused to:

receive a request for access to at least one of the one or more communication endpoints via the proxy server; and

process and/or facilitate a processing of the request and the one or more access policies to determine whether to grant, deny, or restrict the access to the at least one of the one or more communication endpoints.

32. An apparatus of claim 31, wherein the apparatus is further caused to:

determine to present a notification message based, at least in part, on the request, the one or more access policies, the access information, or a combination thereof.

33. An apparatus of claim 32, wherein the notification message specifies, at least in part, a number of users reporting the access information, a date of the access information, one or more flags, or a combination thereof.

34. An apparatus of any of claims 31-33, wherein the apparatus is further caused to:

determine social networking information associated with a user of a device from which the request was received; and

process and/or facilitate a processing of the social networking information to filter at least a portion of the access information, the one or more access policies, or a combination thereof associated with one or more social networks of the user.

35. An apparatus of any of claims 29-34, wherein the access information includes, at least in part, one or more reports regarding risk information, objectionable information, or a combination thereof associated with the one or more communication endpoints.

36. An apparatus of any of claims 29-35, wherein the apparatus is further caused to:

cause, at least in part, a generation of one or more blacklists, one or more whitelists, or a combination thereof regarding the one or more communication endpoints,

wherein the one or more access policies are based, at least in part, on the one or more blacklists, the one or more whitelists, or a combination thereof.

37. An apparatus of any of claims 29-36, wherein the apparatus is a mobile phone further comprising:

user interface circuitry and user interface software configured to facilitate user control of at least some functions of the mobile phone through use of a display and configured to respond to user input; and

a display and display circuitry configured to display at least a portion of a user interface of the mobile phone, the display and display circuitry configured to facilitate user control of at least some functions of the mobile phone.

38. A computer-readable storage medium carrying one or more sequences of one or more instructions which, when executed by one or more processors, cause an apparatus to at least perform a method of at least one of claims 1-8 and/or 21-28.

39. An apparatus comprising means for performing a method of at least one of claims 1-8 and/or 21-28.

40. An apparatus of claim 39, wherein the apparatus is a mobile phone further comprising:

user interface circuitry and user interface software configured to facilitate user control of at least some functions of the mobile phone through use of a display and configured to respond to user input; and

a display and display circuitry configured to display at least a portion of a user interface of the mobile phone, the display and display circuitry configured to facilitate user control of at least some functions of the mobile phone.

41. A computer program product including one or more sequences of one or more instructions which, when executed by one or more processors, cause an apparatus to at least perform the steps of a method of at least one of claims 1-8 and/or 21-28.

42. A method comprising facilitating access to at least one interface configured to allow access to at least one service, the at least one service configured to perform a method of at least one of claims 1-8 and/or 21-28.

43. A method comprising facilitating a processing of and/or processing (1) data and/or (2) information and/or (3) at least one signal, the (1) data and/or (2) information and/or (3) at least one signal based, at least in part, on the method of at least one of claims 1-8 and/or 21-28.

44. A method comprising facilitating creating and/or facilitating modifying (1) at least one device user interface element and/or (2) at least one device user interface functionality, the (1) at least one device user interface element and/or (2) at least one device user interface functionality based, at least in part, on the method of at least one of claims 1-8 and/or 21-28.

45. An apparatus of any of claims 9-16, wherein the apparatus is a mobile phone further comprising:

user interface circuitry and user interface software configured to facilitate user control of at least some functions of the mobile phone through use of a display and configured to respond to user input; and

a display and display circuitry configured to display at least a portion of a user interface of the mobile phone, the display and display circuitry configured to facilitate user control of at least some functions of the mobile phone.

