



(51) International Patent Classification:
H04M 3/42 (2006.01) **H04L 29/06** (2006.01)

(21) International Application Number:
PCT/IB2009/056040

(22) International Filing Date:
17 December 2009 (17.12.2009)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/141,739 31 December 2008 (31.12.2008) US

(71) Applicant (for all designated States except US):
FRANCE TELECOM [FR/FR]; 6, place d'Alleray,
F-75015 Paris (FR).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **MOURYA, Manoj**
[IN/US]; 41551 Apricot Lane, Fremont, CA 94539 (US).
CATANZARITI, Sergio [US/US]; 2790 19th Avenue,
Appt 11, San Francisco, CA 94132 (US).

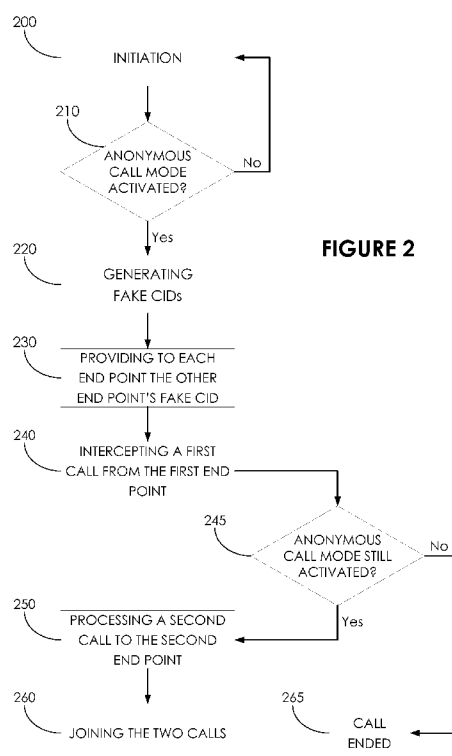
(74) Agent: **FRANCE TELECOM**
FTR&D/PIV/BREVETS; THIEL Frédéric, 38/40, rue du
Général Leclerc, F-92794 Issy Moulineaux Cedex 9 (FR).

(81) Designated States (unless otherwise indicated, for every
kind of national protection available): AE, AG, AL, AM,
AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ,
CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO,
DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT,
HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP,
KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD,
ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI,
NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD,
SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT,
TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every
kind of regional protection available): ARIPO (BW, GH,
GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM,
ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ,
TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE,
ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV,
MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM,

[Continued on next page]

(54) Title: A METHOD TO PROVIDE ANONYMOUS CALL MODE IN A TELECOMMUNICATION SYSTEM



(57) Abstract: A method for providing an anonymous call mode between a first (101) and a second (102) end points, each end point being characterized by a corresponding true caller identification (C ID), the true C IDs being used in a call to identify a caller and a callee of the call, the method including acts of generating (220) a first and second fake C IDs (actually temporary caller IDs), respectively for the first and second end points, when receiving a confirmation message that both the first and second end points requested the anonymous call mode, providing to each end point the other end point fake C ID (230), intercepting (240) a first call from the first end point to the second end point when identifying in the first call the second fake C ID as a callee C ID, processing (250) a second call to the second end point using the first fake C ID as a caller C ID, and joining (260) the first and second calls to generate a call from the first end point to the second end point, thereby hiding the true C IDs to both end points.



TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

— of inventorship (Rule 4.17(iv))

Declarations under Rule 4.17:

Published:

- as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))
- as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))

- with international search report (Art. 21(3))
- before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))

**A METHOD TO PROVIDE ANONYMOUS CALL MODE IN
A TELECOMMUNICATION SYSTEM**

5 FIELD OF THE PRESENT SYSTEM:

The present invention generally relates to communications using telecommunication devices in telecommunication networks, and more specifically to enhanced communications services.

10 BACKGROUND OF THE PRESENT SYSTEM:

Telecommunication devices, such as mobile or landline phones, have become important devices in our daily life. A mobile phone or device is generally a subscriber to a telecommunication network in order to enjoy communication services, such as voice, data, etc. A mobile
15 user is generally identified using an International Mobile Subscriber Identity, or IMSI. The mobile IMSI is a unique number associated with all GSM (Global System for Mobile communications) and Universal Mobile Telecommunications System (UMTS) network mobile phone users. It is stored in the Subscriber Identity Module (SIM) inside the phone. The SIM is
20 actually unique to one subscriber and carries information to identify that subscriber in his home network, i.e. the network he is a subscriber of. This information includes among other things the IMSI and further authentication data. The SIM is generally provided by the network operator when a user gets his subscription, and corresponds on this
25 network to a unique MSISDN (Mobile Station International Subscriber Directory Number) which is actually the mobile device phone number in this network.

A landline, main line or fixed-line is a telephone line which travels through a solid medium, either metal wire or optical fiber. This is
30 distinguished from a mobile cellular line mentioned here above, where

the medium used is the airwaves. A landline telecommunication device can be a hardwired phone or a wireless phone, both connected to a base device connected to the PSIN (Public Switched Telephone Network). Landline devices are also associated to phone number in the
5 PSIN.

When placing a call from a calling party to a called party (respectively named here after the caller and callee), the caller phone number may be presented to the callee device for identification of the caller. The caller phone number is generally referred to as the Caller ID or
10 CID in short. Presenting the Caller ID is a fairly recent service provided by most if not all network operators to their subscribers. For instance Caller ID presentation is a service offered by the PSIN today. CLIP (Calling Line Identification Presentation), a similar service offered for GSM mobile devices, is described in the document 3GPP (3rd Generation Partnership
15 Project) TS23.081. Different solutions are available to transmit the caller ID information to the callee device, for instance an SS7 (Signaling System 7) message for PSIN lines or an SIP (Session Initiation Protocol) message setup in GSM and UMTS networks for Voice over IP. When a contact list is available on the callee device, the contact name associated to the
20 incoming Caller ID may be presented to the callee in place of the Caller ID.

Caller IDs, when referring to phone numbers either for landline or mobile telecommunication devices, are defined according to standardized numbers recommended by ITU-T (Telecommunication
25 Standardization Sector) in the recommendation E.164 (Public telecommunication numbering plan). As they are unique to a given telecommunication device, they can be referred to as globally routable numbers, i.e. they can be dialed from any other telecommunication device to reach the given telecommunication device.

The Caller ID presentation can be problematic when the caller wants to keep his number secret, for instance when the caller and callee are two members of a social network who meet over their common interests.

5 Social networks, available through mobile networks and over the internet, are increasingly successful communication platforms. Members of a social network generally identify themselves through a login or pseudonym that maintains their true identity secret from other members. In some instances, it can be useful for two members to talk over the
10 phone and get to know each other. A problem arises when the members need to exchange contact information as they are at risk of providing their phone number to an untrustworthy member. Members may not be comfortable with sharing their private phones numbers. This is all the more important when the social network is a dating network.

15 Some platforms offer "click to call" services which allows members to speak to each other. The two members need to be connected to the social group simultaneously and the communication is established through the telecommunication device each member used to log in to the social network. When the device is a computer, the member or user
20 cannot move away from the computer as the computer microphone has a limited range. Furthermore, such a solution cannot be used for landline phones.

