Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2871249 A1 2016/05/10

(21) 2 871 249

(12) DEMANDE DE BREVET CANADIEN
CANADIAN PATENT APPLICATION

(13) A1

(22) Date de dépôt/Filing Date: 2014/11/10

(41) Mise à la disp. pub./Open to Public Insp.: 2016/05/10

(51) Cl.Int./Int.Cl. *H04W 4/26* (2009.01), *H04W 4/00* (2009.01), *H04W 4/14* (2009.01)

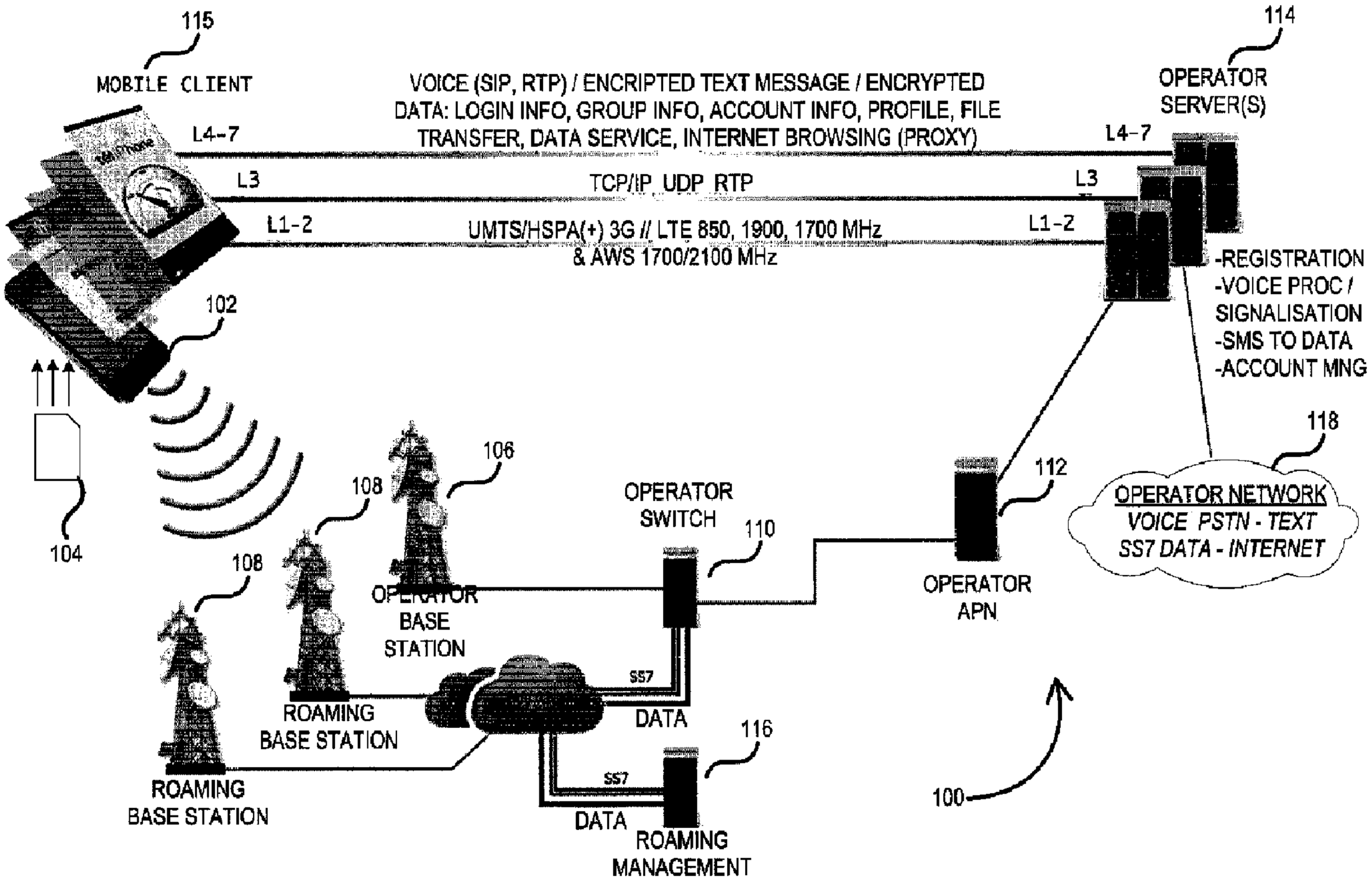
(71) Demandeur/Applicant:
INVESTEL CAPITAL CORPORATION, CA

(72) Inventeur/Inventor:
LALIBERTE, BENOIT, CA

(74) Agent: MERIZZI RAMSBOTTOM & FORSTER

(54) Titre : SYSTEME D'ABONNE MOBILE TOUT DONNEES ET METHODE, ET DISPOSITIF DE TELEPHONE INTELLIGENT-DONNEES MOBILE ET ENVIRONNEMENT INFORMATIQUE ASSOCIE

(54) Title: ALL-DATA MOBILE SUBSCRIBER SYSTEM AND METHOD, AMD MOBILE SMARTPHONE-OVER-DATA DEVICE AND COMPUTER-IMPLEMENTED ENVIRONMENT THEREFOR



(57) Abrégé/Abstract:
Described are various embodiments of an all-data mobile subscriber system and method, and mobile smartphone-over-data device and computer-implemented environment therefor. In some embodiments, a subscriber to a mobile network may gain access to

(21) 2 871 249

(13) A1

(57) Abrégé(suite)/Abstract(continued):
both telephony-over-data (e.g. voice and/or SMS) and other traditionally data-based services over a combined all-data mobile subscription package via a virtualized smartphone-over-data application executed on their mobile device and interfacing through a same data network access point to access all network data services and communications.

ABSTRACT

Described are various embodiments of an all-data mobile subscriber system and method, and mobile smartphone-over-data device and computer-implemented environment therefor. In some embodiments, a subscriber to a mobile network may gain access to both telephony-over-data (e.g. voice and/or SMS) and other traditionally data-based services over a combined all-data mobile subscription package via a virtualized smartphone-over-data application executed on their mobile device and interfacing through a same data network access point to access all network data services and communications.

ALL-DATA MOBILE SUBSCRIBER SYSTEM AND METHOD, AND MOBILE SMARTPHONE-OVER-DATA DEVICE AND COMPUTER-IMPLEMENTED ENVIRONMENT THEREFOR

FIELD OF THE DISCLOSURE

[0001] The present disclosure relates to mobile communications, and in particular, to an all-data mobile subscriber system and method, and mobile smartphone-over-data device and computer-implemented environment therefor.

BACKGROUND

[0002] Mobile communication services are regulated in most jurisdictions and rely on a selection of regulated mobile service providers and network operators to deliver various mobile telephony and data services, such as mobile telephone services including voicemail, call forwarding, conference calls, call transfers and the like; texting or messaging services such as SMS (Short Message Service), EMS (Extended Message Service), MMS (Multimedia Messaging Service); and data services including Internet browsing access, e-mail, Webmail, social media applications, content sharing platforms, etc.

[0003] Generally, each mobile communication device, which may range from the most basic mobile telephony cellphone (e.g. SMS, voice), to the more advanced smartphone or tablet (e.g. text and multimedia messaging, Internet browsing and data sharing platforms/applications, mobile telephony, camera, video, Bluetooth™ connectivity, Near Field Communication (NFC) connectivity, etc.), will interface with and share voice, text and/or multimedia data over a mobile communication network (e.g. a cellular network encompassing both a circuit switched network for voice and SMS and a packet switched network for multimedia data) owned and operated by a mobile network operator (MNO), also known as a wireless service provider, wireless carrier, cellular company, or mobile network carrier. Generally, the MNO is a provider of wireless communication services that owns or controls all the elements necessary to sell and deliver services to an end user including radio spectrum allocation, wireless network

infrastructure, back haul infrastructure, billing, customer care, etc. Each MNO will also generally own or control access to a radio spectrum license from a regulatory or government entity, and own or control the elements of the network infrastructure necessary to provide services to subscribers over the licensed spectrum. Cellphone users may also interface with a Mobile Virtual Network Operator (MVNO), or Mobile Other Licensed Operator (MOLO) that does not own the wireless network infrastructure over which it provides services to its customers, but that has entered into a business agreement with an MNO to obtain bulk access to network services at wholesale rates (e.g. to make use of an underused network infrastructure), and set retail prices independently. The MVNO may use its own customer service, billing support systems, marketing and sales personnel or it may employ the services of a mobile virtual network enabler or the like. The MVNO may in some cases seek to market an alternative brand of services, packages and/or prices to possibly target an undermarketed share of potential or current mobile users in a given area, while using the existing infrastructure provided by the MNO.

[0004] In general, most MNOs and MVNOs will be involved in the retailing of mobile communication devices (cellular phones, smartphones, tablets and other cell-enabled communication devices) loaded with an operator and user-specific subscriber identity or identification module or SIM card for GSM-network enabled devices, a removable user identity module or R-UIM card for use on CDMA networks, a universal integrated circuit card or UICC for use on UMTS networks, and the like, as readily known in the art. For simplicity, focus will be made here on GSM-enabled devices common in North America and other parts of the world, though similarities and equivalents will be naturally known to the skilled artisan in considering devices and applications relying on other wireless network standards.

[0005] A SIM card basically consists of an integrated circuit that securely stores the international mobile subscriber identity (IMSI) and the related key (Ki) used to identify and authenticate subscribers on mobile communication devices. A SIM card also stores its unique serial number or integrated circuit card identifier (ICCID), temporary information related to the local network (routinely exchanged with the Location Area Identity (LAI), a list of the services the user has access to and two passwords: a personal

identification number (PIN) for ordinary use and a personal unblocking code (PUK) for PIN unlocking. Some operators will lock the SIM to a particular device, particularly where a subscriber is bound to a long-term service agreement with the MNO, while others will allow different SIM cards to be used with a same device, for example where a user seeks to draw services from multiple network operators, for example, in different geographic regions. Recent devices also allow for multiple SIM cards to be used with a same device, for example in selecting which operator to use for which service, or in operating different contact telephony numbers for different regions, for example.

[0006] In practice, a new subscriber can purchase a new device from a network operator retail that may at times provide such devices at a discounted rate in exchange for a long-term subscription commitment from the new subscriber. Subscription packages will generally include allocated time or minutes for local, national and/or international telephone voice calls sent and/or received in association with a phone number registered with the new device's SIM card. This allocated time will often be segregated into different timeslots such as weekday daytime minutes, evenings and weekend minutes, or again providing unlimited telephone voice services during certain off-peak periods or for a selected subset of predefined contact numbers. Subscriber packages may also include a SMS and/or MMS, i.e. texting component (e.g. number of included outbound and/or inbound simple/multimedia messages per month), and a data package generally identifying an included data transfer allotment expressed in megabytes/gigabytes (MB/GB) for the user's device. Applicable surcharge rates for overages in local and/or long distance telephone voice minutes, text-based messages and/or data usage are also generally explicitly defined, as can be additional roaming charges applicable when the registered user operates its device outside the operator's home network.

[0007] The purchased device will come pre-loaded with an operator-specific SIM card that is configured on the spot to uniquely identify the subscriber, the services accessible thereto via the operator's home network (and other networks via roaming agreements established between the local operator and operators of such other networks), and in some configurations, lock the SIM card, and thus the user, to this particular device and network operator. Alternatively, a user may purchase an operator-specific SIM card

for use with an existing phone, and have this SIM card uniquely configured and activated as noted above for user and service specificity. Other service options such as pay-as-you go, prepaid phones, and the like, operate more or less as noted above, with the user's personal identity being intrinsically associated with the device's SIM card and associated service restrictions/allocations.

[0008] Given the regulated access to available spectrum in many jurisdictions, often limited to a restricted subset of operators or the like, competition on mobile services fees has been constrained and prices generally remain relatively high despite the increased prevalence of such services and the proliferation of subscribers worldwide. In order to circumvent some of the more onerous fees associated with telephone voice or text-based services offered by network operators, some subscribers have taken to alternative technologies and applications, for instance exchanging voice-telephony communications for available mobile voice-over-data (e.g. VoIP) applications such as Skype™ or Facetime™, and exchanging text-based telephony communications for available text-based data-network applications such as Blackberry Messenger™. Regardless, the standard operator-subscriber and subscriber-device relationships remain unchanged and continue to constrain user flexibility and access to more affordable and/or flexible services.

[0009] This background information is provided to reveal information believed by the applicant to be of possible relevance. No admission is necessarily intended, nor should be construed, that any of the preceding information constitutes prior art.

SUMMARY

[0010] The following presents a simplified summary of the general inventive concept(s) described herein to provide a basic understanding of some aspects of the invention. This summary is not an extensive overview of the invention. It is not intended to restrict key or critical elements of the invention or to delineate the scope of the invention beyond that which is explicitly or implicitly described by the following description and claims.

[0011] A need exists for an all-data mobile subscriber system and method, and mobile smartphone-over-data device and computer-implemented environment therefor, that overcome some of the drawbacks of known systems, or at least, provides a useful alternative thereto. Some aspects of this disclosure provide examples of such systems and methods, in accordance with difference embodiments of the invention.

[0012] In accordance with one broad aspect, there is provided a mobile subscriber network in which a subscriber may gain access to both telephony-over-data (e.g. voice and/or SMS) and other traditionally data-based mobile services over a combined all-data mobile subscription package. In one such embodiment the subscriber gains such access via a virtualized smartphone-over-data application executed on their mobile device and interfacing through a same data network access point to access all network data services and communications.

[0013] In accordance with one aspect there is provided a mobile subscriber system comprising: a mobile data network access point; a server accessible via said data network access point and operable to execute a telephony-over-IP application; a thin client application executable on each subscriber's mobile communication device to interface with said telephony-over-data application via said mobile data network access point; and a subscriber account database tracking data consumption by each said subscriber interfacing with said telephony-over-IP application via respective executions of said thin client application, against a respective all-data mobile subscription account associated with each said subscriber.

[0014] In accordance with one such aspect, the telephony-over-data application includes a voice-over-data function and a SMS-over-data function, wherein the subscriber account database independently tracks data consumption associated with each of said voice-over-data function and said SMS-over-data function.

[0015] In accordance with one such aspect, the subscriber account database further independently tracks data consumption associated with a Web-based function implemented via said mobile data network access point.

[0016] In accordance with one such aspect, the thin client application is further executable to access a current data consumption metric relative to an overall data consumption allocation, and optionally, the current data consumption metric is subdivided into respective data consumption metrics for voice-over-data usage, SMS-over-data usage and Web-based usage.

[0017] In accordance with one aspect, the thin client application is further executable by a first subscriber associated with a first all-data mobile subscription account to transfer a data consumption allocation quantum to a second subscriber associated with a second mobile subscription account.

[0018] Other aspects, features and/or advantages will become more apparent upon reading of the following non-restrictive description of specific embodiments thereof, given by way of example only with reference to the accompanying drawings.