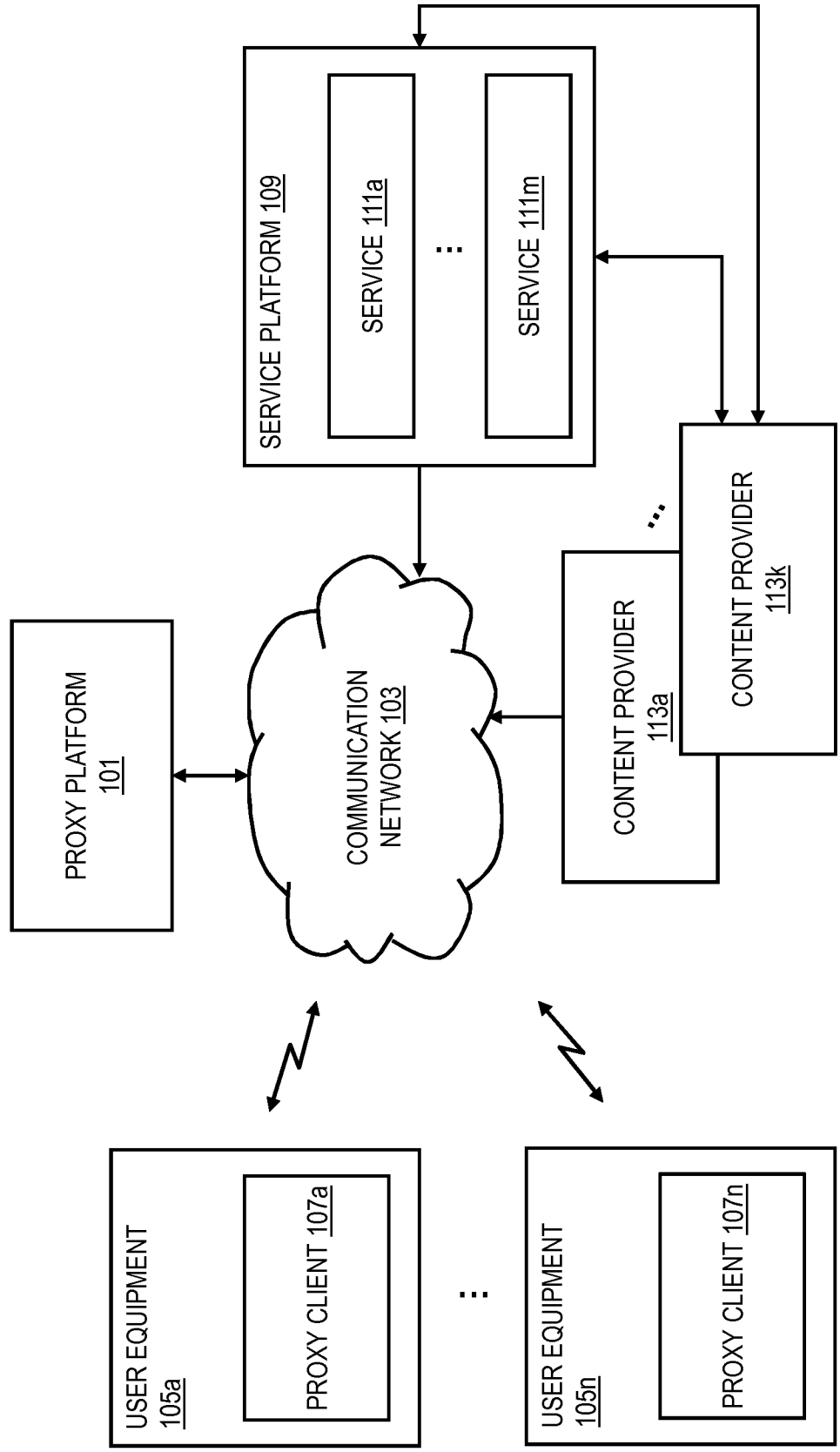

100
PROXY PLATFORM 101
COMMUNICATION NETWORK 103
SERVICE PLATFORM 109
SERVICE 111a
SERVICE 111m
CONTENT PROVIDER 113a
CONTENT PROVIDER 113k
USER EQUIPMENT 105a
PROXY CLIENT 107a
USER EQUIPMENT 105n
PROXY CLIENT 107n