Another solution is for the caller to hide his Caller ID to the callee. Nevertheless, he will need to convince the callee to share his phone
25 number, which is not a satisfactory situation for him.

Today there is still a need for a simple solution that allows two parties to preserve their anonymity when calling each other. There is a further need for a solution that is accessible regardless of the type of telecommunication devices involved in the call.

SUMMARY OF THE PRESENT SYSTEM AND METHOD:

It is an object of the present system, processor and method to overcome disadvantages and/or make improvements in the prior art.

To that extent, the present method proposes a method for
5 providing an anonymous call mode between a first and a second end points, each end point being characterized by a corresponding true caller identification (CID), the true CIDs being used in a call to identify a caller and a callee of the call, the method comprising the acts of:

- generating a first and second fake CIDs, respectively for the first
10 and second end points, when receiving a confirmation message that both the first and second end points requested the anonymous call mode,
- providing to each end point the other end point fake CID,
- intercepting a first call from the first end point to the second end
15 point when identifying in the first call the second fake CID as a callee CID,
- processing a second call to the second end point using the first fake CID as a caller CID,
- joining the first and second calls to generate a call from the first
20 end point to the second end point, thereby hiding the true CIDs to both end points.

Thanks to the present method, the user of the first end point will only place a call using the contact information, i.e. the second fake Caller ID, he/she knows for the user of the second end point. The second
25 user will receive a call with a Caller ID corresponding to fake Caller ID of the first end point. The true Caller ID of both users are never revealed to the other user, thanks to the three stage calling process (first call and second call, and joining of the two calls). Such a process is permitted once both users have requested the anonymous call mode and the fake
30 Caller IDs have been generated.

The present system also relates to a service node for providing an anonymous call mode between a first and a second end points, each end point being characterized by a corresponding true caller identification (CID), the true CIDs being used in a call to identify a caller and a callee, the service node being arranged to:

- generate a first and second fake CIDs, respectively for the first and second end points, when receiving a confirmation message that both the first and second end points requested the anonymous call mode,
- 10 - provide to each end point the other end point fake CID,
- intercept a first call from the first end point to the second end point when identifying in the first call the second fake CID as a callee CID,
- process a second call to the second end point using the first fake
15 CID as a caller CID,
- join the first and second calls to generate a call from the first end point to the second end point, thereby hiding the true CIDs to both end points.

A telecommunication system in accordance with the present
20 system may comprise:

- a first and a second end point, each of the end points being characterized by a corresponding true caller identification (CID), the true CIDs being used in a call to identify a caller and a callee of the call,
- a social network server, hosting a social network each user of an
25 end point is a member of, the social network server being arranged to offer the activation of an anonymous call mode to the users of the first and second end points,
- a service node for providing an anonymous call mode between the first and a second end points, the service node being arranged to:

- generate a first and second fake CIDs, respectively for the first and second end points, when receiving from the social network server a confirmation message that both the first and second end points activated the anonymous call mode,

5 - provide to each end point the other end point fake CID,

- intercept a first call from the first end point to the second end point when identifying in the first call the second fake CID as a callee CID,

- process a second call to the second end point using the first fake
10 CID as a caller CID,

- join the first and second calls to generate a call from the first end point to the second end point, thereby hiding the true CIDs to both end points.

An application embodied on a computer readable medium in
15 accordance with the present system may be arranged to provide an anonymous call mode between a first and a second end point, each end point being characterized by a corresponding true caller identification (CID), the true CIDs being used in a call to identify a caller and a callee in a call, the application comprising:

20 - a portion to generate a first and second fake CIDs, respectively for the first and second end points, when receiving a confirmation message that both the first and second end points requested the anonymous call mode,

- a portion to provide to each end point the other end point fake
25 CID,

- a portion to intercept a first call from the first end point to the second end point when identifying in the first call the second fake CID as a callee CID,

- a portion to process a second call to the second end point using
30 the first fake CID as a caller CID,

- a portion to join the first and second calls to generate a call from the first end point to the second end point, thereby hiding the true CIDs to both end points.

5 BRIEF DESCRIPTION OF THE DRAWINGS:

The present system, call management node and method are explained in further detail, and by way of example, with reference to the accompanying drawings wherein:

FIG. 1 shows an illustrative embodiment of the present system;

10 FIG. 2 is a flow chart illustrating an embodiment of the present method;

FIG. 3 shows another illustrative embodiment of the present system; and,

FIG. 4 is another illustrative embodiment of the present system.

15

DETAILED DESCRIPTION OF THE PRESENT SYSTEM AND METHOD:

The following are descriptions of exemplary embodiments that when taken in conjunction with the drawings will demonstrate the above noted features and advantages, and introduce further ones.

20 In the following description, for purposes of explanation rather than limitation, specific details are set forth such as architecture, interfaces, techniques, etc., for illustration. However, it will be apparent to those of ordinary skill in the art that other embodiments that depart from these details would still be understood to be within the scope of the appended
25 claims.

Moreover, for the purpose of clarity, detailed descriptions of well-known devices, systems, and methods are omitted so as not to obscure the description of the present system. Furthermore, routers, servers, nodes, base stations, gateways or other entities in a telecommunication

network are not detailed as their implementation is beyond the scope of the present system and method.

For purposes of simplifying a description of the present system, the terms "operatively coupled", "coupled", and formatives thereof as utilized 5 herein refer to a connection between devices and/or portions thereof that enables operation in accordance with the present system. For example, an operative coupling may include one or more of a wired connection and/or a wireless connection between two or more devices that enables a one and/or two-way communication path between the 10 devices and/or portions thereof. For example, an operative coupling may include a wired and/or wireless coupling to enable communication between a social network server and one or more user devices. A further operative coupling, in accordance with the present system may include one or more couplings between two or more user devices, such as via a 15 telecommunication network in accordance with an embodiment of the present system.

Unless specified otherwise, the exemplary embodiment here after will be described in its application to mobile devices characterized by the Caller ID as provided by the Telecommunication Network (Telco) the 20 users are subscribers of. This Caller ID will be referred to as the primary or true Caller ID and corresponds to the unique number MSISDN or mobile phone number, i.e. the number through which the device can be reached. This illustration is in no way a limitation of the scope of the present method and system as telecommunication devices such as fixed 25 devices or communication devices behind a PBX (Private Branch eXchange) may implement the present teachings. Variations to the present system will be detailed later on when one or both the parties involved in the anonymous call are not subscriber of the Telco providing the present method.

Furthermore, what will be referred to as a "call" in this description may be a standard voice call or any other communication session established between a first party, referred to as the first user, or caller, and another party referred to as the second user, or callee. One will
5 understand of course that the call is placed more precisely between the users telecommunication devices, i.e. the calling device and the called device, for instance a video call between the first and second users, or data exchange between devices. Each side of the call in the telecommunication network will be referred to as
10 a branch or a leg of the call. The call may also be referred to as a communication path between the two devices. When a communication path is set up between both calling and called devices, different entities of the present telecommunication system are involved and this path generally involves a two level exchange mechanism:

- 15 - a signaling level corresponding to the signaling (or set up) messages exchanges through the network entities between the two devices,
- a media level for handling data, voice, etc.