BRIEF DESCRIPTION OF THE FIGURES

[0019] Several embodiments of the present disclosure will be provided, by way of examples only, with reference to the appended drawings, wherein:

[0020] Figure 1 is a network diagram of a mobile subscriber system, in accordance with one embodiment;

[0021] Figure 2 is a network diagram showing cross-carrier interoperability between subscribers, and between subscribers and non-subscribers to a virtualized smartphone-over-data system and environment, in accordance with one embodiment;

[0022] Figure 3 is a screenshot of a dialer interface rendered on a mobile communication device as part of a virtualized smartphone-over-data environment executed thereon, in accordance with one embodiment;

[0023] Figure 4 is a screenshot of a phone history interface rendered on a mobile communication device as part of the virtualized smartphone-over-data environment of Figure 3, in accordance with one embodiment;

[0024] Figure 5 is a screenshot of a user contacts interface rendered on a mobile communication device as part of the virtualized smartphone-over-data environment of Figure 3, in accordance with one embodiment;

[0025] Figure 6 is a screenshot of a particular contact page of the user contacts interface of Figure 5 identifying a selected user as also being a secured user of the virtualized smartphone-over-data environment, in accordance with one embodiment;

[0026] Figure 7 is another screenshot of the dialer interface of Figure 3 during an ongoing call to the selected secured user identified in Figure 6 and showing a cumulative data consumption for the ongoing call, in accordance with one embodiment;

[0027] Figure 8 is a screenshot of a contact group interface rendered on a mobile communication device as part of the virtualized smartphone-over-data environment of Figure 3 and showing a selected group listing of user contacts and their current availability, in accordance with one embodiment;

[0028] Figure 9 is a screenshot of a user account interface rendered on a mobile communication device as part of the virtualized smartphone-over-data environment of Figure 3 showing a remaining data allocation in the user account, in accordance with one embodiment;

[0029] Figure 10 is a screenshot of another user account interface rendered on a mobile communication device as part of the virtualized smartphone-over-data environment of Figure 3 showing data allocation add-on and transfer options, in accordance with one embodiment;

[0030] Figure 11 is a table showing different illustrative data allocation packages and corresponding usage metrics available upon subscription to a mobile network operator supporting implementation of a virtualized smartphone-over-data service, in accordance one embodiment;

[0031] Figure 12 is a table showing different illustrative services and features available to subscribers of the different illustrative data allocation packages of Figure 11; and

[0032] Figure 13 is a flow diagram for inbound telephony with rerouting option to a virtualized smartphone-over-data environment.

DETAILED DESCRIPTION

[0033] For simplicity, the following will make general reference to mobile operators and carriers to encompass MNOs, VMNOs and other such types of mobile network operators/carriers.

[0034] General reference will also be made to mobile communication networks to encompass different types of networks commonly known as cellular networks or mobile telephone networks that are generally directly or indirectly managed, operated and/or leveraged by mobile operators to provide mobile services to end users. Accordingly, while the description provided herein may focus more specifically on a particular type of mobile network (e.g. GSM networks), it will be appreciated that the embodiments described herein may also be implemented over different types of mobile network architectures, standards and technologies (e.g. CDMA, UMTS, etc.) without departing from the general scope and nature of the present disclosure.

[0035] Further, the following will make general reference to mobile communication devices to encompass different devices amenable for interfacing with and communicating over such mobile communication networks. While these devices may also be amenable for communicating over other types of wireless communication networks, such as Wi-Fi, Bluetooth, NFC, etc., such wireless network communications should not be confused with the mobile network considerations described herein. That being said, and as will be described in greater detail below, some of the features and functions provided by embodiments of the virtualized smartphone environment and telecommunication services described below may also be made available to registered users via other data

connections that may include wireless connections to Wi-Fi networks and the like, and standard landline Internet connections.

[0036] In general, the illustrative systems and devices described herein allow a subscriber to a given mobile operator to partake in traditional mobile services using, in accordance with some embodiments, any mobile communication device operationally associated with this mobile operator. In some embodiments, the subscriber is provided access to these services by way of a virtualized telephony environment, generally and interchangeably referred to as a smartphone-over-IP (SoIP) environment or an Internet personal communication system (iPCS) client. This thin client environment is generally supported if not deployed by the mobile operator to circumvent traditional voice and text-based telephony subscription packages through the provision of a complete telephony-over-data system that is subject to the same data usage charges and/or rates applicable in the context of more standard mobile data communications, such as Internet browsing, email, social networking and the like. Accordingly, this virtualized configuration may allow the subscriber to take advantage of significantly lower mobile data network rates, even or particularly when roaming on another network not directly supported by the subscriber's home network operator, while benefiting from various security and confidentiality enhancements not available with standard mobile telephony.

[0037] In the particular examples provided below, the iPCS system is implemented centrally by or in association with the network operator. Generally, the system is interactively implemented with the subscriber's current (i.e. logged-in) mobile device upon subscriber authentication, which unlocks a virtualized telephony environment on this device that interfaces with the network operator's server-based (i.e. cloud-based) telephony and other applications over an available mobile data network (i.e. local or roaming). Using this centralized implementation, the subscriber may further benefit from increased flexibility in terms of device interchangeability, mobility and personal data access. For instance, subscribers may gain centralized access to telephony-related data such as contacts, call history, text-message history, etc., that can be stored centrally in association with the registered user's account and made available via the thin client application. This may also promote greater data security by centrally storing all sensitive

data on the network operator's server(s) such that unauthorized access to a subscriber's phone, be it lost or stolen, will leave them less vulnerable to data losses and inappropriate information gathering and usage. Of course, the subscriber may also appreciate the ability to use different mobile devices without needing to transfer relevant data (i.e. traditionally done by transferring a user's SIM card to a new phone, but only when the old SIM card is compatible with the new phone).

[0038] Further, as will be described in greater detail below with reference to one particular embodiment, by centralizing telephony functions over a data network and by providing access thereto via a subscriber data login authentication process that is untethered to the physical device in question, the subscriber can access these functions from any mobile device compatible with this data network. In some embodiments, while the mobile devices (or SIM card) issued by a given mobile operator may be integrally associated with the mobile operator, thus facilitating access to the operator's centralized telephony-over-data environment, the issued devices and/or SIM cards may remain user-agnostic in that they need not be specifically and uniquely characterised for association with a particular subscriber, but rather, a given subscriber may seamlessly operate any of the devices issued by the operator (or in the context of a SIM card enabled device, any device configured to operate on a SIM card issued by the operator) to gain authenticated access to their own telephony services, and that, irrespective of how many other subscribers may have common use of this device. Accordingly, subscriber and usage flexibility is drastically increased relative to the standard model, and may provide innumerable options in respect of subscriber package and access customizations (e.g. terms of use, access permissions, restricted usage periods, restricted application or data access, geographical permissions/restrictions, etc.), data sharing, device sharing (e.g. within a given organisation, business, or family unit, or between friends, colleagues, etc.) and the like.

[0039] Further, and as will be expanded on further below when describing one embodiment of the virtualized SoIP environment, non-subscribers may also gain access to the virtualized services offered by the iPCS. For instance, a non-subscriber may nonetheless register with the iPCS and load and execute the SoIP environment on their

device to benefit from its various advantages while corresponding through this environment over an pre-existing native carrier data subscription. Various cross-carrier implementations and options will be described in greater detail below, particularly in considering non-subscriber SoIP environment users and their interactions with other subscriber and non-subscriber users, as well as other generally unrelated telephony contacts.

Mobile Subscriber Network

[0040] With reference now to Figure 1, and in accordance with an embodiment, a mobile subscriber system, generally referred to using the numeral 100, will now be described. In the context of Figure 1, a subscriber to a given mobile operator or carrier operates a mobile communication device 102, such as a mobile phone or tablet, that generally combines both telephony (e.g. voice/text) and data (e.g. Internet browser, e-mail, etc.) communication capabilities. Generally, the mobile communication device 102 will include a graphical user interface such as a touchscreen or other interactive screen, a processor, a memory and a mobile transceiver operable to exchange voice and data with the mobile communication network. As discussed above, different mobile communication standards, architectures and technologies may be considered in the present context, as should be readily apparent to the person of ordinary skill in the art, without departing from the general scope and nature of the present disclosure.

[0041] In this example, the mobile communication device 102 further includes a removable computer-readable authentication medium 104, such as a SIM card or the like, in this case issued by and thus registered to the designated mobile network operator. Generally, the authentication module should be compatible with authentication in the mobile communication networks that the subscriber wishes to utilise. In this example, the authentication medium 104 is automatically authenticated upon operating the mobile device in range of the mobile communication network, be it via a home network base station 106 of the mobile operator in question, or via a roaming base station 108 and network operated by a distinct network operator with which the designated mobile operator has an existing roaming agreement. In any event, the authentication medium will

be authenticated as being registered with the designated mobile network operator and thus automatically gain mobile access to those services associated with this authentication medium.

[0042] In standard mobile network systems, as noted above, the subscriber's identity would be integrally associated with the mobile device's SIM card such that, upon network authentication, the subscriber's device would automatically gain access to the various mobile services associated with and by the subscriber's designated mobile operator service package. Data services could then be accessed and monitored via the network operator's respective data service access points identified by respective access point names (APN) stored in the mobile device in association with the authentication medium (e.g. an Internet APN, MMS APN, etc.), whereas mobile telephony services such as voice and SMS-text could be managed and monitored via standard circuit switched network management for home and roaming network access. Ultimately, the user's identity would be managed, and its account appropriately tracked and billed as a function of the SIM data extracted from the mobile device.

[0043] In the example of Figure 1, while the authentication medium 104 is configured to authenticate registration with the designated mobile network operator, the authentication medium will generally remain user-agnostic, in that all mobile devices issued by the same designated mobile operator will be equally identifiable as registered with this mobile operator without specificity as to the mobile subscriber. Accordingly, different subscribers may use the same device, and thus the same authentication module, without sharing a same subscription package with the designated mobile operator. Likewise, a same subscriber may use different devices 102, and thus different authentication modules 104, to access a same subscription package with the mobile operator. This may also expedite the mobile device acquisition process at an operator's retail store as the device's authentication medium need not be pre-authorized and registered with the subscriber. Rather, a new user may instead seek to open a new account with the operator upon accessing the operator's registration page over a regular Internet connection, and set the identification data to be used for subsequent subscriber authentication, described below.

[0044] In order to authorize and monitor access to and from specific subscribers, the designated mobile operator will effectively grant equal initial authorization to mobile devices operating on their registered authentication module in the form of restricted mobile data access over the mobile communication network via operator switch 110 to a designated mobile data network access point identified by a common access point name 112. In the illustrated embodiment, the access point name 112 acts as a mobile data gateway that funnels all data communications from the mobile device 102 to the operator's server(s) 114, where an authentication engine (e.g. via RADIUS application/protocol) will first seek to authenticate the user of the device 102 as a current subscriber to the mobile operator and thus authorize access to the various data network services enabled by the subscriber's account and profile. In one example, a client application 115 on the mobile device 102 will access subscriber identification data (e.g. via manual input via a secure password management application) and forward this data to the operator's authentication engine for authentication and authorization. Once authorized, the mobile subscriber will gain access to one or more data network applications accessible through the access point name and operator server(s) and operable, at least in part, via the user interface of the mobile device.

[0045] In the illustrative embodiments described below with reference to Figures 3 to 10, the client application 115 consists of a thin client application loaded and executed on the client device 102 to implement a virtualized smartphone-over-IP (SoIP) environment whereby all accessed functions and features in fact reside and execute on the system's server(s) 114, the subscriber interfacing therewith via the virtualized SoIP environment. Further details as to the virtualization of a SoIP environment, both within the context of mobile subscribers to the mobile operator system described herein, but also for the provision of data-telephony services to non-subscribers that nonetheless load and execute the SoIP environment as registered users of the system's various services.

[0046] Ultimately, each user's data consumption as an authenticated mobile network subscriber (e.g. when operating a device authenticated as registered with this network operator) will be monitored by the operator server(s) for account management, reporting and billing purposes. Clearly, where the subscriber is using a device under a roaming

agreement with another network operator, roaming charges may also be associated with the user's account, which in the illustrated embodiment, is at least partially managed by a roaming management server 116. However, as will be described in greater detail below, such roaming charges may be accounted for within the context of the subscriber's mobile data allocation, which may in some embodiments, be indiscriminately consumed as a function of actual data usage irrespective of whether the user is operating the mobile device over a home network, a local roaming network or a foreign roaming network.

[0047] In the context of Figure 1, once a subscriber has been authenticated by the operator's authentication engine, mobile communications other than those directed through the designated network access point will continue to be prohibited. Accordingly all mobile data communications must be funnelled through the designated access point name 112 to act as a gateway for all mobile applications executed by the subscriber. These mobile applications may include, but are not limited to, standard data network applications such as email, Internet browsing and the like, but also a voice-over-data application (e.g. VoIP) which may include voice processing and signalization, and a text-over-data application (e.g. SMS to data). Accordingly, the subscribers entire mobile experience, including both traditional data and telephony-over-data services may be provided through a single data network link to the operator APN 112, and channelled based on the application at hand via the operator's server(s) 114 while being exclusively exposed to data usage tracking and related accounting.

[0048] As external network communications such as standard mobile telephony will not be supported by the mobile operator in this system 100, the device 102 and its related authentication module 104 will become inoperable over available mobile communication networks without subscriber authentication via the operator's access point name 112. This feature thus provides an added advantage that, should a subscriber lose their device or SIM card, they will be effectively useless to another user without the subscriber's identification data (e.g. username and password). Applicable security and confidentiality features will be discussed in greater detail below, particularly in the context of the SoIP environment noted above that may, in some embodiments, be deployed for implementation by subscribers and non-subscribers alike. Namely, in the context of a

virtualized SoIP environment, not only will the operator-registered device become communicatively inoperable without proper subscriber authentication, but all data related to the exchange of communications via the SoIP environment will remain securely stored on or in association with the system's server(s) and solely accessible via the virtualized environment upon being unlocked post subscriber/user-authentication.

[0049] The embodiment of Figure 1 provides further illustrative detail as to illustrative abstraction layers involved in interfacing the mobile device's thin client mobile application 115 and those executed on the operator's server(s) 114. In particular, the physical and data link layers (L1-L2) may be implemented via UMTS/HSPA(+) 3G // LTE 850, 1900, 1700 MHz & AWS 1700/2100 MHz; network layers (L3) may be implemented over TCP/IP, UDP and/or RTP; whereas upper layers (L4-L7) may be used for voice-over-data applications and protocols (SIP, RTP) / encrypted text messages / encrypted data (e.g. login info), group info., account info, subscriber profiles, file transfer, data services and internet browsing (proxy).

[0050] The following provides various illustrative functions and features rendered available and accessible upon implementing an exemplary embodiment of the mobile operator system, mobile communication device and virtualized smartphone-over-data (SoIP) environment(s)/system/server(s) described above, generically and interchangeably referred to herein as an internet personal communication system (iPCS).