FIG. 1

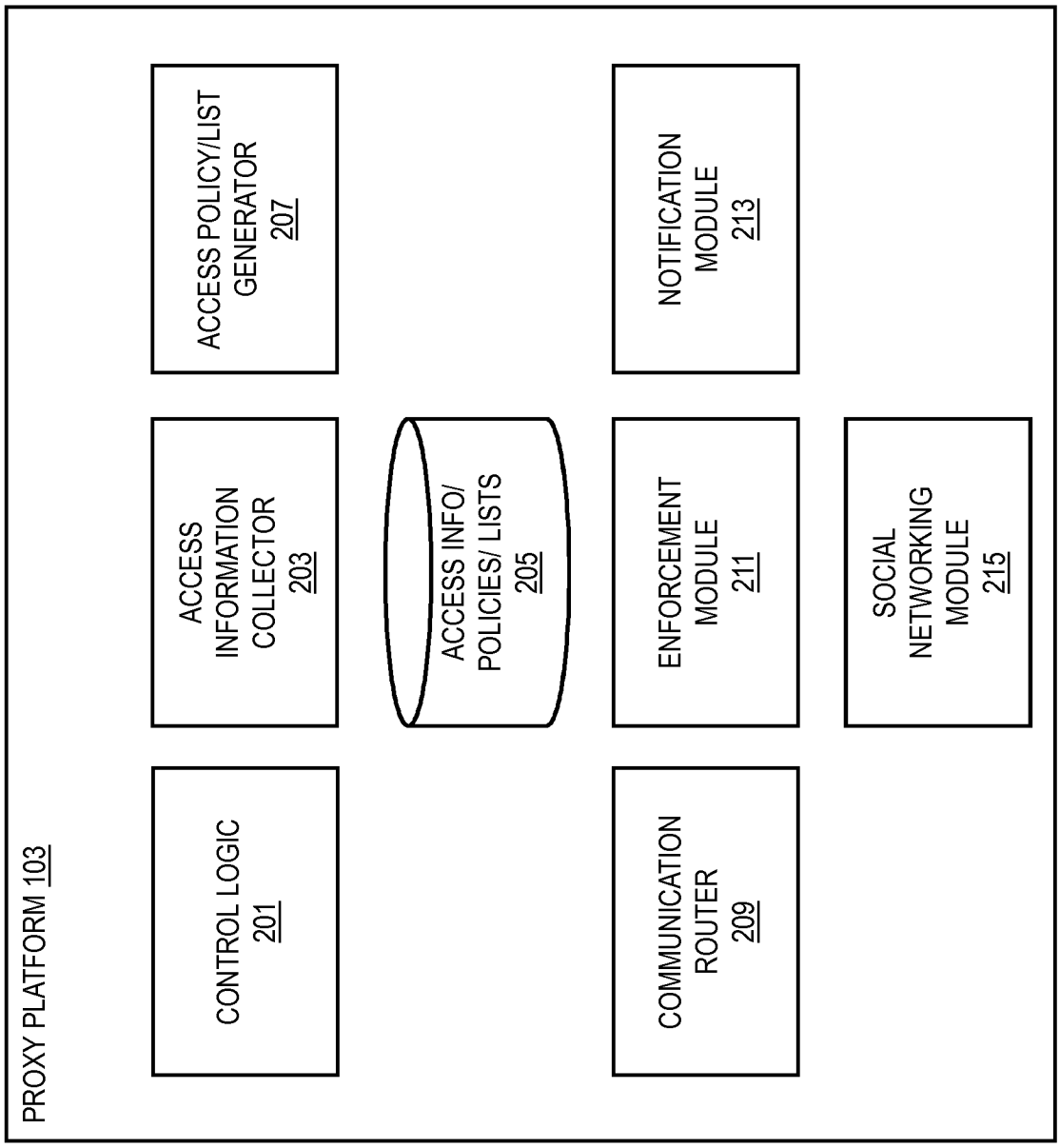

PROXY PLATFORM 103
CONTROL LOGIC 201
ACCESS INFORMATION COLLECTOR 203
ACCESS POLICY/LIST GENERATOR 207
ACCESS INFO/ POLICIES/ LISTS 205
COMMUNICATION ROUTER 209
ENFORCEMENT MODULE 211
NOTIFICATION MODULE 213
SOCIAL NETWORKING MODULE 215