Furthermore, the calling and called devices will also be referred to
20 as end points as they represent both ends to the communication path.

In addition, it should be expressly understood that the drawings are included for illustrative purposes and do not represent the scope of the present system.

FIG. 1 shows an exemplary embodiment of the present system. A
25 first telecommunication device, or first end point, 101 is illustrated as a mobile device comprising a SIM with information to identify itself in its network 160. The first device 101, belonging to a first user A, is further characterized by a first Caller ID NUM_A, which corresponds to its primary Caller ID. In the exemplary embodiment of a GSM or UMTS network, a
30 device is associated to the unique IMSI in its subscriber network as

explained before. The Caller ID is generally the MSISDN associated to this IMSI. Depending on the type of network the Caller ID could be a different identifier for the calling device. It could be for instance metadata associated to the user, like a picture or details information about this user
5 such as a name and address, depending on the possibility offered by the network as well as the consent of the user. The term Caller ID will encompass these different possibilities. When placing a call, the first device is referred to as the calling device.

A second device 102 or second end point is also provided in the
10 present network. When receiving the call, the second device will be referred to as the called device. The second device 102 belongs to a second user B and is further characterized by a second Caller ID NUM_B, which corresponds to its primary Caller ID. When a call is placed from user A to user B, user A is the caller while user B is the callee.

15 The present system also comprises a telecommunication network 160, or Telco, both users are subscribers of. One mobile switching center (MSC) 110 is provided to handle communications between users of network 160. A database 115 is associated to MSC 110 for storing information about subscribers of Telco 160, and more specifically about
20 users A and B.

A social network (or community) server 150 is also provided in the present system for offering a social network platform to users, whether subscribers of Telco 160 or not, to exchange information about themselves, common subjects of interest, news, sports ... The social
25 network may comprise communities like Myspace™, Facebook™, communities hosting blogs from users, etc. Such social network servers are generally accessible over the Internet. Users may need to register to a social network to become a member in order to receive or define a username, a profile to better describe himself/herself, etc. In the present

illustration of FIG. 1, both users A and B are members of a dating social network called dateme.com hosted on the social network server 150.

A partnership is also provided in the present system between Telco 160 and the social network. This partnership, as illustrated here after, ensures that relevant user information is passed on from the social network server 150 to the Telco 160 and subsequently to the users when both request an anonymous call mode according to the present system.

FIG. 2 is a flow chart illustrating an exemplary embodiment of the present method, wherein the first device places an anonymous call to the second device using the present method.

In a preliminary act 200, both users A and B register with the server 150 to become members of the social group dateme.com. They may register either through their respective first and second devices or through other devices with access to the internet. To that extent, they may define a personal profile, choose a username, etc. The username is generally a unique identifier to login to the social network server 150. This can be an email address for instance (like with Facebook™) or a username chosen by the user himself provided it has not been allocated before. User A and user B get to know each other through their online activity with the social group and decide to call each other using the anonymous call mode enabled with the present system.

The anonymous call mode may for instance be activated through mutual invitations like the friend invitation currently available on most social networks. The activation may be on a request/confirmation basis, i.e. one of the users, say user A, will send a request to the other user B, who can either accept the request or decline it. Both users A and B requesting the anonymous call mode may also trigger its activation simultaneously.

Provided one of the users does not accept or request the mode (answer no to act 210), the users A and B will not enjoy the possibility of

calling each other anonymously. When the anonymous call mode is activated (answer Yes to act 210), a confirmation message, comprising relevant user information or data, is passed on between the social network server 150 and Telco 160, confirming that both users A and B are
5 "paired" with the anonymous call mode of the present system. The partnership mentioned here above allows the transfer of such a confirmation message.

Relevant user information is information that permits Telco 160 to identify users from the social network who requested the anonymous call
10 mode of the present system. Such relevant user information may be for instance:

- the user Caller ID provided both users A and B registered with the social network server using their Caller ID for Telco 160,
- their unique identifier with the social network, provided Telco 160
15 can retrieve the corresponding subscriber. The anonymous call mode according to the present system may be offered to members of the social network through subscribing to a corresponding service provided by Telco 160. Upon subscribing to the service, users may have to provide the name of the social network as well as their username, so that Telco
20 160 can subsequently match the relevant user information provided in the confirmation message with the usernames as provided by users A and B when subscribing to the service.

Other user data such as their actual name, a membership number etc. are readily available to the man skilled in the art for identification by
25 Telco 160 of the anonymous call mode requesters.

Once both users A and B have been identified, in a further act 220, a fake Caller ID is generated for both users A and B, respectively FAKE_NUM_A and FAKE_NUM_B. In the present system, the fake Caller ID of a user is used as the contact data for the user, i.e. that it will be used

as the callee CID. As such this ID is unique as it is used in the present system to contact a user.

The fake Caller ID may be generated in different ways. In an additional embodiment of the present system, the fake Caller ID is
5 retrieved from a pool of available (i.e. non allocated) Caller IDs stored in database 115. Once the fake Caller IDs are allocated to both users A and B, Telco 160 may store in a table the correspondences between the actual and fake Caller IDs:

Social network	First user Caller ID	First user fake CID	Second user CID	Second user fake CID	Anonymous call mode
Dateme	NUM_A	FAKE_NUM_A	NUM_B	FAKE_NUM_B	Active
Dateme	NUM_A	FAKE_NUM_A	NUM_C	FAKE_NUM_C	Active
Facebook	NUM_A	FAKE_NUM_A	NUM_D	FAKE_NUM_D	Active
Facebook	NUM_D	FAKE_NUM_D	NUM_B	FAKE_NUM_B	Cancelled
Facebook	NUM_A	FAKE_NUM_A	NUM_E	FAKE_NUM_E	Active

10

Table 1: correspondences stored by Telco

As illustrated here after, the association of the different Caller IDs and fake Caller IDs for each couple of users will allow to guarantee an
15 anonymous call between these users. The anonymous call mode column is defined as "active" when a confirmation message from the social network server 150 has been received for both users A and B.

In an alternative embodiment of the present system, both fake Caller IDs may be generated through reversible functions using NUM_A,
20 NUM_B and the social network:

fake CID of callee = FUNCTION (caller CID, callee Caller ID, social network)

where in:

- callee is user B when caller is user A i.e. user A is the recipient of
5 the fake CID of callee, and reverse ly.

- the function FUNCTION is reversible, i.e. Telco - upon intercepting a call to a fake Caller ID - can retrieve the true caller CID and callee CID and the social network both users are members of.

This alternative embodiment is suitable when both users are
10 subscribers of Telco 160. Indeed the fake Caller IDs do not need to match standardized numbers as recommended by ITU-T in the recommendation E.164, and hence do not need to be globally routable numbers. For instance, a fake Caller ID could be a 12 digit number: XX YYYYYY ZZZZZ, where in:

15 - XX is an identifier for one of the social networks which partner with Telco 160,

- YYYYYY is a number representing the caller, i.e. the user who is the recipient of, i.e. who will receive the fake Caller ID,

- ZZZZZ is a number representing the callee, i.e. the real user
20 behind the fake Caller ID.