[0051] In one embodiment, the iPCS combines traditional PSTN/CLEC phone services (public switch telephone network / competitive local exchange carrier) with the geographically independent and virtual services of VoIP while leveraging the benefits of implementing a thin client architecture that uses powerful and sophisticated cloud-based services to power a user's telecommunication needs. iPCS therefore integrates relevant functions into a native mobile service, merging traditional telephony with Internet telephony in a convenient, competitive and secure package. Using this approach, the iPCS can assemble an innovative and attractive suite of features and components. Furthermore, as introduced above, the iPCS environment and services can be made to execute on effectively any mobile device, and that, irrespective of whether the device is

registered for mobile services provided by the iPCS operator/carrier. That is, any user of a mobile device, irrespective of its native carrier, can load and execute the virtualized iPCS/SoIP environment on their device and gain access the suite of iPCS services and advantages while also gaining access to a phone number from a choice of multiple countries (e.g. 58 countries in this example), making it a truly worldwide communication service.

SoIP System Security and Confidentiality

[0052] As noted above, all relevant iPCS functionality can be configured to reside on the "Cloud", thus turning the Internet enabled device into an access point and control for cloud-based functions, while optionally storing all relevant user data on the cloud independently of the physical device used to access the services. For instance, the only communication device requirement may be that it store and execute an IPCS thin client application to access these cloud-based functionalities. Accordingly, a same subscriber can use multiple devices via a common IPCS subscription to access and/or move all IPCS services from device to device at their choosing by logging out of one device and in to another. Users can log in via the thin client application and have immediate access to all enabled functions including voice, data, telecommunications management, text, browsing and group functions, for example, which enabled functions remain active only so long as the user remains logged into his IPCS account. Likewise, functionality can be added, modified or updated on the Cloud at any time meaning that users do not have to update their device software to benefit from these changes.

[0053] Accordingly, the IPCS can provide universal access via a single point of contact, thus providing subscribers with universal access regardless of location or service provider through their IPCS phone number or through their email which is registered on the IPCS system. Therefore an IPCS subscriber can be called or texted anywhere in the world via a single point of contact that is integrated into the service and requires no additional software and login.

[0054] Amongst others, this can provide the added benefit of receiving immediate notification of missed calls upon logging back into the iPCS environment, irrespective of

the device used to log back in. This is unlike traditional mobile operator systems where a mobile device must be turned on and within a service area to receive such call log information. Likewise, missed text messages will be queued in the iPCS server(s) and notification thereof received by the user immediately upon logging back into the system without delay (i.e. the user will gain immediate remote visualization access to the text message stored on the cloud-based text server).

[0055] Furthermore, in the event that a device is lost, there will be no need to remotely "erase phone data". If the user is logged off the mobile device when it is lost, then there is effectively nothing to erase in respect of phone data usage, history, contacts, etc. Where a user loses their mobile device while still logged into the iPCS environment, then one can simply log out remotely and thus block any further access to user data.

[0056] While the mobile device is effectively reduced to an access point to iPCS data, the subscriber may nonetheless chose to downloaded this data at any time to their current mobile device. This may include, but is not limited to, subscriber contacts, call listings, text messages, multimedia messages (including any embedded multimedia content), schedules, notes, etc. On the other hand, if IPCS data is not downloaded to the mobile device, upon logging out of the system, there will be no iPCS data on the mobile device's internal memory or SIM card, for example (e.g. contacts, call records, text, browsing history, email). Subscribers can regain access to all IPCS data stored in association with their user profile as such data will automatically sync with the mobile device upon subsequent user login. Therefore users have full access to their data each time they log in regardless of the device.

[0057] As introduced above, embodiments of the virtualized SoIP environment and services can provide for enhanced security and privacy, both in respect of user data being securely stored on the iPCS server to limit unintentional access to this data via the user's various mobile devices, as noted above, but also in optionally providing secure communication channels to those users seeking to take advantage of such options. Accordingly, users of the virtualized SoIP environment, and particularly paying subscribers to iPCS services can elect to have all functions including voice and text

encrypted, for example, via a 128bit encryption (private) key. Much as the iPCS environment, the encryption key is not hardware dependent (as in the case of other technologies such as Blackberry Messenger™ which relies on the device PIN) but is based, in this example, on the unique username and password of the iPCS user. Accordingly, the encryption option follows the user from device to device as do the contacts and other information. As the key is known only to the user's device when in use and the iPCS server, transmission and receipt of data to and from the iPCS server is secure. Likewise, when corresponding with other iPCS users having elected the enhanced security option, the transmission and receipt of data such as voice and text information between the iPCS server and such other IPCS user's dervices will be equally secured through the recipients' respective unique username and password.

[0058] In one embodiment, each user-specific encryption key will be simultaneously generated by the phone and the server when the passphrase is recognized, whereby an illustrative algorithm may be employed on the client and server sides of the virtualized environment to generate a key based on the passphrase for each new session with the server. For example, the encryption key may be changed every session using the same algorithm and combining the passphrase with a date and time associated with each new session that is synchronized between the server and client.

[0059] Following from the above, and with reference to Figure 2, the system 100 may thus be further configured to provide enhanced security for communications exchanged between users of iPCS and its virtualized environment. For example, in one configuration, the mobile operator may provide access to encrypted voice and text-based services to users electing to subscribe to such services, possibly in exchange for a higher subscription fee and included data usage limits given the higher data consumption and processing requirements for encrypted communications. For example, Figure 2 shows a number of enhanced security subscribers 120 operating registered SoIP-enabled devices over a home iPCS carrier network 106 or a roaming carrier network 108, either way ultimately securely corresponding with one another (e.g. by voice-over-data or SMS-over-data) via respective secure and encrypted connections 122 to the system's server(s) 114. On the other hand, when corresponding with non-secured contacts 124, such as non-

users (e.g. subscribers to other mobile operator networks 108 or general PSTN 109 subscribers), or in the example provided below, non-subscribers that may nonetheless use and benefit from the system's SoIP virtualization, while communications between the secured subscribers 120 and the system's server(s) 114 may still be secured by encryption, corresponding communications between the system server(s) 114 and the devices of these non-secured contacts 124 will not be so secured.

[0060] As will be described in greater detail below with reference to illustrated examples, in some embodiments, when corresponding with another secured or unsecured user, a corresponding icon or identifier will appear for visualization by the secured user as a notice as to the encryption and security status/level associated with correspondence directed to such secure and unsecure users, respectively. Therefore, when a secured user 120 corresponds with an unsecured recipient 124 (e.g. a non-secured iPCS user or a non-iPCS user altogether), this secured user 120 may deliberately avoid transmitting sensitive information that they would otherwise feel secure in sending to another secured iPCS user. Otherwise, where a given contact includes both secure and non-secure contact coordinates, a secure user may elect to only communicate sensitive information to this given contact via their secure coordinates, and use only their non-secure coordinates for less sensitive correspondence.

[0061] Again, for added security and privacy, no texts, call logs etc. ever reside on the mobile device being used via the SoIP virtualization environment unless expressly downloaded thereto by the user. They exist only on the iPCS Cloud. Users can access or delete texts, call logs and other data at any time through an iPCS Cloud Web interface or on their virtualized phone environment when logged in. Therefore on logout, the session ends and there is no data on the phone.

Virtualized SoIP Environment

[0062] Following from the previous examples of Figures 1 and 2, and in accordance with different embodiments, the mobile communication device 102 will ultimately gain access, post-subscriber authentication, to an operable virtualized smartphone-over-IP (SoIP) environment 200, illustratively depicted by the screenshots of Figures 3 to 10.

While the SoIP environment 200 may be more commonly deployed to and executed by SoIP carrier subscribers, the SoIP environment may also be downloaded and executed by registered users that subscribe to the mobile services of another native carrier and thus, are subject to carrier service fees and charges associated with that other native carrier. Irrespective, such registered users may still take advantage of the SoIP environment and related features/functions and may eventually seek-out subscription to the SoIP carrier using a registered SoIP carrier device.

[0063] For example, in the embodiment of Figure 3, the virtualized environment 200 includes a softphone application 204 emulating one or more mobile telephony functions over the device's native data network and cooperatively operating as a thin client on the mobile device 102 in communication with the system's SoIP server(s) 114. Namely, the softphone application 204 may be centrally implemented on or in association with the SoIP server(s) 114 and provide some of the various features, functions and advantages discussed in greater detail below with reference to various exemplary embodiments.

[0064] Beyond voice-over-data call functions (e.g. accessible via single touch dialler function button 205), the illustrative embodiments of Figures 3 to 10 provide remote SoIP environment users access to at least one of a centralized voicemail system (e.g. via single touch button 206), a centralized call/SMS history listing (e.g. via single touch button 208), a centralized phone contact listing function (e.g. via single touch button 210), an SMS-over-data or instant messaging IM function (e.g. via single touch button 212), a user group function (e.g. via single touch button 214), a real-time subscriber account information function (e.g. via single touch button 216) and a general settings access function (e.g. via single touch button 218). The environment 200 will also generally show an accessed network identifier 220 (and other connectivity and device operation indicia) identifying the mobile network currently being accessed (e.g. either the subscriber's home mobile operator network or a roaming network accessible by subscribers of the home mobile operator through a pre-established cross-network roaming agreement, and that, irrespective of whether the environment is being executed on a SoIP carrier device or not), and a registered user authentication indicia 222 identifying that the user has been

successfully authenticated with the SoIP server(s) 114 as a registered user of the SoIP environment 200.

[0065] The SoIP environment 200 also includes, as part of the dialer interface 204, a single touch SoIP environment loggin/logout button 224, for example allowing users to quickly log-off the SoIP environment and consequently shut-down access to any and all user information on that particular device, which user information will nonetheless remain safely stored on the SoIP server(s) 114 and associated databases and accessible therefrom upon subsequent user login via the same or another SoIP-enabled device. To login, in one embodiment, the user may be directed to a login screen or interface upon launching the SoIP environment, where username and password may be manually entered by the user or automatically unlocked and dispatched via one or more security measures (e.g. biometric or other access security applications). Alternatively, the user may be automatically directed to the softphone interface 204 upon launching the SoIP interface 200, and access a user registration function via the single touch login/logout button 224.

[0066] With particular reference to Figure 4, and in accordance with one embodiment, upon the user successfully logging-in to the SoIP environment, the user may gain access via history button 208 to a cloud-based softphone usage history 226 of all inbound calls received and outbound calls placed via the SoIP environment 200. Unlike a standard smartphone, the call history will remain stored on the system server(s) 114 and can be accessed and managed (e.g. delete entries via trash button 228) via the SoIP environment 200 irrespective of which device is used to gain registered access the SoIP environment 200 and its call history list 226.

[0067] With particular reference to Figure 5, and in accordance with one embodiment, upon the user successfully logging-in to the SoIP environment 200, the user may gain access via contacts button 210 to a searchable/scrollable cloud-based All Contacts directory 230, which may include not only entries for contacts that are also users of the SoIP service, but also general contact entries either imported manually or automatically via an associated contacts import function (e.g. an associated SoIP user Web portal function, a device-specific contact transfer function, and automated social-

media or mail client contact transfer function, etc.). The cloud-based and maintained contact directory 230, much like the call history log of Figure 2, will remain stored on the system server(s) 114 and can be accessed and managed via the SoIP environment 200 irrespective of which device is used to gain registered access to the SoIP environment 200 and its contacts directory 226. In this example, the All Contacts interface 230 also provides access to contact Groups via button 231, discussed in greater detail below.

[0068] While logged into the environment 200, the registered user may select a given contact entry, such as by tapping a given entry 232, and gain access to a detailed contact entry 234, shown illustratively on Figure 6. The user can then select to place a SoIP call directly via the selected contact's mobile phone listing 236, which call will be directed to the called party, first over IP via the SoIP network, and then, depending on whether the contact number in question is assigned to the SoIP carrier or to another carrier, and in the latter case, whether this contact number is nonetheless associated with an SoIP user, over an packet or circuit switched network to the recipient. The SoIP user may also use this interface to automatically select and send an IM/SMS message to the contact, this message being routed, as in the context of a voice call, depending on similar recipient number associations. Traffic routing to and from the SoIP environment will be discussed in greater detail below with reference to Figure 13, which particularly relates to inbound call/SMS management and routing options in the context of the herein described SoIP environment and supporting native network architecture.

[0069] In the particular example, the selected contact is also a registered SoIP user, and thus, can systematically partake in VoIP calls via the SoIP network, and that, irrespective of the device on which this contact is logged into for SoIP services, irrespective of which native network carrier he subscribes to for mobile data network coverage, and irrespective of which mobile data carrier he is currently actively connected to, if not in fact connected through another data connection such as Wi-Fi or broadband Internet, for example. As noted with reference to Figure 2, this contact's registered SoIP status also allows the registered user in this example, upon subscribing to this feature with the SoIP carrier, to communicate with this particular contact over encrypted sessions on either side of the SoIP server(s) (e.g. via respectively encrypted user-specific sessions

using each user's respective passphrase and associated session-specific data). Accordingly, this contact mobile phone entry 236 includes a "secured connection" symbol 238 confirming the security level available upon accessing the contact with this number. In fact, the contact entry could include different phone or SMS contact entries having different applicable security levels. For example, a traditional PSTN home or office phone number may be listed for a given contact and accessible via the SoIP environment 200, albeit at the expense of an otherwise available encryption security should the call be otherwise made to the listed contact's secure mobile SoIP number. Different variations and permutations may also be considered depending on each registered user's subscription package (e.g. selectable encryption package upgrade), available data allotments, etc.

[0070] Furthermore, the SoIP environment 200 may be configured so probe the SoIP server(s) 114 to identify if a selected contact and user of the SoIP service is actively logged into his SoIP environment, and if so, if this contact is also labelled as available. In the example of Figure 6, the selected contact has not only a secured connection icon 238 displayed against the listed mobile SoIP number, but also a green availability indicia 239 identifying the selected contact as online and available. Otherwise, a red indicia may indicate that the selected contact is offline, and a yellow indicia indicate that he is busy (e.g. on another call, or self-labeled as such so not to be disturbed). In these latter cases, the system may then be configured to allow the user to nonetheless leave a voicemail to the selected contact, or again, request that they be notified upon the selected contact becoming available. Again, these features may be seamlessly integrated within the SoIP environment to provide each SoIP user and their SoIP-enabled contacts combined access to enhanced telephony and data communication features and functions otherwise unavailable using standard mobile telephony network architectures.

[0071] With reference now to Figure 7, upon placing a call to the selected contact via the identified secure and available SoIP contact number, the registered user is returned to a dynamic rendering of the softphone interface 204 to show the selected contact's details via ongoing call portion 240, which may also show the secure connection symbol 238

confirming end-to-end call encryption, as well as an ongoing data usage metric 242 for the call in progress.

Group/Administrative Functions

[0072] The iPCS can provide subscribers and subscriber groups alike with complete real-time control over accessed functions and features, for example, via a complete suite of SoIP management tools as well as available filters and permissions related to calling, texting and browsing, for example.