FIG. 2

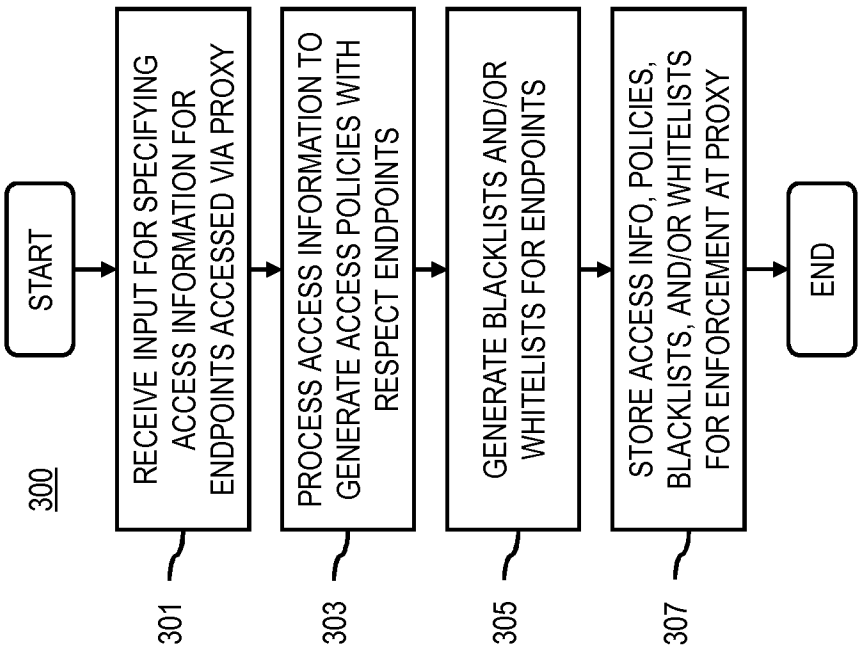

300
START
RECEIVE INPUT FOR SPECIFYING ACCESS INFORMATION FOR ENDPOINTS ACCESSED VIA PROXY
PROCESS ACCESS INFORMATION TO GENERATE ACCESS POLICIES WITH RESPECT ENDPOINTS
GENERATE BLACKLISTS AND/OR WHITELISTS FOR ENDPOINTS
STORE ACCESS INFO, POLICIES, BLACKLISTS, AND/OR WHITELISTS FOR ENFORCEMENT AT PROXY
END
301
303
305
307