Other methods are readily available to the man skilled in the art to generate fake Caller IDs that associate in a reversible manner both users A and B primary Caller IDs and the social network. Each fake Caller ID, FAKE_NUM_A for user B and FAKE_NUM_B for user A, will also be used to
25 check the current status of the anonymous call mode between both users, as explained later on.

In a further act 230, the fake Caller ID of one end point is provided to the other end point. In other words, FAKE_NUM_A is provided to the second telecommunication device 102 of user B while FAKE_NUM_B is
30 provided to the first telecommunication device 101 of user A. The

provision may be carried out through a short message such as an SMS or MMS, or any other type of data transfer. SMS is a convenient support as it allows for mobile phones an update of the mobile phone contact list (also referred to as address book). The new entry will comprise for instance the name of the user as identified on the social group, i.e. the name used by user B to present himself/herself to user A, and the corresponding fake Caller ID, i.e. FAKE_NUM_B. Tables 2 and 3 here after illustrate the update of both users' contact list:

10

User B's phone	
Address book of user B	
User name A	FAKE_NUM_A

Table 2: user B address book updated through SMS

User A's phone	
Address book of user A	
Use mame B	FAKE_NUM_B
Use mame C	FAKE_NUM_C
Use mame D	FAKE_NUM_B

Table 3: user A address book updated through SMS

5

In an alternative embodiment according to the present system, both the generating of the fake Caller IDs and their provision to both users may be carried out by the social network server itself. In the agreements between Telco 160 and the social network platform 150, 10 these acts may be allocated to the social network itself. The fake Caller IDs, once generated, will then also be provided to the Telco so that it can process any subsequent anonymous calls between both users A and B.

Subsequent acts 240 to 265 correspond to an actual call using the 15 anonymous call mode. The hereafter call will be described with user A calling user B. The present teachings are of course transposable to user B calling user A. In a call between a caller and a callee, the caller and callee CIDs are respectively used to identify the caller and the callee, i.e. they are passed on as parameters in the call signaling messages 20 between the calling device, the Telco and the called device.

With a contact information for user B in his/her telecommunication device, user A can proceed with calling user B using the number

associated to user B in his/her address book, i.e. FAKE_NUM_B. A node in Telco 160, such as MSC 110, is aware of all call signaling messages within the network of Telco 160, and as such, can intercept in a further act 240 a first call from the first end point to the second end point, when
5 identifying in this first call the second fake CID FAKE_NUM_B as the callee CID. The first call corresponds to the first leg of the anonymous call between both users A and B. Whether the callee number belongs to a specific pool of numbers or has been generated using reversible functions, or any methods as mentioned before, MSC 110 can identify a
10 fake Caller ID in the first call issued from the first end point. The first call also comprises NUM_A as the caller CID.

With the first call, MSC 110 can identify:

- that user A is placing a call,
- to a fake Caller ID that actually belongs to user B (using the
15 reverse function of table 1),
- both users having requested an anonymous call mode through the social network dateme.com.

In an additional act 245, prior to processing the anonymous call mode, MSC 110 may verify if the anonymous call mode is still activated
20 between both users. Indeed, user B may have in the mean time requested the cancellation of the anonymous call mode. To do so, he/she may for instance cancel the mode associated to user A on his buddy list attached to his/her profile in the social network. Other deactivation of the mode may be readily available to the man skilled in
25 the art. Once the deactivation is completed on the social network, an update (deactivation message) is sent from social network 150 to Telco 160 so as to update the status of the anonymous call mode between both users. In the exemplary embodiment of Table 1, the last column gives the current status of the anonymous call mode between two users.
30 As seen with user C and user D, it has been cancelled by one of the two

users. With the exemplary embodiment of the XX YYYYYY ZZZZZ numbers, the identification of the social network through XX will allow MSC 110 to check the most up to date status of the anonymous call mode between user A and user B, as identified through YYYYYY and ZZZZZ respectively.

5 In the more generic exemplary embodiment, wherein the fake Caller ID is given by a reversible function, the social network component will cause the reverse function to return a "FALSE" result when Telco 160 has received a deactivation message for the anonymous call mode between both users A and B.

10 If the anonymous call mode is no longer activated (answer No to act 245), the call will not follow through and will end in a further act 265. Provided the anonymous call mode is still active (answer Yes to act 245), MSC 110 will process a second call to the second end point, using the first fake CID FAKE_NUM_A as the caller Caller ID and the primary Caller
15 ID NUM_B for the callee Caller ID. This second call corresponds to the second leg of the anonymous call between both users A and B. When receiving the second call (perceived as a regular call from user B side), user B will see an incoming call from user A, as identified from user B address book (as illustrated with Table 2), i.e. with FAKE_NUM_A as the
20 Caller ID. He/she can immediately recognize the member from the social network with whom he/she requested the anonymous call mode.

In a further act 260, MSC 110 will join the two calls, i.e. the first and second legs of the anonymous call. Thanks to the present system, Telco 160 performs a swap in the Caller IDs:

- 25
- from an outgoing call (first leg initiated from the first telecommunication device 101) from NUM_A to FAKE_NUM_B, to
 - an incoming call (second leg, bound to the second telecommunication device 102) from FAKE_NUM_A to NUM_B.

In accordance with the present system, one user need never actually know the other users true number. In the present system, the fake Caller ID of a user is both used:

- as the contact information to call the user,
- 5 - as an anonymous Caller ID to present himself/herself as the member from the social group, without giving out his/her actual number.

An interesting aspect with the additional act 245 (is the anonymous call mode still active ?) is the fact that the fake Caller IDs can be reused as soon as a deactivation message is received by Telco 160. Provided for
10 instance user B deactivated the anonymous call mode using the social network platform, as user A and user B are no longer "paired" with the present anonymous call service, any subsequent attempt by user A to call user B using FAKE_NUM_B will fail (answer No to act 245). Telco 160 may reallocate the number to another user B' involved with user A, or to
15 any other couple of members from the social network, as long as Telco 160 can identify such a number as the callee CID in a call and retrieve the two users, and the social network involved.

As mentioned before, when both users A and B are subscribers of Telco 160, fake Caller IDs do not need to be globally routable numbers.
20 In the event one if not two of the users are not subscribers, as the anonymous call mode is hosted in Telco 160, the fake Caller IDs will need to be globally routable numbers associated with Telco 160 so that the first call can be intercepted as intended to a number managed by Telco 160.

25 FIG. 3 is an illustration of the different setup messages that may be exchanged in the present system. Setup 1 corresponds to the registration of users A and B with server 150 to become members of social network datame.com. Setup 2 corresponds to the confirmation message that both users requested the anonymous call mode of the present system.
30 The setup 2 message may also be used when one of the two users

deactivate the anonymous call mode. Both setup 3 and 4 messages correspond to the transfer of the fake Caller IDs of a user to the other user, i.e.:

- setup 3 message to send FAKE_NUM_B and username B to user A,
- 5 - setup 4 message to send FAKE_NUM_A and username A to user B.