[0073] For instance, the virtualized SoIP environment can provide various features and functions unique to this environment and specific to the formation of user groups and group functions. For example, the SoIP environment can incorporate functions available to uniquely defined user groups of specially connected SoIP subscribers/users that may consist of family/friends in the case of residential users, employees in the case of a company, or other connected individuals (e.g. special interest group, politically affiliated groups, professional groups, etc.). Within these groups, connectivity relationships can be customized to make communication easier and more efficient. Where all members of a particular group subscribe to an enhanced security/encryption service package, intra-group communications can be securely stored and maintained on the system server(s) 114 and encrypted on either side thereof between respective registered user SoIP environments, and again, irrespective of the device being used by each user.

[0074] In the context of individual subscribers, a group can be initiated by sending invitations to people they would like in their group (via the invitee's phone number or registered email). Invitees can simply accept or reject the invitation. In the context of corporate subscribers, customized groups can be established as they wish within their corporate environment, and optionally managed via an accessible group administrator portal or account on the SoIP server(s). Other group formation and management functions and features may also be considered, as will be discussed in greater detail below.

[0075] Once part of a group, users can gain access to a suite of special connectivity features that can be controlled by the individuals (in the case of residential services) or by

a telecom manager in the case of an organization, for example. Since these groups are formed around cloud-based applications, the suite of services can be expanded at any time based on market requirements or trends. Examples of group functions may include, but are not limited to:

[0076] Paging: a function that can be enabled for each member of a group whereby a message (e.g. up to 30 seconds) can be sent to an individual or multiple people within the group and automatically broadcast on the recipient speaker.

[0077] Push-to-talk: a function that can allow grouped SoIP-enabled devices to operate essentially as walkie-talkies but with enhanced functionality. Under push-to-talk, an iPCS sender can broadcast a message to specific individuals, or groups of individuals, which message broadcasts on a respective recipient device's speaker. Recipients can respond from their device in the same push-to-talk fashion. All recipients are able to hear the response. This is ideal for situations such as dispatch where multiple respondents and direct communications are required, for example. Furthermore, Push-to-talk services are not limited to wireless devices, but may rather work between any SoIP-enabled devices, fixed or mobile.

[0078] With reference to Figure 8, and following from the example discussed above in accordance with one embodiment, the registered user may gain access, upon logging into the SoIP environment 200, to one or more group function interfaces 244, for example via one touch group button 214 and/or via the All Contacts' group button 231 (Figure 5). In this example, the registered user can select a particular contact group of interest (e.g. Sales group) using a drop down group menu 246, which then dynamically updates a group contact list portion 248 identifying each user contact belonging to this group. While such list could include non-SoIP user contacts, it is generally contemplated in this example that all contacts forming part of a given group will also be a registered SoIP user, though not necessarily an SoIP carrier subscriber. Accordingly, upon subscribing to the enhanced security option, a group of users may form a secured group whereby all correspondence between this group of users will be encrypted on either side of the SoIP server(s) 114 by respective user-specific and session-specific encryption keys.

[0079] Next to each group contact identifier, an availability indicia 250 is also provided, in this example showing a green symbol for users that are logged into their SoIP environment and available, a yellow symbol for users that are logged into their SoIP environment but currently unavailable (e.g. either actively engaged in an SoIP environment exchange or deliberately marked as such to identify that they are currently too busy to receive a call), and a red symbol for users currently "offline", that is, not currently logged to their SoIP environment.

[0080] In this example, the contact group interface 244 provides different direct correspondence options between group contacts, such as a paging option 252, a push-to-talk option 254, a 2-way communication option 256 (e.g. VoIP), and a tracking option 258. In the illustrated example, the Push-to-Talk option 252 is selected, and two group contacts 260 and 262 identified as "available" are dynamically selected to participate in this exchange. Again, all exchanges will be fully encrypted, and any tracking thereof will be exclusive stored and maintained on, and later accessible from, a cloud-based repository, unless of course otherwise downloaded to a particular device when allowed under user/group/administrator settings.

[0081] As noted above, the SoIP service may also allow individuals, groups and administrative users to customize service access permissions and restrictions, and/or gather informative user access metrics and information, as well as enable and/or manage various group or inter-user functions such as data allocation sharing and/or exchange; referral incentive, tracking and compensation; and the like. This may be particularly attractive to enterprise users in seeking to maintain some control and understanding as to how enterprise devices are used by their employees/members.

[0082] For example, a user or group manager may invoke certain telecommunications management tools via an administrative SoIP environment interface and/or via a Web portal to the system's server(s) 114, whereby a managing user can oversee and control device/subscription usage permissions/restrictions and have access to comprehensive real time usage data. In an organization, devices/subscriptions can be managed as a group or individually. In some examples, iPCS may incorporate user-driven real-time controls

over all or most functions and features. This may allow users to customize their telecommunications experience to their specific needs at any given time and to program the functionalities for unattended control.

[0083] Examples of call management functions accessible to individuals, groups and/or managers through the iPCS administrative and/or Web interface may include, but are not limited to:

-- Time of day permissions/restrictions (when calls can be sent / received);

-- Long distance permissions/restrictions (where calls can be placed);

-Call Filtering (block numbers in or out);

-- Simultaneous ring function controlling which mobile phone will ring when a specific number is called (e.g. where a same subscription phone number is shared over multiple devices or between group users that may be concurrently logged into to SoIP system), which can be programmed by day and time of day, for example. Accordingly, different devices may ring depending on whether it is normal or after business hours, or again, in the case of a support line, a single number can be set to ring on several devices at once (e.g. multiple active SoIP environments);

-- Call Forwarding, whereby a call is automatically forwarded to another number or numbers, and can again be controlled by day and/or time of day;

-- Cascading Functions, whereby a call can be automatically forwarded to a defined sequence of numbers if the call is not answered;

-- Phone Activation/Deactivation, whereby a particular user access to the SoIP environment can be activated or deactivated automatically according to a preprogrammed schedule (e.g. day and/or time of day), or again remotely;

-- 4 digit access and transfer, whereby SoIP-enabled devices within a same organization regardless of location can be accessed internally by dialing a 4 digit extension, or again transferred using this same 4 digit access; and

-- Do not Disturb, whereby a particular user's SoIP-enabled device may be set to identify days and/or times of day when a phone will ring or receive other notifications via their enabled SoIP environment.

[0084] Examples of text-based or multimedia messaging management functions accessible to individuals (e.g. parents), groups and/or managers through the iPCS administrative interface and/or Web portal may include, but are not limited to:

-Day and/or time of day texting permissions/restrictions;

-- Content filtering, for example consisting of an intelligent filtering algorithm which blocks and reports inappropriate messages between registered users; and

-- Received and read functions.

[0085] Examples of browsing management functions accessible to individuals (e.g. parents), groups and/or managers through the iPCS administrative interface and/or Web portal may include, but are not limited to:

- Day and/or time of day browsing permissions/restrictions;

- Content filtering for inappropriate content;

- Website-specific or application-specific filters to block specific web sites or platforms (e.g. select social networking sites, YouTube™, etc.)

[0086] Examples of real-time or historical usage management (e.g. statistics) accessible to individuals (e.g. parents), groups and/or managers through the iPCS administrative interface and/or Web portal may include, but are not limited to:

- Data usage / Data remaining;

- Call records;

- Text entries;

- Web page history; and

- Current users online.

[0087] Other features and options may also be considered.

Network Subscription Metrics

[0088] As noted above, iPCS allows for the combination of traditional telephony features and functionality (e.g. voice and text) with traditional mobile data services under a common mobile data service plan. By using an IP-only approach for all functions and

features, no voice channels are used or needed, thus simplifying usage metrics and native carrier subscription packages, not to mention reduce applicable fees, particularly when roaming. For instance, native carrier subscription packages can be set and managed on a "per megabyte" basis whereby users purchase megabytes (either prepaid, post-paid or based on certain package amounts), and consumes these megabytes over time at a rate that will depend on the specific application at hand. Therefore, megabytes become the "currency" of iPCS, as opposed to traditional methods that also necessarily exchange in minutes, sent/received text messages, etc. For example, using current iPCS standards, 1 MB of data usage can provide approximately 9 minutes of voice calling, 90 text messages, or 4 Webpages (bearing in mind that Internet browsing will consume MBs at a variable rate according to nature of the content being browsed -- e.g. text vs. graphics vs. multimedia vs. HD multimedia). By monitoring or estimating subscriber usages, one may allocate or budget a particular amount of MBs per month and select an appropriate service package accordingly. Figure 11 provides an example of different iPCS service subscription packages that may be offered, and the level of usage that may be afforded to subscribers on these subscription packages, whereas Figure 12 provides a list of features/functions available under each subscription package, including that available to non-native users (e.g. those subscribed to another native carrier but registered to use the SoIP environment).

[0089] For instance, registered iPCS users operating on another mobile operator's network may also benefit from the various advantages of iPCS, but will be subject to the data plan charges and allocations provided by their native mobile carrier. In one embodiment, such non-native users may be provided free access to iPCS services, not only to encourage loyalty transfer to the iPCS mobile operator, but also to enhance security and versatility options for existing iPCS mobile operator subscribers in providing them access to a greater pool of iPCS users in their contact list.

[0090] iPCS can also service its subscribers irrespective of the device they are using, such that any Internet-enabled device with multimedia capability (microphone, speaker, interactive screen via touch or mouse) can effectively become a virtualized smartphone upon accessing an authenticated data network connection (e.g. landline (Ethernet),

wireless (Wi-Fi) and/or mobile (cellular)) to the IPCS server. Accordingly, complete roaming and portability is provided, particularly for users of mobile communication devices that can access the Internet via the iPCS mobile operator's data services (or that of another mobile operator under a separate data plan) via a home or roaming mobile network, as well as via other wireless services such as Wi-Fi or Ethernet.

[0091] The iPCS also allows for real time subscriber access to a unitary data consumption measure covering all data usages irrespective of the application (VoIP, text-over-IP, Internet browsing, email, etc.). In one example, a current data usage and account balance is made available to the subscriber in real time via the thin client SoIP environment. This may include general information such as overall and/or function-specific data consumption, as well as predictive measures for remaining data allotments, extra data purchase options, and data transfer options to other users, for example.

[0092] With reference to Figure 9, and in accordance with one embodiment following from previous examples, upon a registered user successfully logging-in to the SoIP environment 200, the user may gain access via account button 216 to a subscriber account interface 263 and various subscriber-account functions. In the particular example of Figure 9, the user is first presented with an up-to-date graphical data-usage indicator 264 that shows a current data consumption relative to an overall subscription allocation (e.g. 737MB used and 263MB left out of a total monthly data allocation of 1GB), and further graphically illustrates a respective colour-coded portion of this consumed data associated with each of voice 266, data 268 and text services 270, along with a specific number of minutes 272, Web Pages 274 and Text Messages 276 associated with each consumed portion. The subscriber can then accurately observe consumption trends and predict future usage requirements, and adjust the subscription package accordingly, not to mention appreciate the overall benefits of an all-over-IP subscription package over traditional mobile telephony packages.

[0093] In the context of a group administrator portal, a similar display may be provided for group-wide usage, for example where a group data allotment can be shared between users of a same enterprise group or the like. Such shared group resources could

also be broken down based on each user's personal consumption, and respectively broken down into distinct service usage.

[0094] In the present example, the subscriber interface 263 includes a logout button 278 to log out of the SoIP environment on that device, as well as a Transfer MB button 280 leading the subscriber to a data Purchase/Transfer interface 282, shown illustratively in Figure 10.

[0095] With reference to Figure 10, the data purchase/transfer interface 282 reprises the graphical data consumption graphic 264 of the previous interface, and adds a real-time or refreshable current monetary balance in the account 284, and two one-touch options 286 to add further data credits to the subscription for the month in progress. This interface also includes a MB transfer function portion 288 that includes a preset or dynamic drag-selectable MB transfer amount function 290 to identify an amount of MB to be transferred (for example relative to an overall monthly allotment), and a drop-down menu function 292 allowing selection of a particular data recipient subscriber from a list of known subscribers (e.g. defined by the user's membership to a particular user group or groups of subscribers, such as linked family members, business partners and/or employees under an enterprise group setting). Once the amount and recipient subscriber has been selected, the transferring subscriber may activate the transfer and inject the transferred data allotment in the recipient's account.

[0096] Unlike a monetary transfer function, both the transferring subscriber and the recipient can accurately predict the relevance and impact of the transferred data allotment, both relative to each subscriber's current data usage and in respect of an expressed need for added data access. For example, a subscriber wishing to correspond with another subscriber may elect to transfer a certain data allotment thereto prior to or after placing a voice call in order to mitigate an impact this voice call may have on the called parties subscription package. This may also be relevant where a given subscriber predicts a substantial data overage for the month in progress and requests a friendly transfer from someone underusing their subscription package (e.g. from a friend,

colleague or family member that is on vacation and thus making limited use of their current subscription, for example).

[0097] The SoIP environment, or related Web portal, may also track such transfers, both in and out, in managing a form of subscription data exchange network, where one can actively track data transfers and, for example, suggest account reconciliations downstream or that a particular recipient increase their monthly allotment to address repetitive requests for data transfers. This may also be particular convenient in the context of a working group or enterprise account to manage and oversee respective data usages and transfers between employees, colleagues, partners and the like.

[0098] In one embodiment, a referral compensation system may also be put into place to reward system subscribers upon successfully referring new subscribers to the iPCS network. For example, a subscriber wishing to promote iPCS subscription to one of its contacts can input this contact's mobile phone number to a referral engine that, as a result, sends a text invitation to this contact with direct option to subscribe to the iPCS network, which direct option may automatically link the new subscription back to the referrer. However, as the contact is likely to port their mobile number to the iPCS network when they subscribe to it, even if this new subscriber does not subscribe in direct response to the system's invitation, the referral may nonetheless be tracked to the original subscriber, who may be compensated accordingly. In one example, for each month of active subscription by each referred subscriber, the referrer may receive a predefined bonus data allotment to its account (e.g. 25MB). Other referral techniques and compensation-based referral incentives may also be considered.

Telephony (Re)routing for Virtualized SoIP Users

[0099] As noted above, the IPCS can also be used as a mobile phone enhancement for IPCS users who are also subscribed to another mobile service provider and may be locked into a long-term service contract or other commitment. Call numbers placed from an IPCS user from another service provider can be vetted through an iPCS database and, if the number is an IPCS user and online, the call is completed through IPCS.

[00100] For example, in one embodiment, the iPCS mobile operator system may be configured to implement a dipping process whereby a call can be routed through and terminated by an iPCS switch even when originating from and destined to non-iPCS subscribers. For instance, in one embodiment, the iPCS system may be configured to operate or interface with one or more call termination switches generally involved in the termination of regional, national and/or international calls originating from different carriers. Accordingly, calls routed through such iPCS-accessible switches can be rerouted, as appropriate, to a registered iPCS user's virtualized environment even when this user is subscribed to another native carrier, thereby taking full advantage of iPCS services and rate options.