FIG. 3

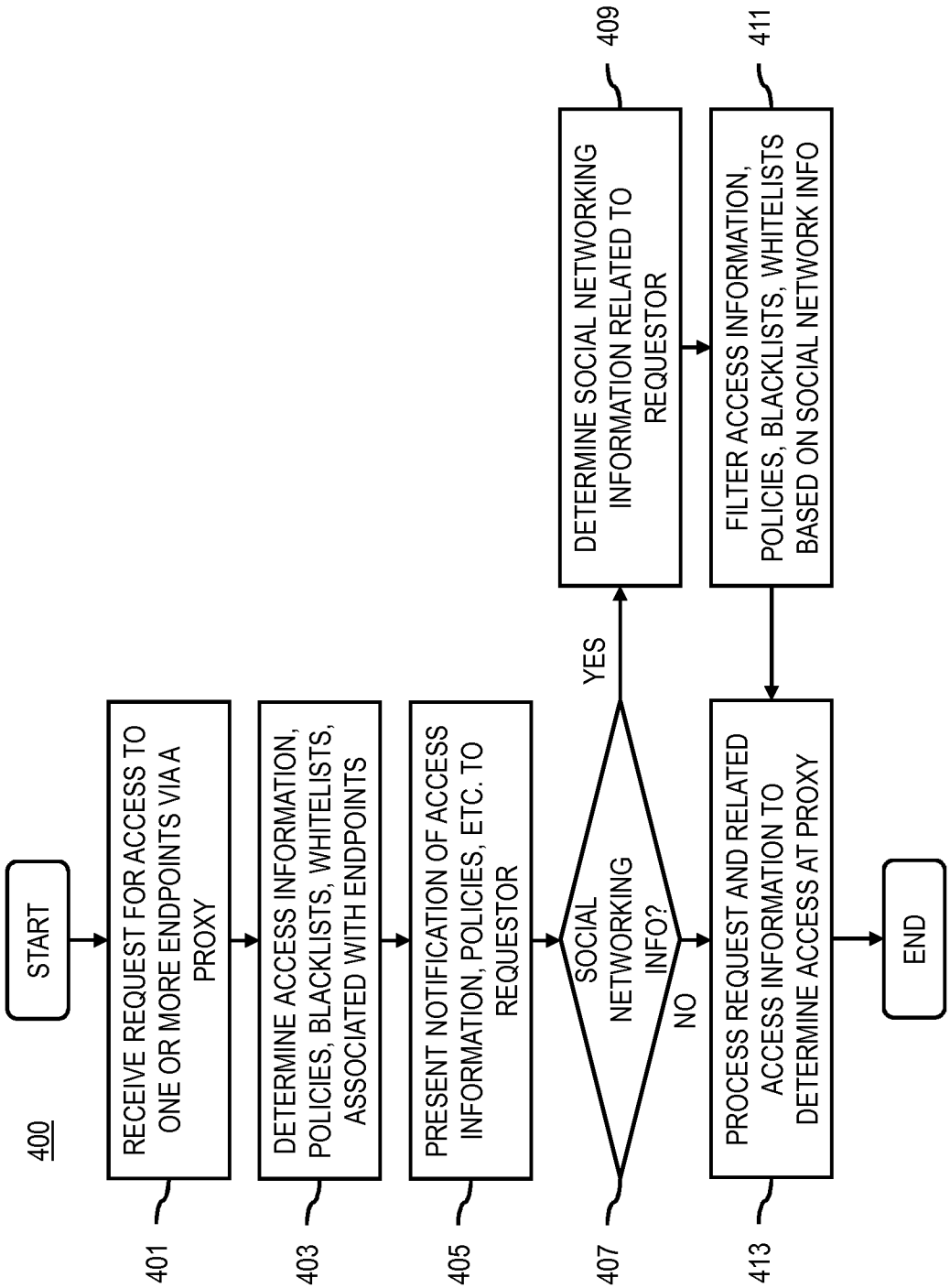

400
START
RECEIVE REQUEST FOR ACCESS TO ONE OR MORE ENDPOINTS VIA A PROXY
401
DETERMINE ACCESS INFORMATION, POLICIES, BLACKLISTS, WHITELISTS, ASSOCIATED WITH ENDPOINTS
403
PRESENT NOTIFICATION OF ACCESS INFORMATION, POLICIES, ETC. TO REQUESTOR
405
SOCIAL NETWORKING INFO?
407
YES
NO
DETERMINE SOCIAL NETWORKING INFORMATION RELATED TO REQUESTOR
409
FILTER ACCESS INFORMATION, POLICIES, BLACKLISTS, WHITELISTS BASED ON SOCIAL NETWORK INFO
411
PROCESS REQUEST AND RELATED ACCESS INFORMATION TO DETERMINE ACCESS AT PROXY
413
END

FIG. 4

FIG. 5A

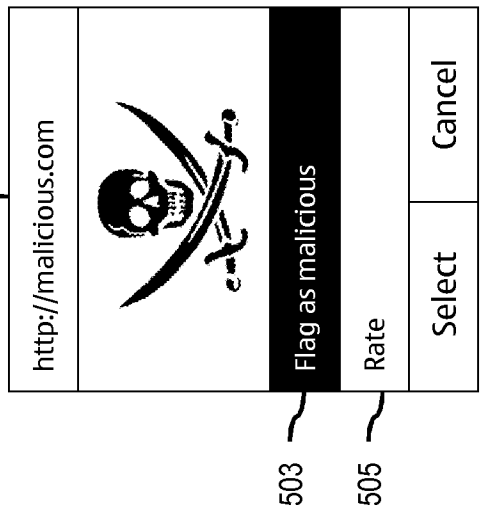
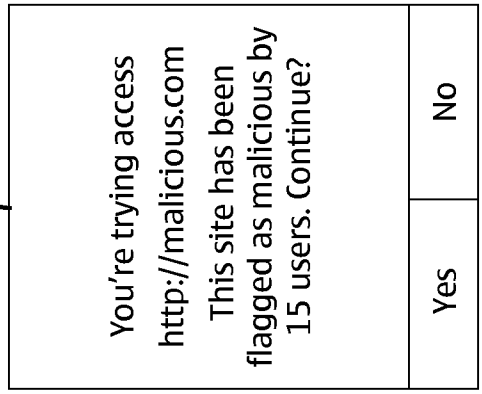