Setup 5 message will allow the processing of the first call from user A intended to user B. Setup 6 message corresponds to the processing of the second leg of the call, from user A presented with FAKE_NUM_A, to user B. As a consequence, a communication path (dashed line) will be
10 generated in an anonymous way between both users A and B.

In the hereabove illustrations, telecommunication devices 101 and 102 were illustrated as mobile devices, such as PDAs, cellular phones, smart phones and the likes. The present teachings can be readily implemented with either one, or both, of the first and second
15 telecommunication devices being a landline phone.

In the present illustration, MSC 110 is a node from Telco 160 implementing the present method. One may note that MSC 110 may comprise one or more parts and that illustrating the MSC 110 as comprising one part is in no way limiting as these more parts could be
20 hosted by one or more other nodes or servers of Telco 160, these parts being operatively coupled to each other. In accordance with a further embodiment of the present system, another coupled node other than MSC 110 in Telco 160 may readily implement the method according to the present system, provided it can intercept the first call, process the
25 second call and join these two calls. Such a node or the MSC, when implementing the present method may be seen as a service node offering the anonymous call mode.

The present system also brings enhanced anonymity as the user does not have to give his true Caller ID. Furthermore, as the anonymous

call mode may be available on a payment basis, identification of a user, and/or of the social network may allow further billings of the service.

FIG. 4 shows a system 400 in accordance with an embodiment of the present system. The system 400 includes a service node 490 hosting the present anonymous call mode. Service node 490 has a processor 410 operationally coupled to a memory 420, a rendering device 430, such as one or more of a display, speaker, etc., a user input device 470, such as a sensor panel, a keyboard, trackball and the likes, and a connection 440 operationally coupled to other entities and nodes of Telco 160 (not shown in FIG. 4). The connection 440 may be an operable connection between the service node 490 and another node or server that has similar elements as service node 490, such as a web server hosting one or more social networks.

The memory 420 may be any type of device for storing for instance the application data related to the operating system of the service node, as well as to application data in accordance with the present method. The application data are received by the processor 410 for configuring the processor 410 to perform operation acts in accordance with the present system. The operation acts include receiving the confirmation message, generating the fake Caller IDs and processing the first and second calls to ensure an anonymous call between two users A and B who requested the anonymous call mode of the present system.

The user input 470 may include a sensor panel as well as a keyboard, mouse, trackball, touchpad or other devices, which may be stand alone or be a part of a system, such as part of a personal computer (e.g., desktop computer, laptop computer, etc.) personal digital assistant, mobile phone, converged device, or other rendering device for communicating with the processor 410 via any type of coupling, such as a wired or wireless coupling. The user input device 470 is operable for interacting with the processor 410 including interaction within a paradigm

of a GUI and/or other elements of the present system, such as to enable entry of data by an operator.

Clearly the service node 490, the processor 410, memory 420, rendering device 430 and/or user input device 470 may all or partly be
5 portions of a computer system or other device, and/or be embedded in one or more servers.

The system, device and method described herein address problems in prior art systems. In accordance with an embodiment of the present system, the telecommunication devices 101 and 102 may interact with
10 service node 490 to enjoy an anonymous call mode in accordance with the present system. As may be readily appreciated, one or more of the user devices (i.e., first device 101, second device 102) may also include a corresponding processor, memory, rendering device, user input device and operable coupling as the service node 490 and as such, the
15 description of operation, etc. of the service node 490 should be understood to encompass a description of illustrative operable portions of the users devices, suitably coupled and configured for operation in accordance with the present system.

The methods of the present system are particularly suited to be
20 carried out by a computer software program, such program containing modules corresponding to one or more of the individual steps or acts described and/or envisioned by the present system. Such program may of course be embodied in a computer-readable medium, such as an integrated chip, a peripheral device or memory, such as the memory 420
25 or other memory coupled to the processor 410.

The computer-readable medium and/or memory 420 may be any recordable medium (e.g., RAM, ROM, removable memory, CD-ROM, hard drives, DVD, floppy disks or memory cards) or may be a transmission medium utilizing one or more of radio frequency (RF) coupling, Bluetooth
30 coupling, infrared coupling, etc. Any medium known or developed that

can store and/or transmit information suitable for use with a computer system may be used as the computer-readable medium and/or memory 420.

Additional memories may also be used. These memories configure
5 processor 410 to implement the methods, operational acts, and functions disclosed herein. The operation acts may include controlling the rendering device 430 to render elements in a form of a GUI and/or controlling the rendering device 430 to render other information in accordance with the present system.

10 Moreover, the term "memory" should be construed broadly enough to encompass any information able to be read from or written to an address in the addressable space accessed by a processor. With this definition, information on a network is still within memory 420, for instance, because the processor 410 may retrieve the information from the network
15 for operation in accordance with the present system. For example, a portion of the memory as understood herein may reside as a portion of the content providers, and/or the user device.

The processor 410 is capable of performing operations in response to incoming confirmation messages and first calls and executing
20 instructions stored in the memory 420. The processor 410 may be an application-specific or general-use integrated circuit(s). Further, the processor 410 may be a dedicated processor for performing in accordance with the present system or may be a general-purpose processor wherein only one of many functions operates for performing in
25 accordance with the present system. The processor 410 may operate utilizing a program portion, multiple program segments, or may be a hardware device utilizing a dedicated or multi-purpose integrated circuit.

Finally, the above discussion is intended to be merely illustrative of the present system and should not be construed as limiting the appended
30 claims to any particular embodiment or group of embodiments. Thus,

while the present system has been described with reference to exemplary embodiments, including user interfaces, it should also be appreciated that numerous modifications and alternative embodiments may be devised by those having ordinary skill in the art without departing from the broader and intended spirit and scope of the present system as set forth in the claims that follow. Further, while exemplary user interfaces are provided to facilitate an understanding of the present system, other user interfaces may be provided and/or elements of one user interface may be combined with another of the user interfaces in accordance with further embodiments of the present system.

The section headings included herein are intended to facilitate a review but are not intended to limit the scope of the present system. Accordingly, the specifications and drawings are to be regarded in an illustrative manner and are not intended to limit the scope of the appended claims.

In interpreting the appended claims, it should be understood that:

- a) the words "comprising" or "including" do not exclude the presence of other elements or acts than those listed in a given claim;
- b) the word "a" or "an" preceding an element does not exclude the presence of a plurality of such elements;
- c) any reference signs in the claims do not limit their scope;
- d) several "means" may be represented by the same item or hardware or software implemented structure or function;
- e) any of the disclosed elements may be comprised of hardware portions (e.g., including discrete and integrated electronic circuitry), software portions (e.g., computer programming), and any combination thereof;
- f) hardware portions may be comprised of one or both of analogue and digital portions;
- g) any of the disclosed devices or portions thereof may be

combined together or separated into further portions unless specifically stated otherwise;

h) no specific sequence of acts or steps is intended to be required unless specifically indicated; and

- 5 i) the term "plurality of" an element includes two or more of the claimed element, and does not imply any particular range of number of elements; that is, a plurality of elements may be as few as two elements, and may include an immeasurable number of elements.