[00101] For example, for inbound calls, where the iPCS system has access to one or more local call termination switches processing a significant volume of inbound calls originating from other local or international carriers (e.g. through various interconnection agreements), the termination number associated with such calls as they come into the iPCS-accessible switch can be cross checked with a database of IPCS users. If the terminating number is associated with an IPCS user, the switch can redirect the call for processing through the iPCS system rather than sending it to the native carrier with whom the number is registered. As a result, the call is completed via the iPCS data line and applicable user data usage rates, rather than using up the user's native carrier telephony minutes.

[00102] With reference to Figure 13, and in accordance with one embodiment, a flow diagram for inbound telephony with rerouting option to a destination user's virtualized smartphone-over-data (SoIP) environment will now be described in greater detail. In this example, an inbound call/SMS 1302 is initiated and directed to an originating wired or wireless service provider 1304. As noted above, the inbound call may be a local or international call and, in this example, is directed to a phone number associated with a mobile subscriber to a native mobile carrier that does not support a SoIP environment as discussed above, but where this subscriber is a registered user to another native carrier's SoIP environment (e.g. a SoIP carrier). Where the inbound call is routed directly via the subscriber's native carrier, the call is carried through over the subscriber's standard native

carrier telephony voice/SMS network (e.g. GSM/UMTS/LTE/SMS). However, where the call/SMS is routed via the SoIP carrier's destination local exchange carrier network 1306 and switch 1308, or one administratively associated therewith, the SoIP carrier's switch 1308 may first dip into an internal SoIP user database to identify if the called number is associated with an SoIP user that is currently logged into their SoIP environment. If so, the switch 1308 may but need not dip into the mobile carrier subscriber database 1314 (generally available to all CLEC and ILECs, and used via standard SS7 dipping protocol to compile and provide access to up-to-date mobile subscriber carrier information and the like for call routing/termination) to identify the subscriber's native carrier, and rather automatically reroutes the call/SMS through the SoIP Network 1312. It is converted for transmission over IP and directed to the user's SoIP environment running on the user's device 1324 via the subscriber's native carrier data (IP) network 1316, or again via another available data connection, if not altogether running on another device. Otherwise, the switch 1308 dips into the mobile carrier subscriber database 1314 to identify the subscriber's native carrier and routes the call/SMS via standard voice/SMS protocols over the subscriber's native carrier voice/SMS telephony network 1322 to the user's device 1324.

[00103] Clearly, where the call/SMS originates from a caller's SoIP environment, the call/SMS will be automatically channeled through the SoIP network and, where the called party is also a user of the SoIP network, the call/SMS can be appropriately channeled over an IP network associated with the called number. Of course, all calls directed to a number registered with the SoIP carrier will terminate over IP to the called party's SoIP environment.

[00104] Likewise, for outbound long distance calls originating from an iPCS customer, the terminating number can be checked with the iPCS database. If the number corresponds with that of an iPCS user that is registered with another native carrier, it can be rerouted through the iPCS interface automatically, resulting in the recipient benefiting from his non-native iPCS service including cheaper talk time and long distance rates (i.e. data vs. telephony, etc.).

[00105] Further, this dipping process can also be used when an iPCS customer initiates a call outside his home country. All calls can be checked with the iPCS user database and, when the termination number is another iPCS customer, international roaming charges can be eliminated.

[00106] Naturally, non-native iPCS users also have the option to route long distance calls through the iPCS environment as opposed to using direct voice telephony over their native carrier network, thus benefiting from iPCS's competitive voice-over-data rates rather than to pay the higher voice minute rates applied by their native carrier. IPCS Text-over-data services may also be used to like effect.

[00107] Finally, IPCS users anywhere in the world may be able to take advantage of the system's international call resolution. When sending a text or placing a voice call, the IPCS server resolves the text or call and routes it to the most appropriate local service. As an example, a Rogers customer in Canada can place a call or text to an MTS subscriber in South Africa via IPCS, rather than incurring the Rogers long distance charge. The IPSC call resolution allows it to be treated as a local call or text. This is regardless of from where the Rogers client is calling.

Emergency and Location-Based Functions

[00108] The IPCS can also make a number of basic and enhanced emergency services available to its users, which make full use of Smartphone functionality. For example, Enhanced 911 (or e911) may come as a standard mandatory feature for all iPCS users. Due to the roaming nature of cell service, 911 calls using e911 are routed to an e911 emergency center, which obtains location information from the caller or in the case of iPCS, through the phone's GPS capability.

[00109] The iPCS may also be configured to support emergency direct communications, for example, by having the e911 function automatically activate the mobile device's speakerphone to relay a message in the case of an emergency. This can be used for example, to notify an iPCS user of an emergency situation such as a home break-in, an elderly parent in distress, etc. Emergency Direct Communication can work in

tandem with other emergency services such as emergency bracelets, alarm companies, etc.

[00110] iPCS can also make full use of smartphone GPS functionality and provide users with a series of safety and convenience features. For example, e911 location services can be incorporated into the iPCS service to provide location data to the e911 service centre in the event of an emergency. For example, based on the phone's GPS coordinates, iPCS can resolve the nearest physical address and communicate this information to the e911 service centre as well as the mobile devices precise latitude and longitude.

[00111] Other GPS usages may also be contemplated. For example, a set of Convenience Service Buttons can provide for the user with easy assess to location-based services searches, such as via single button search access by major category such as food, gas, shopping and emergency services, for example.

[00112] While the present disclosure describes various exemplary embodiments, the disclosure is not so limited. To the contrary, the disclosure is intended to cover various modifications and equivalent arrangements included within the general scope of the present disclosure.

CLAIMS

What is claimed is:

1. A mobile subscriber system comprising:

a mobile data network access point;

a server accessible via said data network access point and operable to execute a telephony-over-IP application;

a thin client application executable on each subscriber's mobile communication device to interface with said telephony-over-data application via said mobile data network access point; and

a subscriber account database tracking data consumption by each said subscriber interfacing with said telephony-over-IP application via respective executions of said thin client application, against a respective all-data mobile subscription account associated with each said subscriber.

2. The mobile subscriber system of claim 1, wherein said telephony-over-data application includes a voice-over-data function and a SMS-over-data function, wherein said subscriber account database independently tracks data consumption associated with each of said voice-over-data function and said SMS-over-data function.

3. The mobile subscriber system of claim 1 or claim 2, wherein said subscriber account database further independently tracks data consumption associated with a Web-based function implemented via said mobile data network access point.

4. The mobile subscriber system of claim 3, wherein said thin client application is further executable to access a current data consumption metric relative to an overall data consumption allocation.

5. The mobile subscriber system of claim 4, wherein said current data consumption metric is subdivided into respective data consumption metrics for voice-over-data usage, SMS-over-data usage and Web-based usage.

6. The mobile subscriber system of any one of claims 1 to 5, wherein said thin client application is further executable by a first subscriber associated with a first all-data mobile subscription account to transfer a data consumption allocation quantum to a second subscriber associated with a second mobile subscription account.

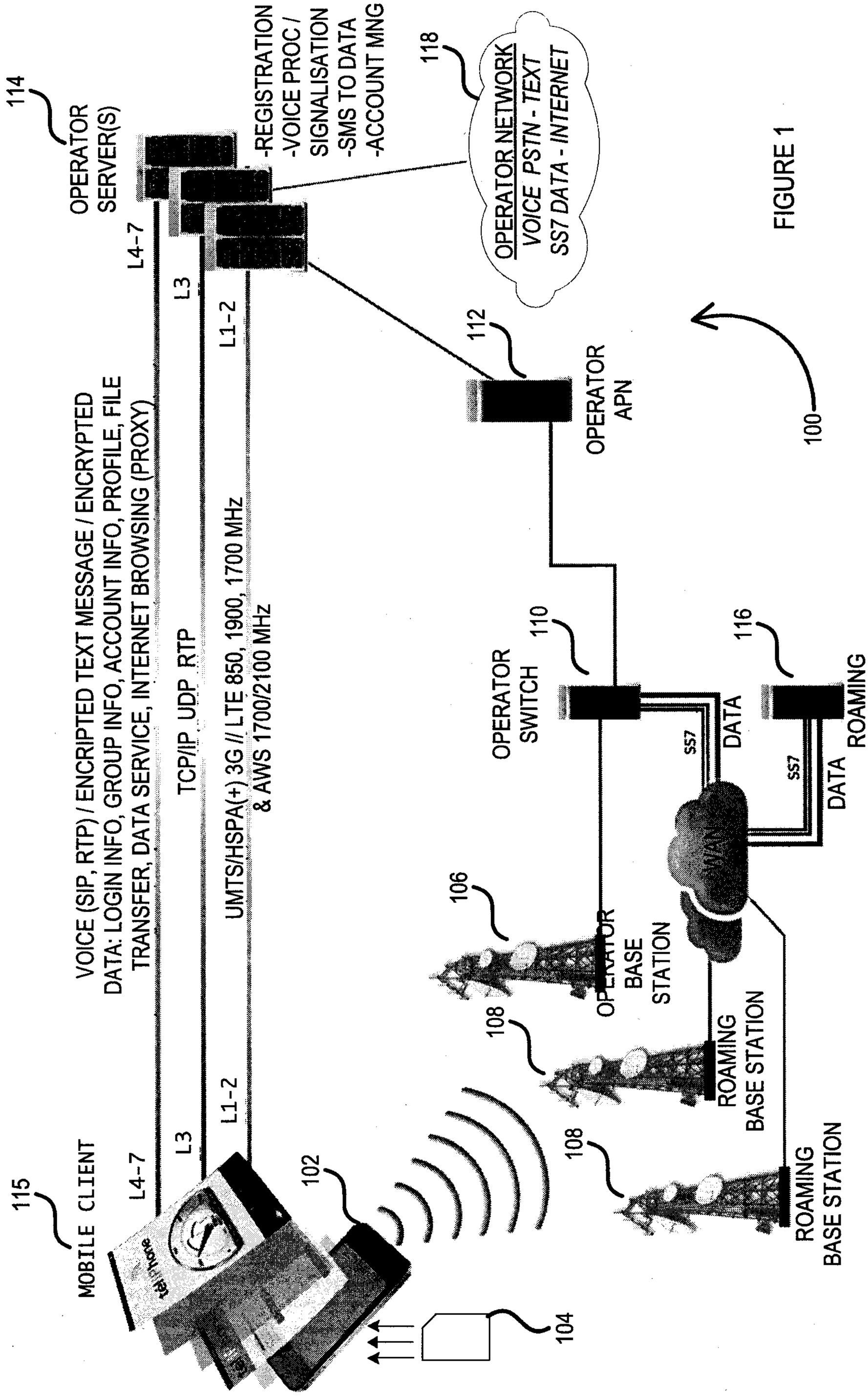

114
OPERATOR SERVER(S)
-REGISTRATION
-VOICE PROC / SIGNALISATION
-SMS TO DATA
-ACCOUNT MNG
118
OPERATOR NETWORK
VOICE PSTN - TEXT
SS7 DATA - INTERNET
L4-7
L3
L1-2
VOICE (SIP, RTP) / ENCRIPTED TEXT MESSAGE / ENCRYPTED
DATA: LOGIN INFO, GROUP INFO, ACCOUNT INFO, PROFILE, FILE
TRANSFER, DATA SERVICE, INTERNET BROWSING (PROXY)
TCP/IP UDP RTP
UMTS/HSPA(+) 3G // LTE 850, 1900, 1700 MHz
& AWS 1700/2100 MHz
112
OPERATOR APN
110
OPERATOR SWITCH
116
ROAMING MANAGEMENT
100
106
OPERATOR BASE STATION
108
ROAMING BASE STATION
SS7
DATA
SS7
DATA
108
ROAMING BASE STATION
115
MOBILE CLIENT
102
104

FIGURE 1

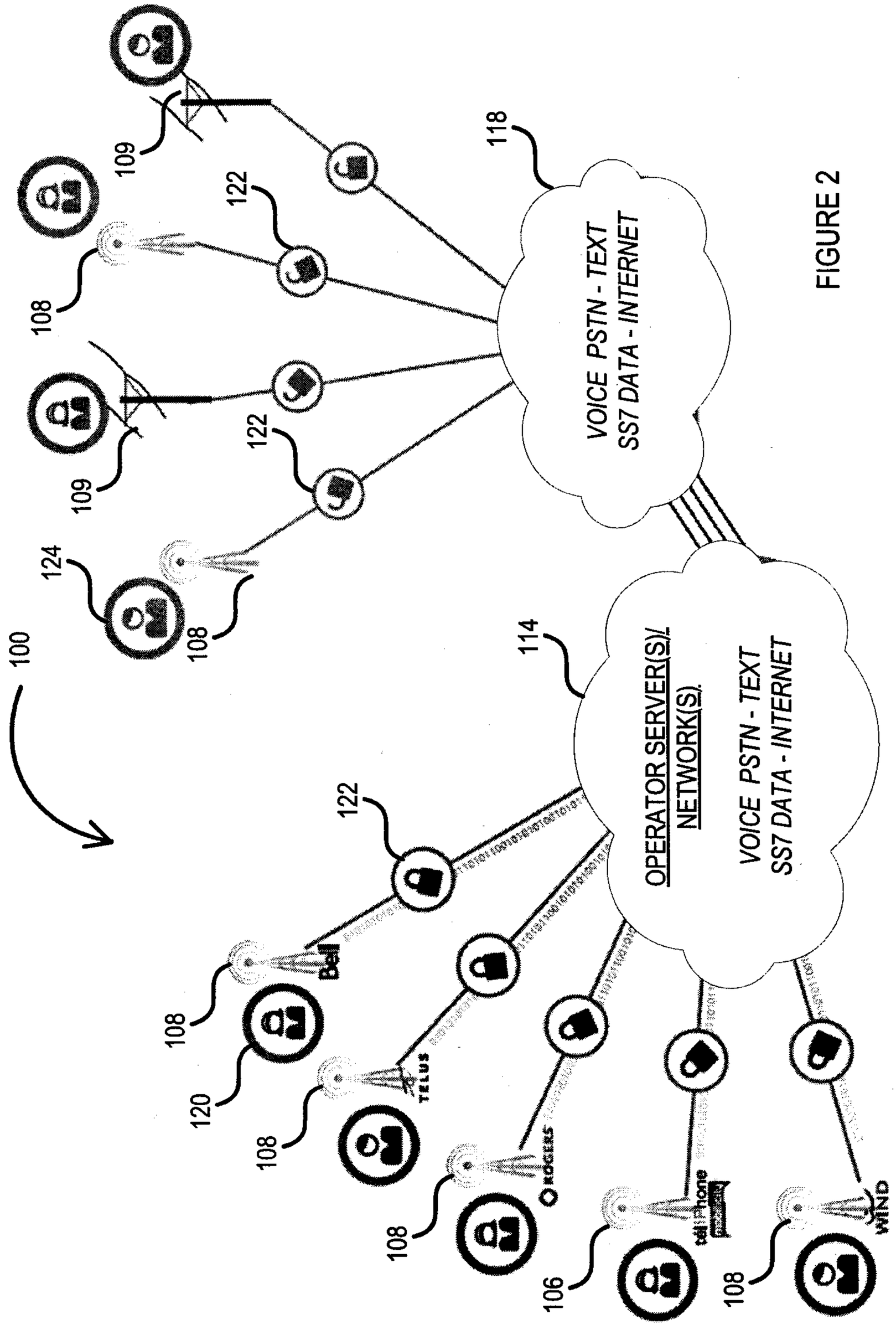

100
108
109
122
124
118
VOICE PSTN - TEXT
SS7 DATA - INTERNET
114
OPERATOR SERVER(S)/
NETWORK(S).
VOICE PSTN - TEXT
SS7 DATA - INTERNET
106
120
Bell
TELUS
ROGERS
WIND