501
http://malicious.com
Flag as malicious
Rate
Select
Cancel
503
505

FIG. 5B


521
You're trying access http://malicious.com This site has been flagged as malicious by 15 users. Continue?
Yes
No

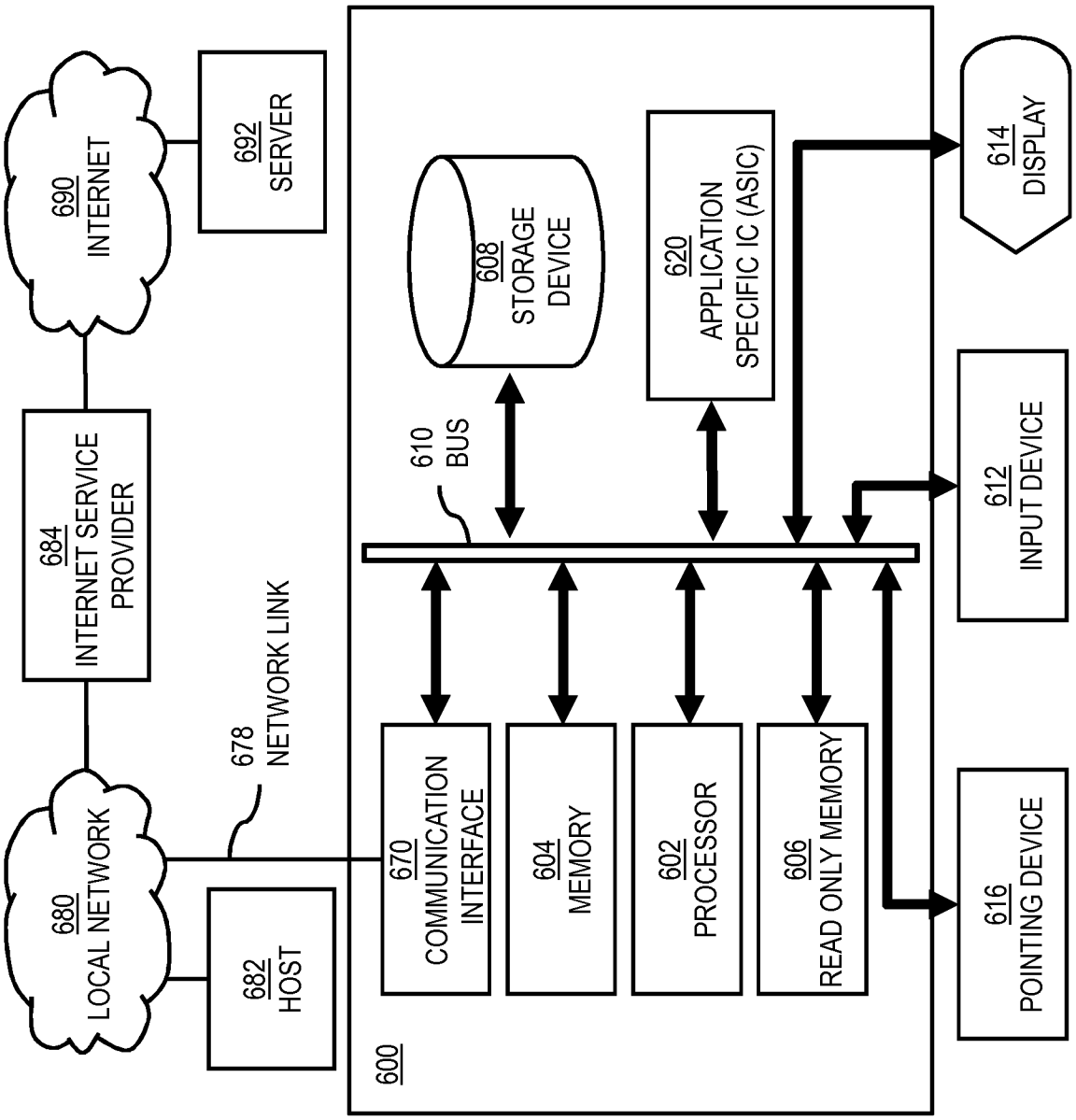

690 INTERNET
692 SERVER
684 INTERNET SERVICE PROVIDER
678 NETWORK LINK
680 LOCAL NETWORK
682 HOST
600
670 COMMUNICATION INTERFACE
604 MEMORY
602 PROCESSOR
606 READ ONLY MEMORY
610 BUS
608 STORAGE DEVICE
620 APPLICATION SPECIFIC IC (ASIC)
614 DISPLAY
612 INPUT DEVICE
616 POINTING DEVICE