CLAIMS

What is claimed is:

1. A method for providing an anonymous call mode between a first
5 and a second end point, each end point being characterized by a
corresponding true caller identification (CID), the true CIDs being used in
a call to identify a caller and a callee of the call, the method comprising
acts of:
 - generating a first and second fake CIDs, respectively for the first
10 and second end points, when receiving a confirmation message that
both the first and second end points requested the anonymous call
mode,
 - providing to each end point the other end point fake CID,
 - intercepting a first call from the first end point to the second end
15 point when identifying in the first call the second fake CID as a callee
CID,
 - processing a second call to the second end point using the first
fake CID as a caller CID,
 - joining the first and second calls to generate a call from the first
20 end point to the second end point, thereby hiding the true CIDs to both
end points.
2. The method of claim 1, further comprising, after the act of
intercepting a first call, an act of verifying that the anonymous call mode
25 is still active between the caller and the callee.
3. The method of claim 1, wherein the confirmation message
originates from a social network users of each end point are members of,
the confirmation message being issued when both users activated the
30 anonymous call mode.

4. The method of claim 1, wherein the fake CID of an end point is a reversible function of the true CIDs of the first end point, the second end point, and the social network.

5

5. The method of claim 4, wherein the anonymous call mode is hosted by a telecommunication network (Telco), one of the end points is not a subscriber of, the first and second fake CIDs corresponding to globally routable numbers attached to the Telco.

10

6. The method of claim 4, wherein the anonymous call mode is hosted by a telecommunication network (Telco), both end points are subscribers of.

15 7. A service node for providing an anonymous call mode between a first and a second end point, each end point being characterized by a corresponding true caller identification (CID), the true CIDs being used in a call to identify a caller and a callee, the service node being arranged to:

20 - generate a first and second fake CIDs, respectively for the first and second end points, when receiving a confirmation message that both the first and second end points requested the anonymous call mode,

- provide to each end point the other end point fake CID,

25 - intercept a first call from the first end point to the second end point when identifying in the first call the second fake CID as a callee CID,

- process a second call to the second end point using the first fake CID as a caller CID,

- join the first and second calls to generate a call from the first end point to the second end point, thereby hiding the true CIDs to both end points.

5 8. The service node of claim 7, further arranged to verify that the anonymous call mode is still active between the caller and the callee after intercepting the first call from the first end point to the second end point.

10 9. The service node of claim 7, wherein the fake CID of an end point is a reversible function of the true CIDs of the first end point, the second end point, and the social network.

15 10. A telecommunication system comprising:

- a first and a second end point, each of the end points being characterized by a corresponding true caller identification (CID), the true CIDs being used in a call to identify a caller and a callee of the call,

- a social network server, hosting a social network each user of an
20 end point is a member of, the social network server being arranged to offer activation of an anonymous call mode to the users of the first and second end points,

- a service node for providing an anonymous call mode between the first and a second end points, the service node being arranged to:

25 - generate a first and second fake CIDs, respectively for the first and second end points, when receiving from the social network server a confirmation message that both the first and second end points activated the anonymous call mode,

- provide to each end point the other end point fake CID,

- intercept a first call from the first end point to the second end point when identifying in the first call the second fake CID as a callee CID,

- process a second call to the second end point using the first fake
5 CID as a caller CID,

- join the first and second calls to generate a call from the first end point to the second end point, thereby hiding the true CIDs to both end points.

10 11. The system of claim 10, wherein the social network server is further arranged to send to the service node a deactivation message when one of the users requested the deactivation of the anonymous call mode, the service node being further arranged to terminate any first call from the first end point to the second end point once the deactivation message
15 has been received.

12. The system of claim 10, wherein the fake CID of an end point is a reversible function of the true CIDs of the first end point, the second end point, and the social network.

20

13. An application embodied on a computer readable medium and arranged to provide an anonymous call mode between a first and a second end points, each end point being characterized by a
25 corresponding true caller identification (CID), the true CIDs being used in a call to identify a caller and a callee in a call, the application comprising:

- a portion to generate a first and second fake CIDs, respectively for the first and second end points, when receiving a confirmation

message that both the first and second end points requested the anonymous call mode,

- a portion to provide to each end point the other end point fake CID,

5 - a portion to intercept a first call from the first end point to the second end point when identifying in the first call the second fake CID as a callee CID,

- a portion to process a second call to the second end point using the first fake CID as a caller CID,

10 - a portion to join the first and second calls to generate a call from the first end point to the second end point, thereby hiding the true CIDs to both end points.

14. The application of claim 13, further comprising a portion to verify
15 that the anonymous call mode is still active between the caller and the callee after intercepting the first call from the first end point to the second end point.