FIGURE 2

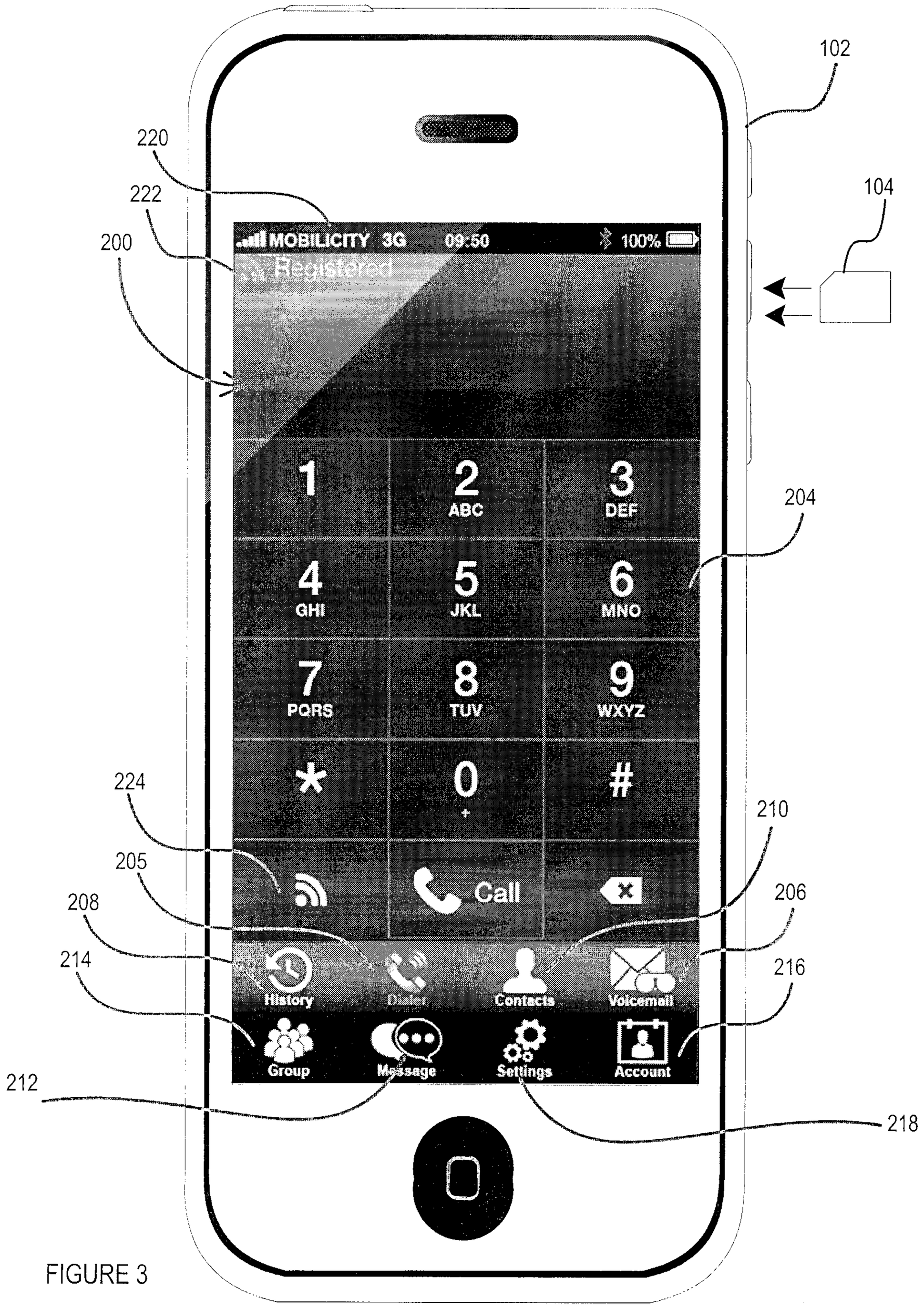

102
220
222
200
104
MOBILICITY 3G 09:50 100%
No Registered
1
2 ABC
3 DEF
4 GHI
5 JKL
6 MNO
204
7 PQRS
8 TUV
9 WXYZ
*
0 +
#
224
205
208
214
210
206
216
Call
History
Dialer
Contacts
Voicemail
Group
Message
Settings
Account
212
218

FIGURE 3

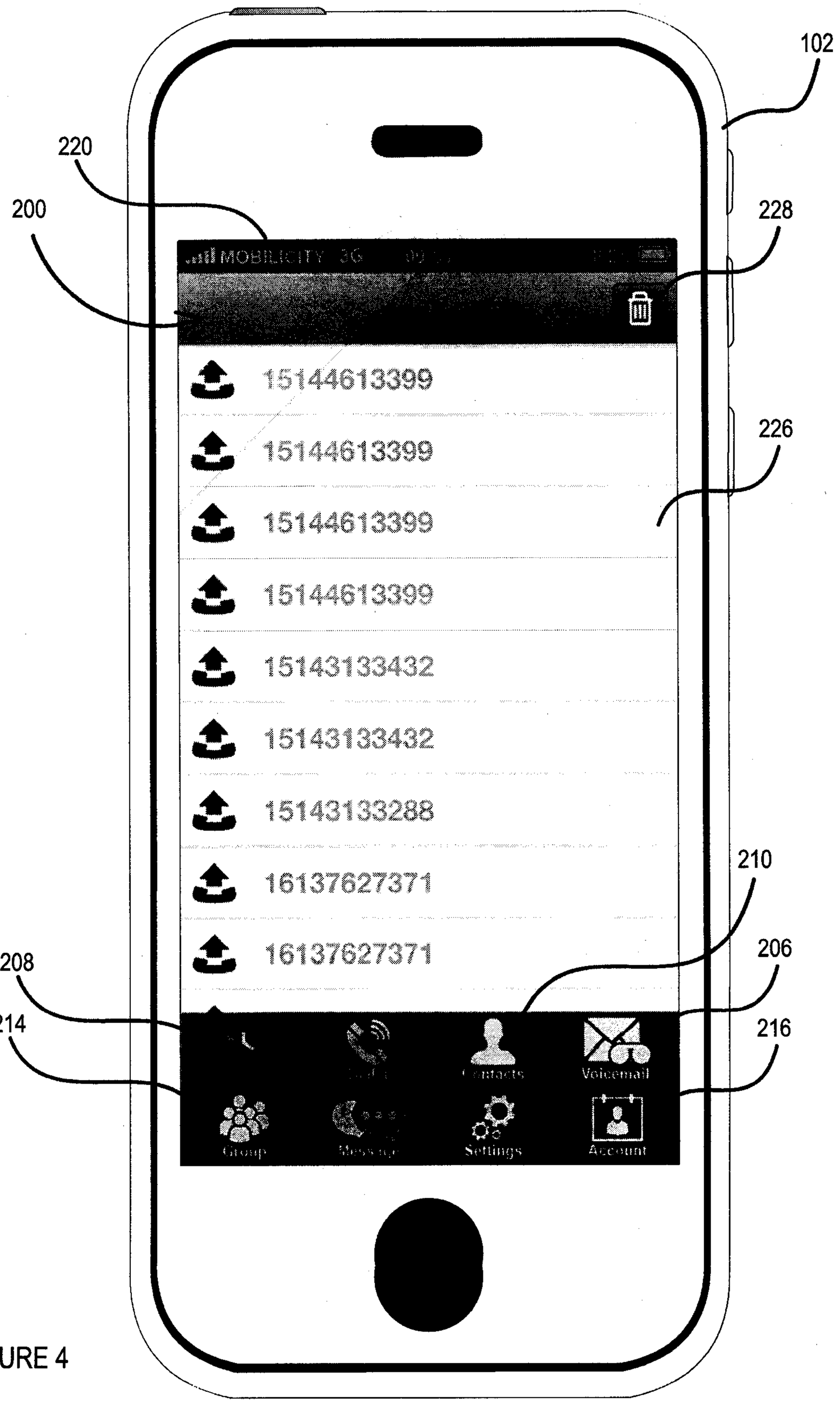

102
220
200
228
MOBILICITY 3G
15144613399
15144613399
15144613399
15144613399
15143133432
15143133432
15143133288
16137627371
16137627371
226
210
208
206
214
216
Contacts
Voicemail
Group
Settings
Account

FIGURE 4

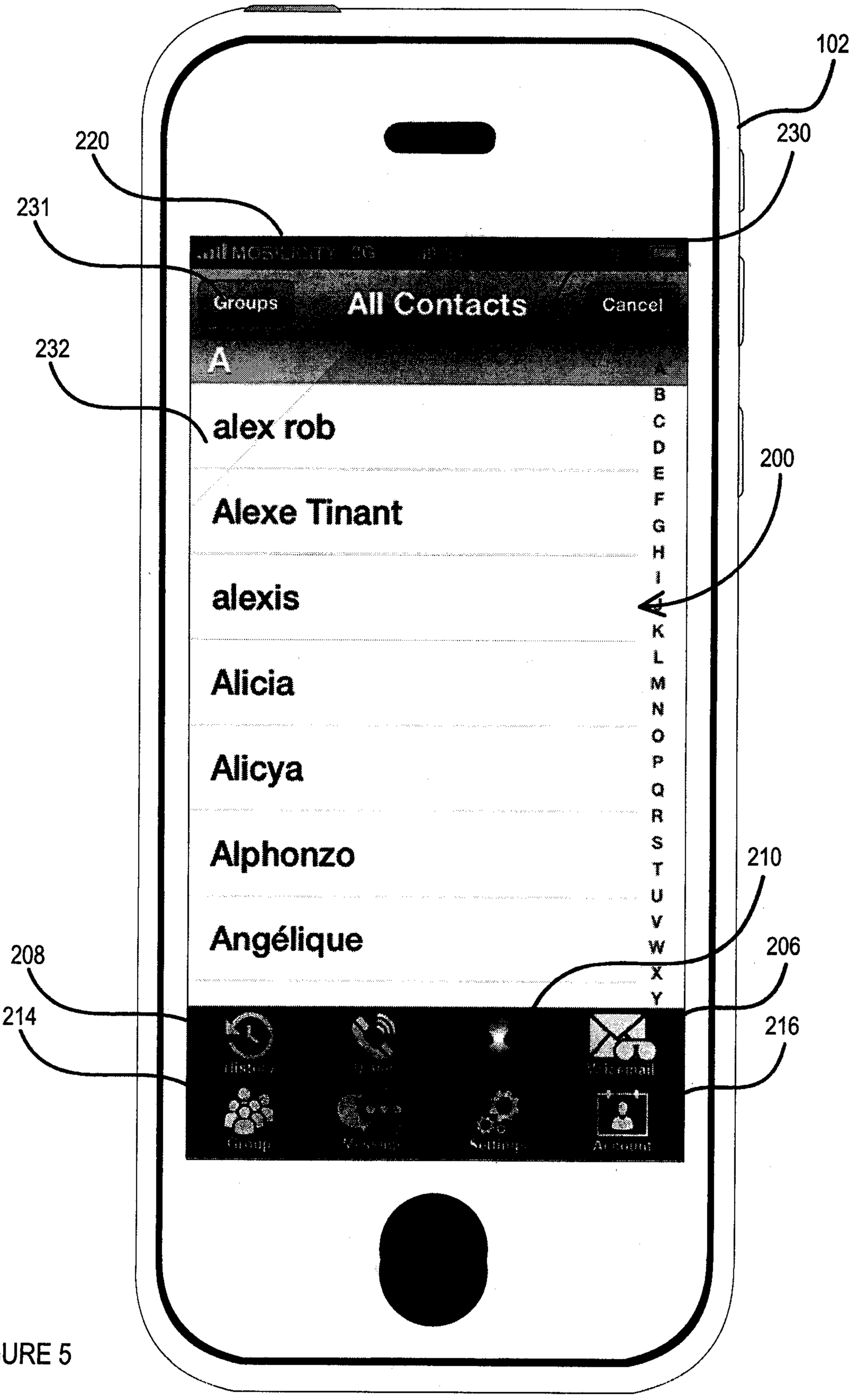

102
220
230
231
Groups
All Contacts
Cancel
232
A
alex rob
Alexe Tinant
alexis
Alicia
Alicya
Alphonzo
Angélique
200
B C D E F G H I J K L M N O P Q R S T U V W X Y
208
210
206
214
216