FIG. 6

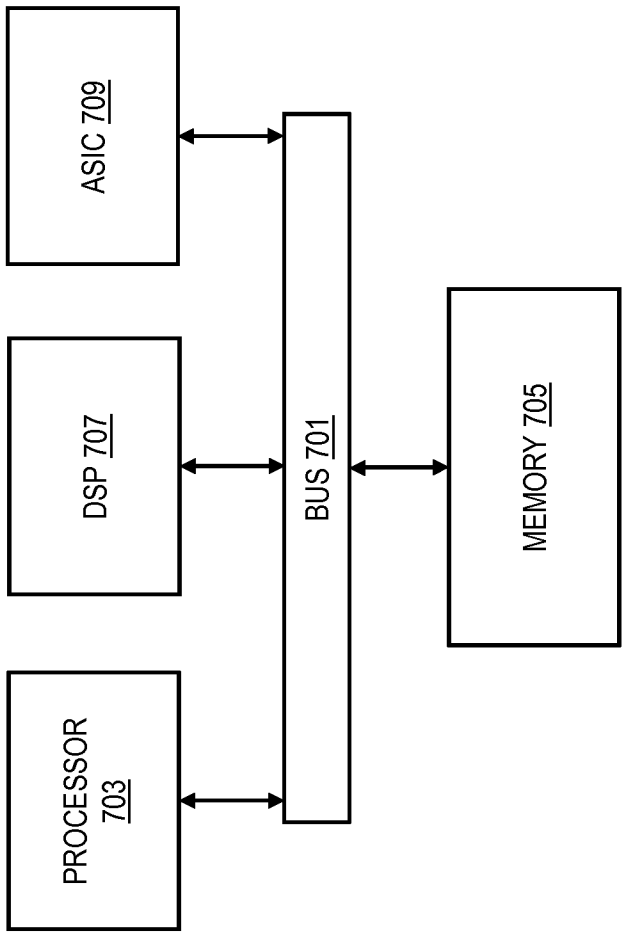
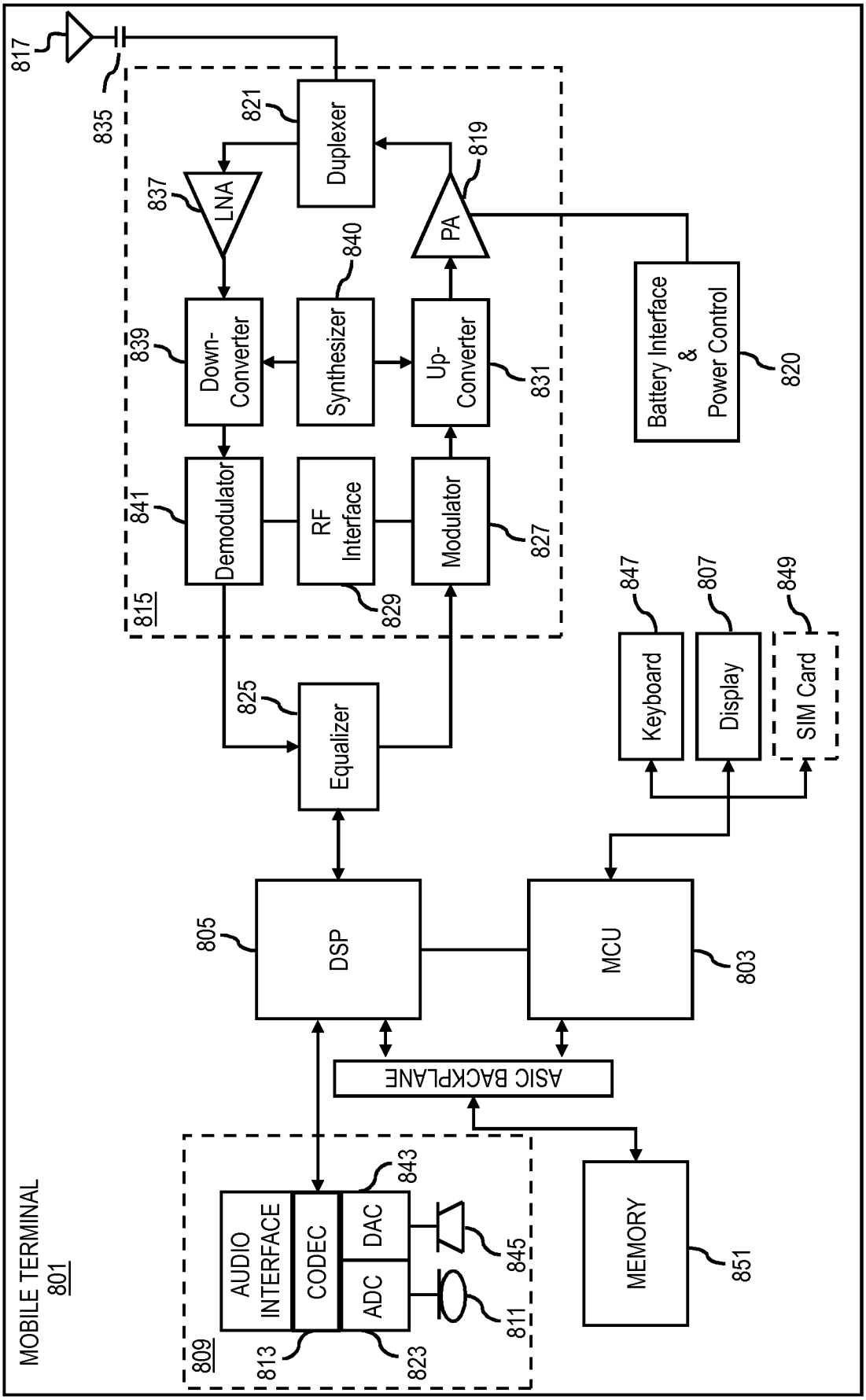