1/4

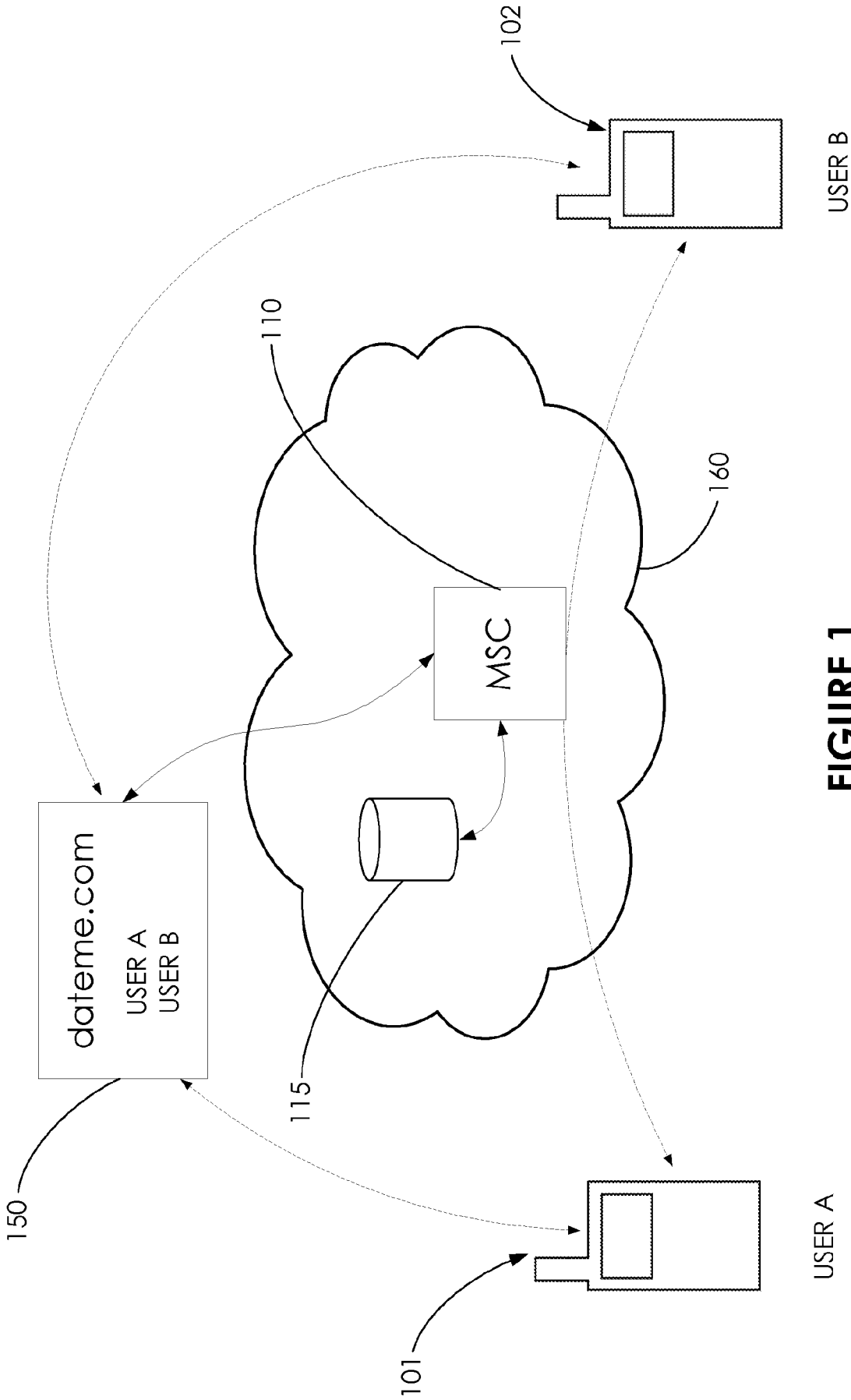
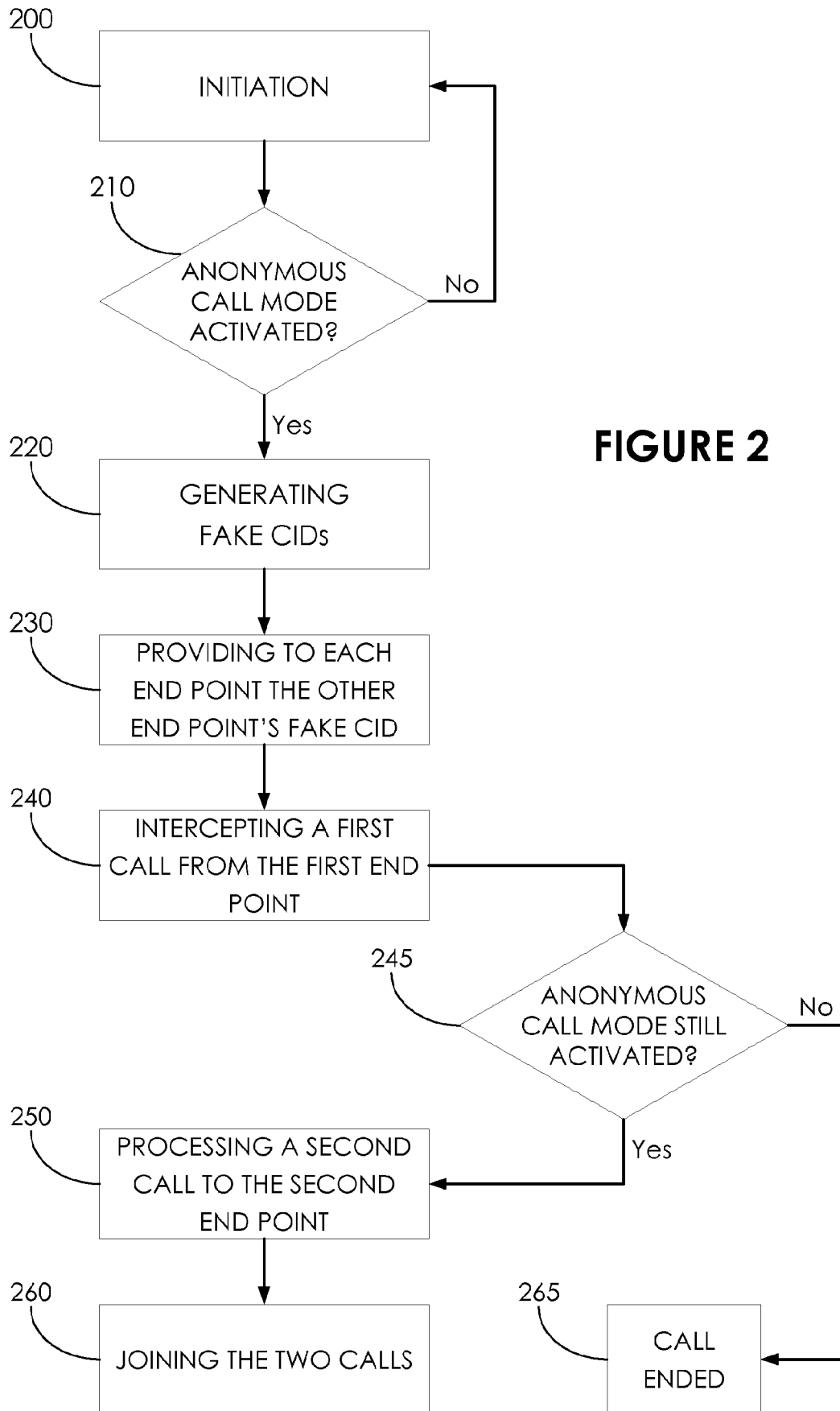