FIGURE 5

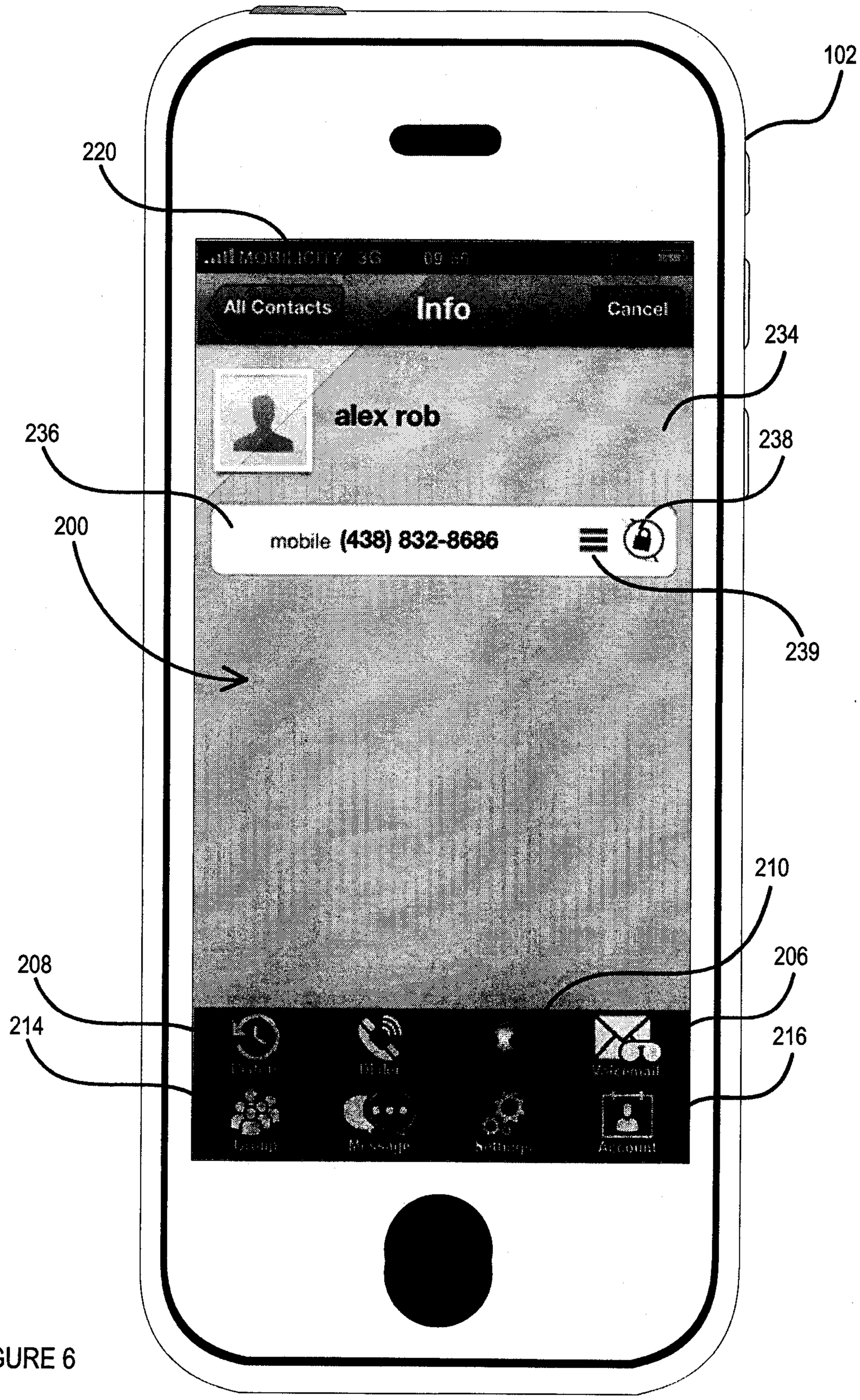

102
220
All Contacts
Info
Cancel
234
alex rob
236
238
mobile (438) 832-8686
200
239
210
208
206
214
216

FIGURE 6

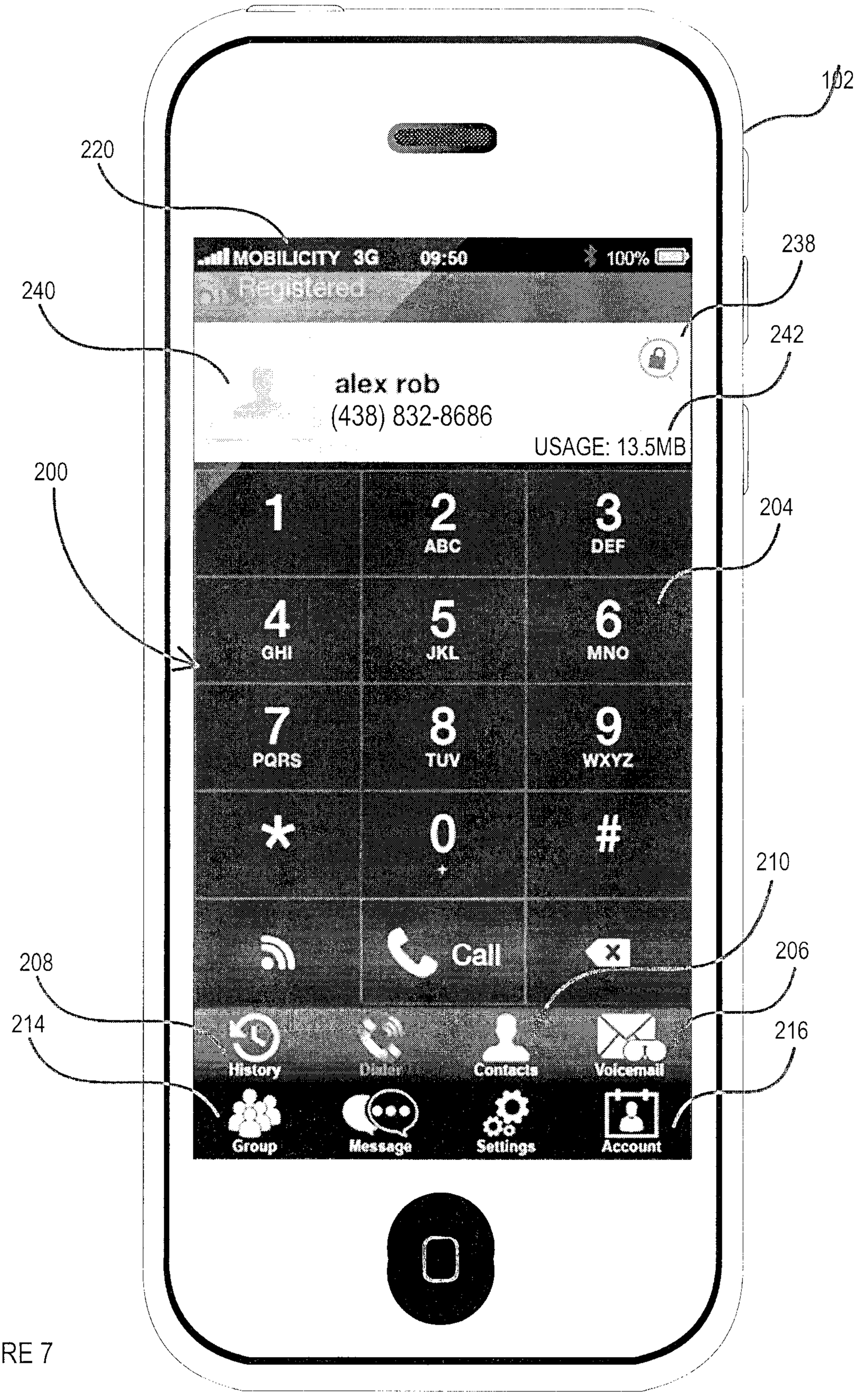

102
220
MOBILICITY 3G 09:50
100%
Registered
238
240
242
alex rob
(438) 832-8686
USAGE: 13.5MB
200
204
1
2 ABC
3 DEF
4 GHI
5 JKL
6 MNO
7 PQRS
8 TUV
9 WXYZ
*
0 +
#
Call
210
208
206
214
216
History
Dialer
Contacts
Voicemail
Group
Message
Settings
Account

FIGURE 7

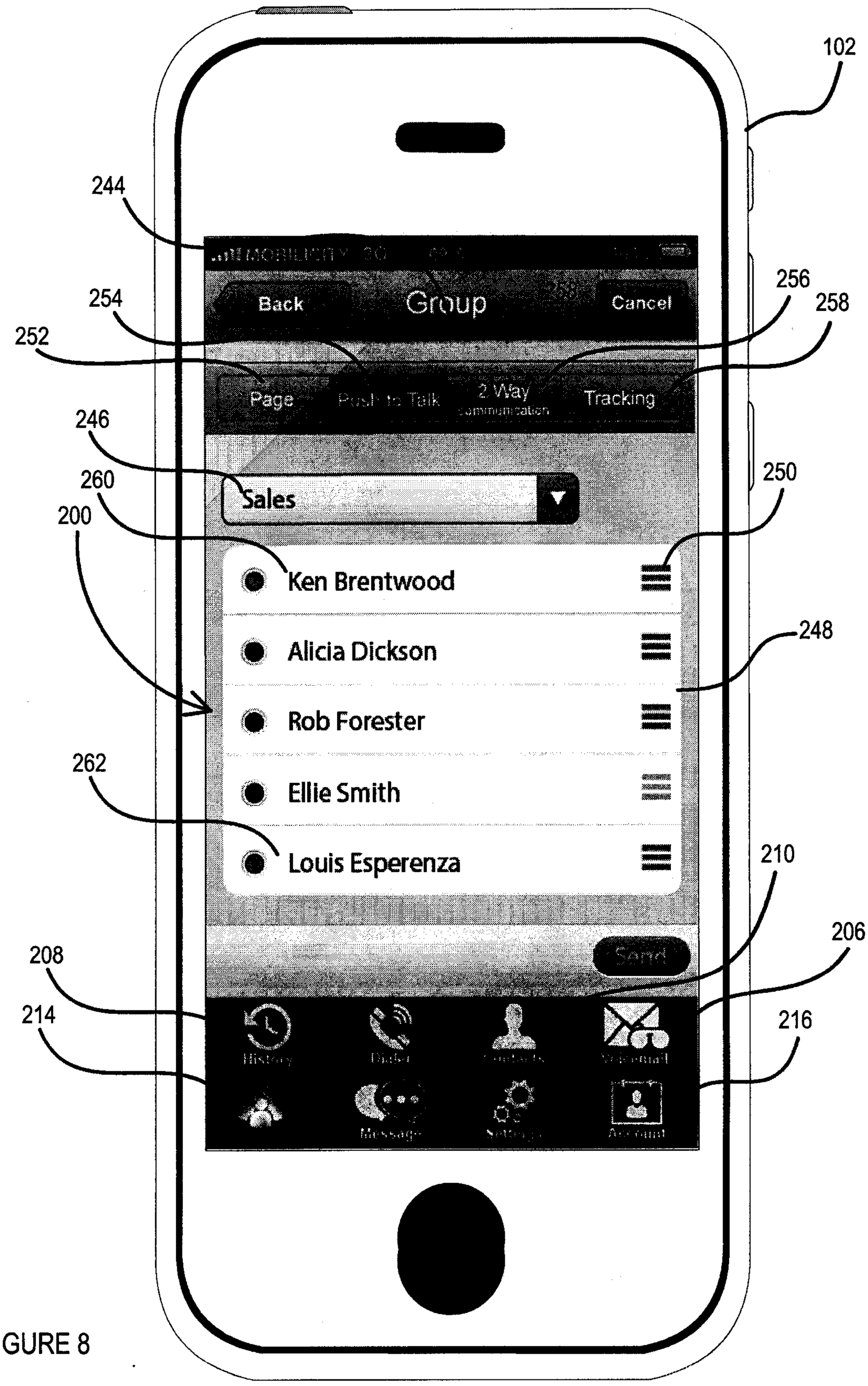

102
244
254
252
256
258
246
260
200
250
248
262
210
206
208
214
216
Back
Group
Cancel
Page
Push to Talk
2 Way
Tracking
Sales
Ken Brentwood
Alicia Dickson
Rob Forester
Ellie Smith
Louis Esperenza
Send

FIGURE 8

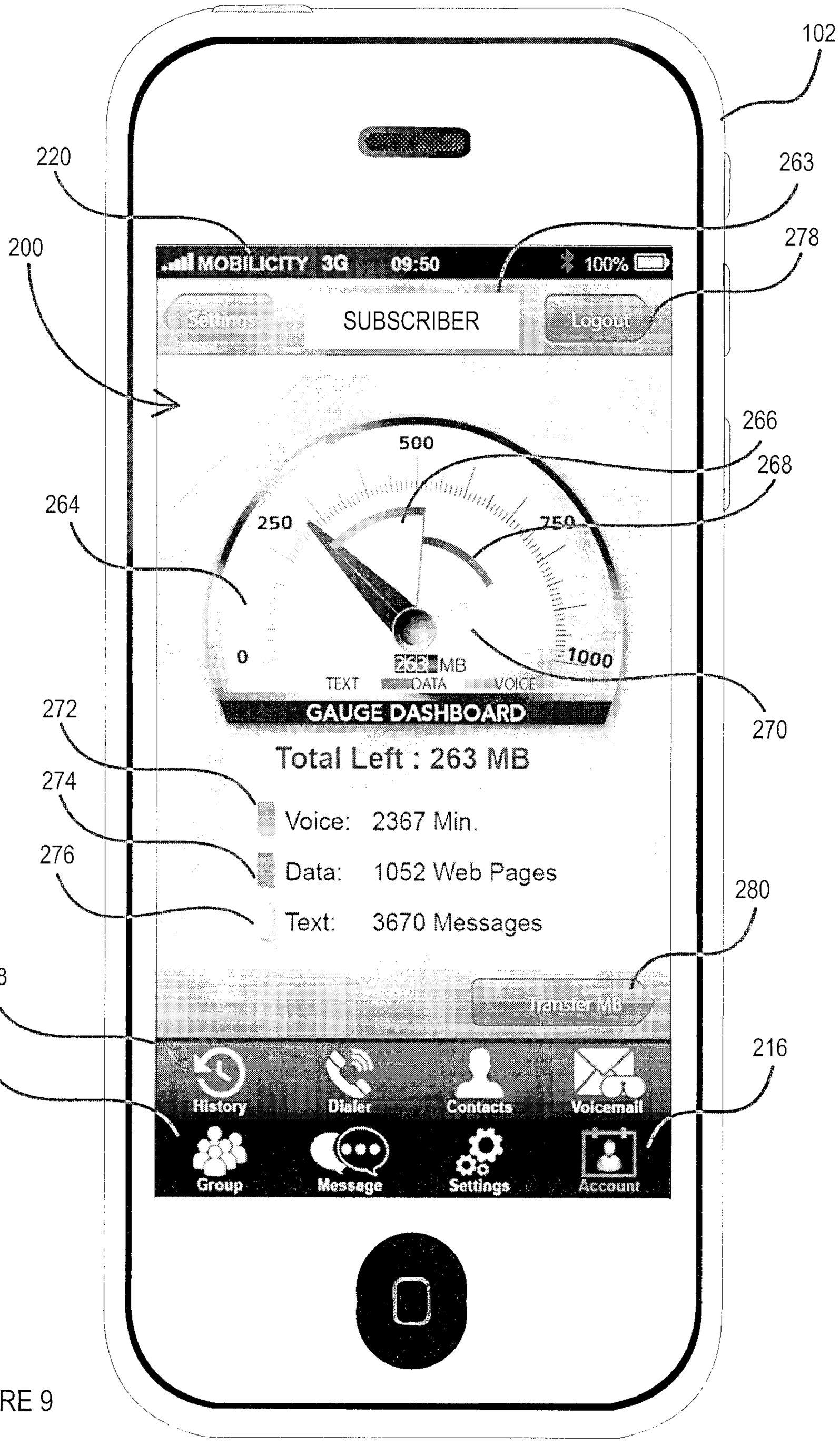

102
220
263
200
278
MOBILICITY 3G 09:50 100%
Settings
SUBSCRIBER
Logout
266
500
268
264
250
750
0
1000
MB
TEXT DATA VOICE
GAUGE DASHBOARD
272
270
Total Left : 263 MB
274
Voice: 2367 Min.
276
Data: 1052 Web Pages
Text: 3670 Messages
280
208
Transfer MB
214
216
History
Dialer
Contacts
Voicemail
Group
Message
Settings
Account