FIG. 7

FIG. 8


MOBILE TERMINAL
801
817
835
821
Duplexer
819
837
LNA
PA
840
Synthesizer
839
Down-
Converter
Up-
Converter
831
Battery Interface
&
Power Control
820
841
Demodulator
RF
Interface
Modulator
827
829
815
825
Equalizer
847
Keyboard
807
Display
849
SIM Card
805
DSP
MCU
803
ASIC BACKPLANE
809
AUDIO
INTERFACE
CODEC
DAC
ADC
843
845
811
813
823
MEMORY
851

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI2012/050169

A. CLASSIFICATION OF SUBJECT MATTER

See extra sheet

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)

IPC: G06F, H04L

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

FI, SE, NO, DK

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

EPO-Internal, WPI, INSPEC, XPIPCOM, XPI3E, XP3GPP, XPETSI

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2004111870 A1 (FREEMAN JAMES) 23 December 2004 (23.12.2004) page 9, line 4 – page 10, line 26	1-45
A	WO 2006054276 A1 (WHELAN JOHN et al.) 26 May 2006 (26.05.2006)	1-45
A	US 2010036779 A1 (SADEH-KONIECPOL NORMAN et al.) 11 February 2010 (11.02.2010) paragraph [0051]	1-45
A	US 2007180510 A1 (LONG DARRELL et al.) 02 August 2007 (02.08.2007)	1-45

☐ 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	Date of mailing of the international search report
18 May 2012 (18.05.2012)	22 May 2012 (22.05.2012)

Name and mailing address of the ISA/FI
National Board of Patents and Registration of Finland
P.O. Box 1160, FI-00101 HELSINKI, Finland
Facsimile No. +358 9 6939 5328

Authorized officer
Tapio Ikäheimo
Telephone No. +358 9 6939 500

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/FI2012/050169

Patent document cited in search report	Publication date	Patent family members(s)	Publication date
WO 2004111870 A1	23/12/2004	None	
WO 2006054276 A1	26/05/2006	IE 20050764 A2 IE 20050763 A1	14/06/2006 14/06/2006
US 2010036779 A1	11/02/2010	None	
US 2007180510 A1	02/08/2007	None	

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI2012/050169

CLASSIFICATION OF SUBJECT MATTER

Int.Cl.
H04L 29/08 (2006.01)
H04L 29/06 (2006.01)
G06F 17/30 (2006.01)