FIGURE 1

2/4

**FIGURE 2**

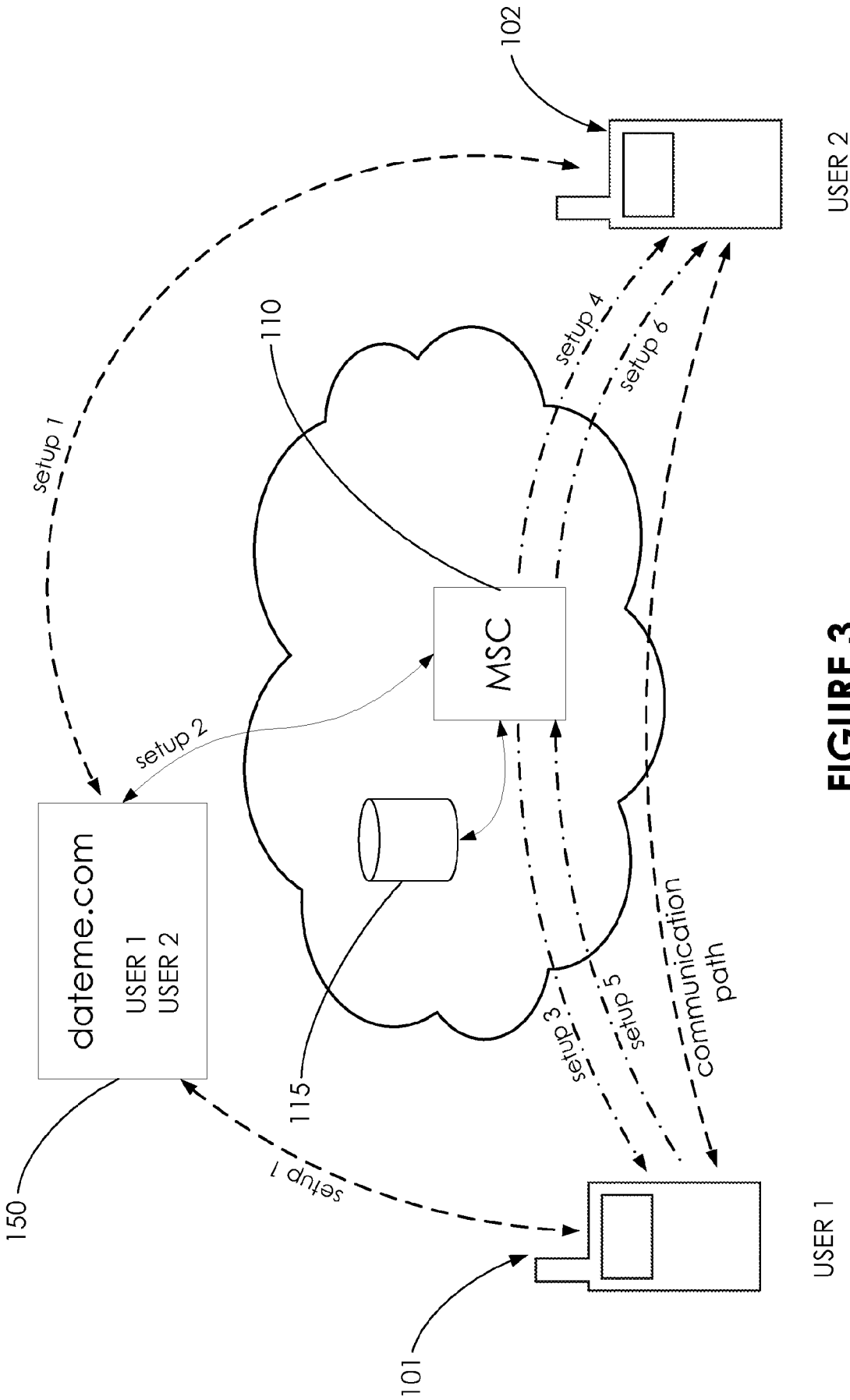
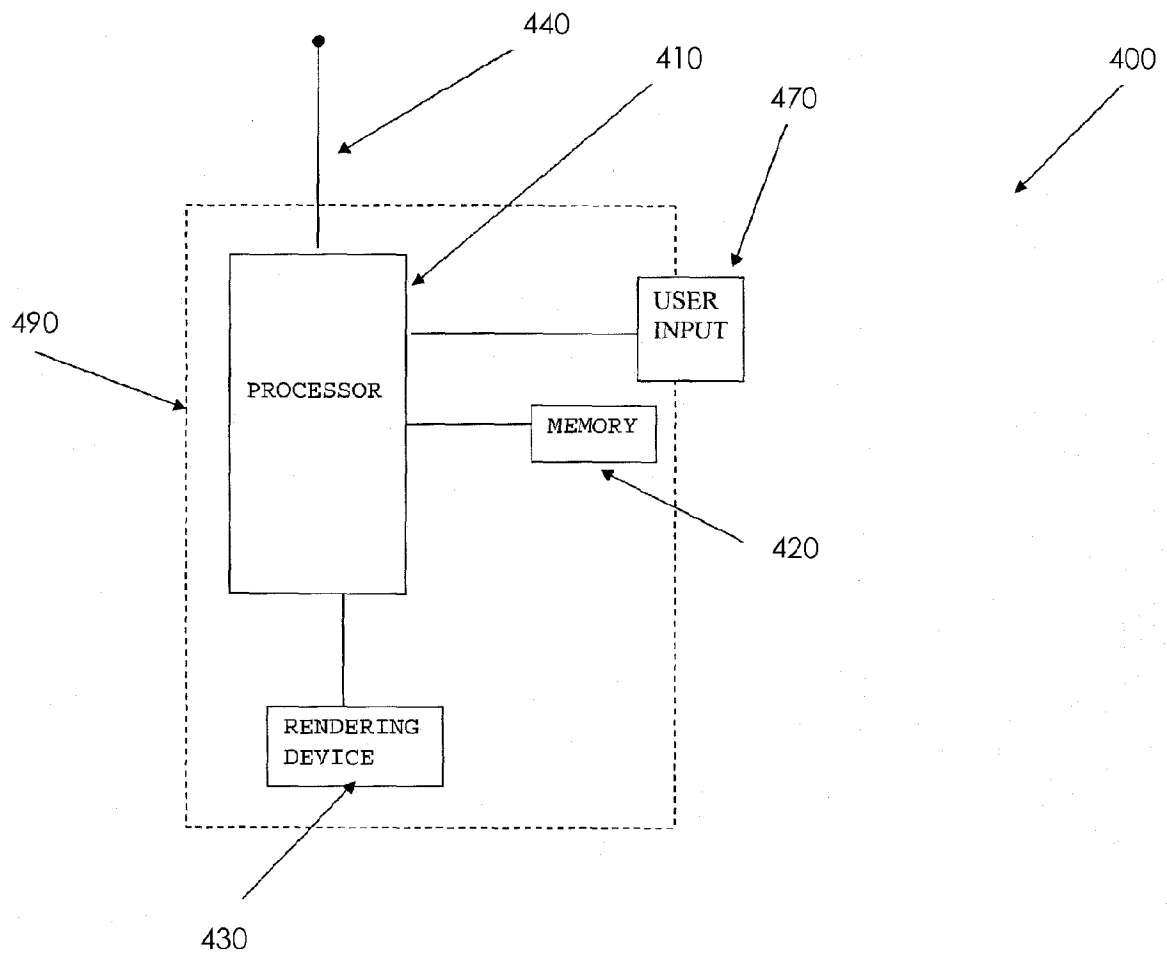


FIGURE 3

**FIGURE 4**

INTERNATIONAL SEARCH REPORT

International application No
PCT/IB2009/056040

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04M3/42 H04L29/06
ADD.

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04M H04L

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

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

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2006/177029 A1 (DOTAN ERAN [IL] ET AL) 10 August 2006 (2006-08-10) paragraphs [0008], [0010] paragraph [0035] - paragraph [0043] paragraph [0059] - paragraph [0070] -----	1-14
X	US 2007/105531 A1 (SCHROEDER B S JR [US]) 10 May 2007 (2007-05-10) paragraph [0003] - paragraph [0011] paragraphs [0013], [0015] paragraph [0025] - paragraph [0077] -----	1-14
X	DE 101 36 085 A1 (SCHUSTER WOLFGANG [DE]) 13 February 2003 (2003-02-13) the whole document -----	1-14



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search

4 May 2010

Date of mailing of the international search report

12/05/2010

Name and mailing address of the ISA/

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

Authorized officer

Nash, Michael

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/IB2009/056040

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2006177029 A1	10-08-2006	WO 2006085303 A2	17-08-2006
US 2007105531 A1	10-05-2007	EP 1955530 A2	13-08-2008
		WO 2007053768 A2	10-05-2007
DE 10136085 A1	13-02-2003	NONE	