FIGURE 9

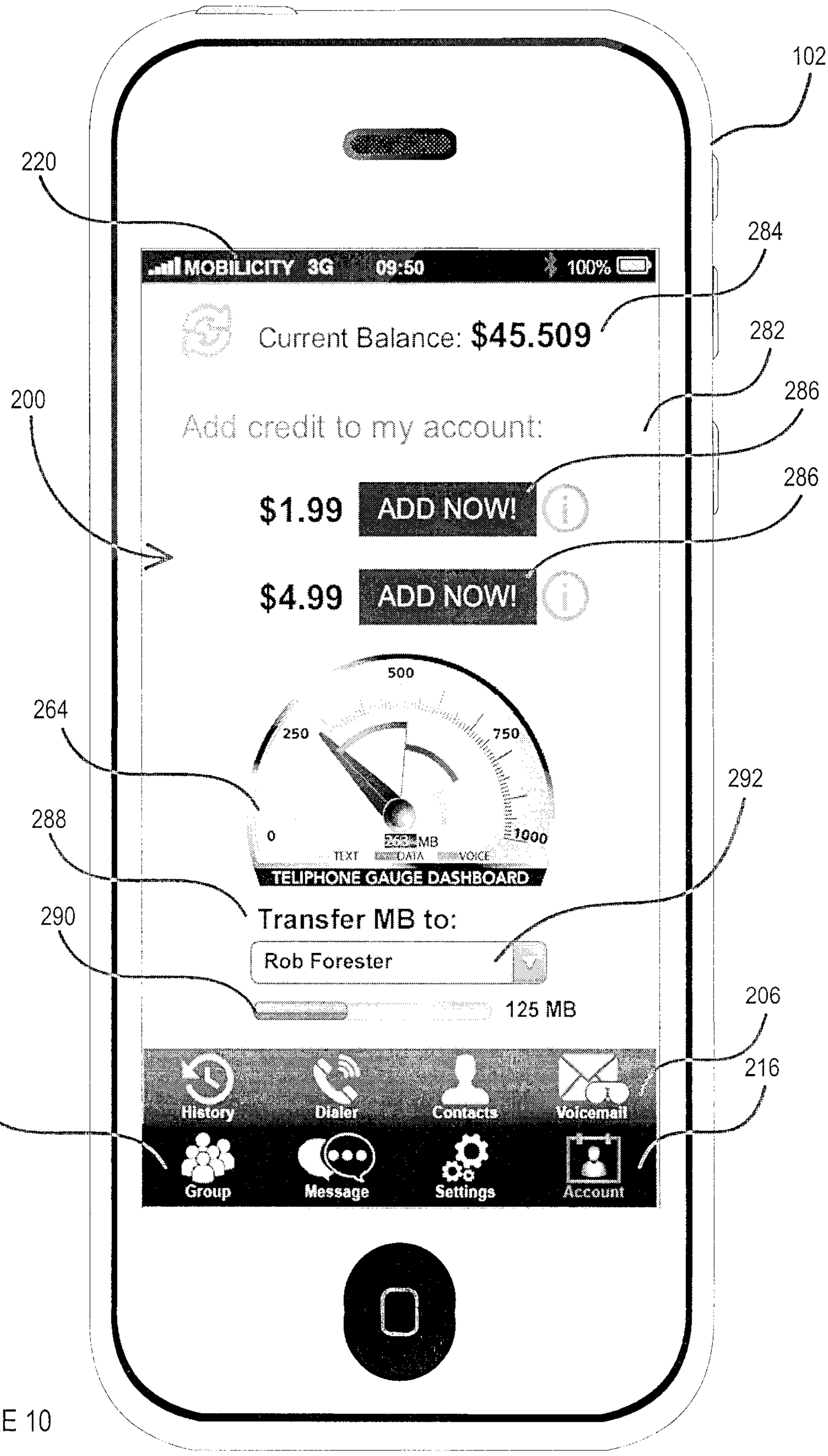

102
220
284
MOBILICITY 3G 09:50 100%
Current Balance: $45.509
282
200
286
Add credit to my account:
$1.99 ADD NOW!
286
$4.99 ADD NOW!
500
264
250
750
0
1000
MB
TEXT DATA VOICE
TELIPHONE GAUGE DASHBOARD
292
288
Transfer MB to:
Rob Forester
290
125 MB
206
214
216
History
Dialer
Contacts
Voicemail
Group
Message
Settings
Account

FIGURE 10

CS Service	$0	$9	$19	$29	$39	$49
MB	*Current provider data plan	125	300	500	650	850
Voice Minutes	*	1,000	2,400	4,000	5,200	6,800
or						
Data / Internet (pages)	*	500	1,200	2,000	2,600	3,400
or						
Text North America	*	10,000	24,000	40,000	52,000	68,000
or						
Text Global	*	5,000	12,000	20,000	26,000	34,000
or						
Text Picture Message	*	250	600	1,000	1,300	1,700
or						
Or any combination	9 minutes talk = 1 MB • 90 text messages = 1MB • 4 Web pages = 1 MB					

FIGURE 11

Canadian National Coverage	See your provider	✔	✔	✔	✔	✔
Your phone number anywhere in Canada or any of 50 countries	✔	✔	✔	✔	✔	✔
Voicemail (enhanced)	✔	✔	✔	✔	✔	✔
CallerID/Call Waiting & Forwarding, 3-way	✔	✔	✔	✔	✔	✔
Canada Long Distance	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited
US Long Distance	No	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited
Secure Communications	No	No	No	No	No	✔
E-911 Enhanced Can & USA	✔	✔	✔	✔	✔	✔
Push2Talk / 2way Com/ Paging/ Track	✔	✔	✔	✔	✔	✔

FIGURE 12

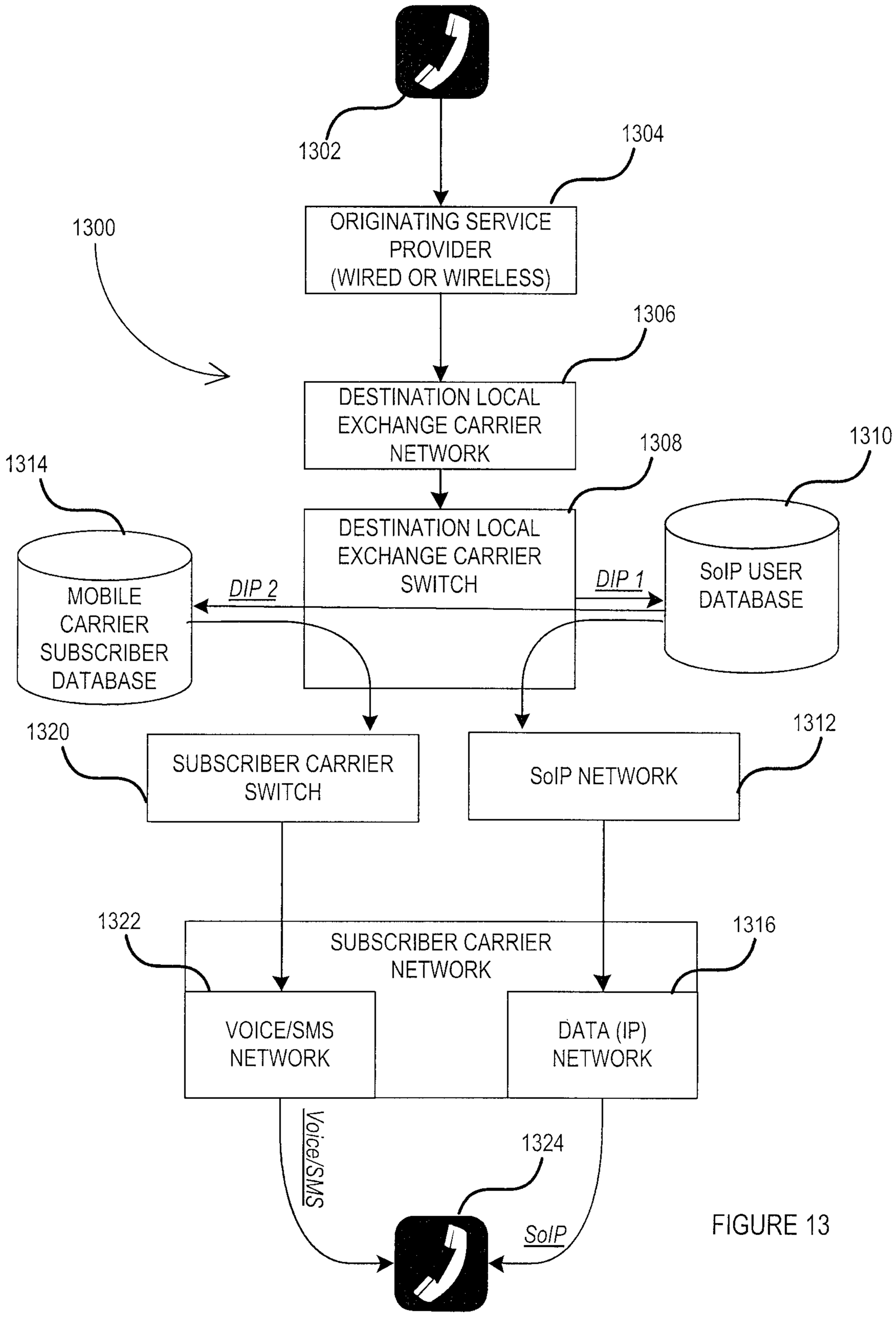
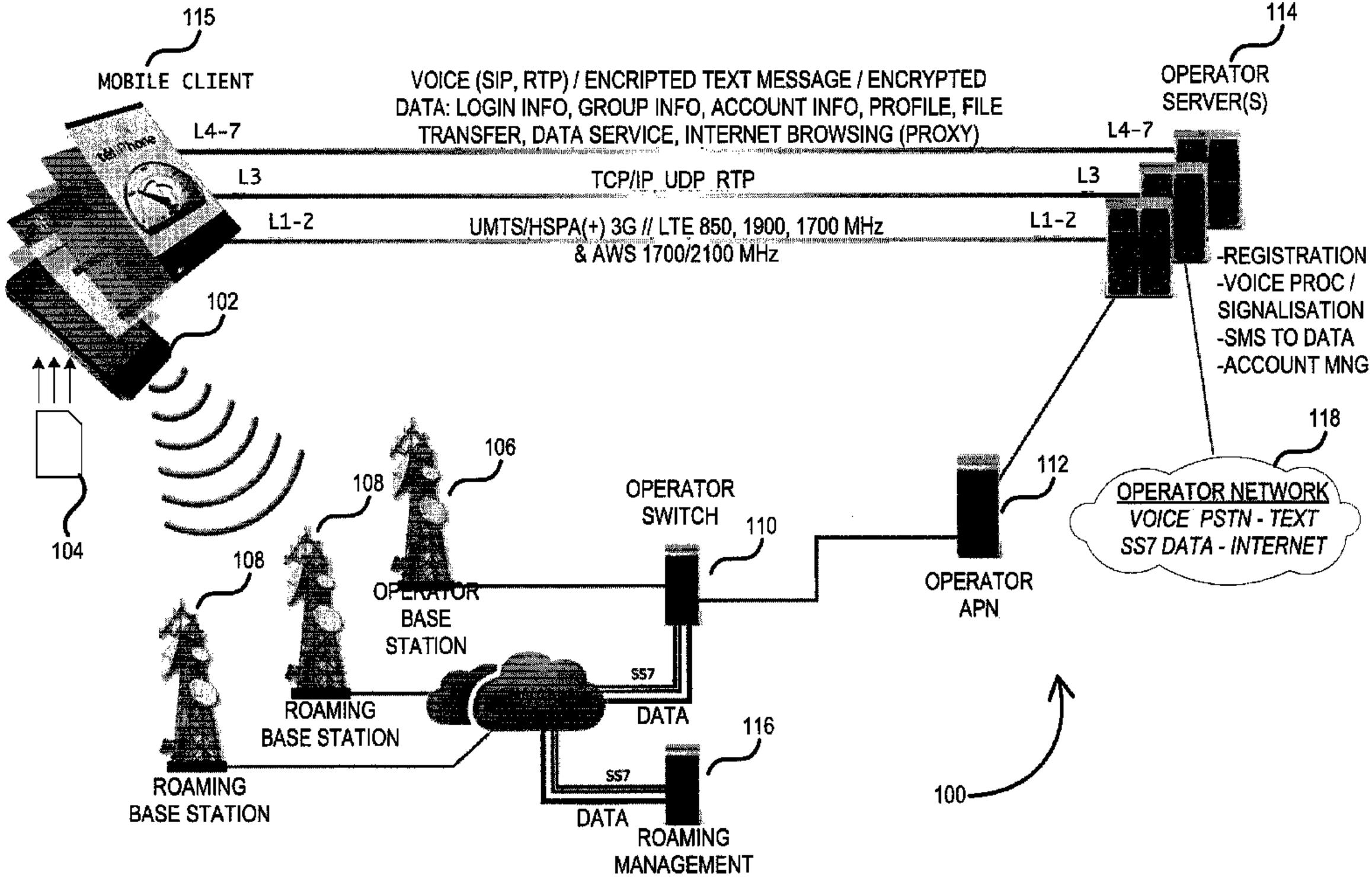

1300
1302
1304
ORIGINATING SERVICE PROVIDER (WIRED OR WIRELESS)
1306
DESTINATION LOCAL EXCHANGE CARRIER NETWORK
1308
1310
1314
DESTINATION LOCAL EXCHANGE CARRIER SWITCH
DIP 2
DIP 1
MOBILE CARRIER SUBSCRIBER DATABASE
SoIP USER DATABASE
1320
1312
SUBSCRIBER CARRIER SWITCH
SoIP NETWORK
1322
1316
SUBSCRIBER CARRIER NETWORK
VOICE/SMS NETWORK
DATA (IP) NETWORK
Voice/SMS
1324
SoIP

FIGURE 13


115
MOBILE CLIENT
VOICE (SIP, RTP) / ENCRIPTED TEXT MESSAGE / ENCRYPTED DATA: LOGIN INFO, GROUP INFO, ACCOUNT INFO, PROFILE, FILE TRANSFER, DATA SERVICE, INTERNET BROWSING (PROXY)
114
OPERATOR SERVER(S)
L4-7
L4-7
L3
TCP/IP UDP RTP
L3
L1-2
UMTS/HSPA(+) 3G // LTE 850, 1900, 1700 MHz & AWS 1700/2100 MHz
L1-2
-REGISTRATION
-VOICE PROC / SIGNALISATION
-SMS TO DATA
-ACCOUNT MNG
102
104
106
108
108
108
OPERATOR BASE STATION
ROAMING BASE STATION
ROAMING BASE STATION
OPERATOR SWITCH
110
SS7
DATA
112
OPERATOR APN
118
OPERATOR NETWORK
VOICE PSTN - TEXT
SS7 DATA - INTERNET
116
SS7
DATA
ROAMING MANAGEMENT
100