SYSTEM AND METHOD FOR DISPLAYING AN IDENTIFIER OF A SOURCE ON A RECIPIENT DEVICE

FIELD OF THE INVENTION

The present invention relates to a system and method of displaying an identifier of a source on a recipient device. The invention is particularly suited but is not exclusive to the display of a number of a caller on a recipient mobile phone.

BACKGROUND ART

The following discussion of the background to the invention is intended to facilitate an understanding of the present invention only. It should be appreciated that the discussion is not an acknowledgement or admission that any of the material referred to was published, known or is part of the common general knowledge of the person skilled in the art in any jurisdiction as of the priority date of the invention.

Public switched telephone networks (PSTN) numbers are typically assigned to the physical line and that number remains unchanged. Similarly, mobile phone numbers are assigned to the subscriber identity module (SIM).

One known way of assigning PSTN numbers and mobile phone numbers is based on the E.164 ITU-T recommendation which defines the format of telephone numbers and the international public telecommunication numbering plan used in PSTN and other data networks.

There is, however, a perceived need for a service that could provide dynamic and temporary allocation of phone numbers which will allow the creation of different identifiers for the caller to different recipients.

Although users of mobile phones may utilize caller ID and call lists, these features are merely informational and require the user to actively update and associate callers to a contact, such as by saving each caller's number in a contact list or electronic phonebook. Under the caller ID system, there is no

active links or automatic association between the caller and the person being called.

A known method of associating between a caller and the person being called is to create a ‘social connection’ or social link**.** However such systems are limited and restricted to callers and persons receiving the calls within the same network due to trust/security issues.

Further, while it is possible to switch off the caller ID option or mask a phone number, many current phones and phone systems do not support number masking due to possible abuse by end users.

The present invention seeks to alleviate or reduce the above mentioned drawbacks.

SUMMARY OF THE INVENTION

In accordance with a first aspect of the present invention there is provided a system for displaying an identifier of a source on a recipient device in communication with the source, the system comprising an association database defining a list of sources associated with the recipient device; and a processing manager arranged to process communications from the source to the recipient device and arranged to access the association database to determine if the source is associated with the recipient device and, if so, to display an established identifier of the source, otherwise to determine the privacy settings of the source and display a further identifier on the recipient device in accordance with the determined privacy settings.

Preferably the processing manager is integrated with the source or recipient device.

Preferably the recipient device is a mobile device configured to allow barring of phone calls. Advantageously the recipient device comprises a system log for determining whether the source is watchlisted or blacklisted.

Preferably the system further comprises a Location Based Service (LBS) to determine the location of the calling party. Advantageously the LBS is further configured to determine the number of registered users of the LBS nearest to the location of the calling party.

Preferably the processing manager is adapted to be in data communication with an external gateway for routing calls if it is determined that the source and recipient devices are not within the same communication network.

Preferably the processing manager is arranged to access a network address book to determine if the source is associated with the recipient device.

In accordance with a second aspect of the present invention there is provided a method for displaying an identifier of a source on a recipient device, the recipient device adapted to receive calls from the source, comprising the following steps: a. determining whether a link exists between the source and recipient device and display an existing identifier of the source on the recipient device if the link exist; and b. checking the privacy settings of the source to determine the identifier to be displayed on the recipient device where there is no existing link;

Preferably, the step of checking the privacy settings of the source includes determining if the source is unlisted or has its caller ID masked.

Preferably, upon determining that the source and recipient device are within the same communication network, the method further includes the step of checking if the source is blacklisted or watchlisted within the communication network.

Advantageously, if the source is not blacklisted and watchlisted, the privacy settings of the recipient device is checked to determine if the identifier of the source may be displayed on the recipient device. The method may further

include a step of establishing the route between the source and recipient device, wherein the route establishment step includes checking the identifier attribute of the source to determine how the identifier is derived. In such an instance, the step of checking the identifier attribute may further include determining if the identifier was forwarded, downloaded or manually inputted to the source.

Preferably, if the source is watchlisted within the communication network, an alert is triggered and the call is terminated.

Preferably, if the source is blacklisted within the communication network, the call is terminated.

If it is determined that the source and recipient device are not within the same communication network, calls from the source are routed.

Preferably, the step of determining whether a link exists between the source and recipient device includes accessing a network address book.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will now be described, by way of illustrative example only, with reference to the accompanying drawings, of which:

Fig. 1 is a system block diagram in accordance with an embodiment of the invention.

Fig. 2 is a flow diagram illustrating the processing of a phone call to a recipient in accordance with an embodiment of the present invention.

Fig. 3 is a flow diagram illustrating the routing of the phone call to a recipient in accordance with an embodiment of the present invention.

Fig. 4 is a flow diagram illustrating the initiation of a phone call from a caller to an intended recipient, the caller within the same network employing an embodiment of the present invention

Fig. 5 is a flow diagram illustrating the initiation of a phone call from a caller to an intended recipient in a different network, and

Fig. 6 is a flow diagram illustrating how an embodiment of the present invention may be used as an 'In case of Emergency' tool in conjunction with a Location based service.

DESCRIPTION OF EMBODIMENTS OF THE INVENTION

In accordance with an embodiment of the invention, illustrated in Figure 1, there is a system 10 for displaying an identifier of a source 12 on a recipient device 14. For the purpose of illustration, the source 12 and recipient 14 are mobile devices. The identifier of the source 12 is typically the mobile phone number allocated to the source 12.

The system 10 further comprises a processing manager 16 adapted to process calls from the source 12 by which a call is made to recipient 14. The processing manager 16 may be integrated within the source 12 and recipient 14, for example the processing manager 16 may include one or both of the mobile devices that are being used.

The system further comprises an association database 20 and a number masking database 22. The association database 20 is typically a number look-up and management database 20. The number look-up and management database 20 further comprises a number resolution database 24. The number resolution database 24 resolves any dialled number from the source 12 of the call to determine whether it is within the social network of the recipient 14. The number masking database 22 is connected to an external gateway 26 for routing external calls. Any phone number routing out of the system 10 is masked to make it compatible with international standards such as the E.164 ITU-T recommendation.

The association database 20 further maintains a network address book 27 of all subscribers within the system 10. The network address book 27 is linked to the number masking database 22 and the number resolution database 24. The network address book 27 is configured to further establish/update any

social links between subscribers within the system 10. This may be achieved by performing regular synchronization between the address book 27 and the subscriber's mobile device local phonebook.

When a call is made, a number is dynamically generated from a number range blocked out for the purpose. The dynamic generation of the number may be random within the limits of the number range. The generated number is added to the number look-up and management database 20. The management database 20 provides a mapping of the original phone number and the dynamically generated (i.e. masked) phone number. The number resolution database 24 is looked up to determine the originator of the call. Such an arrangement ensures that the original phone number from the source 12 of the call is masked and only the service operator is aware of the mapping. The arrangement further allows the recipient device 14 to bar any parties from calling him/her at the point of look-up.

The processing server 16 may also comprise a client interface 28 which supports mapping, un-mapping and assigning or managing the system.

The caller mobile device/source 12 may be any mobile device as known in the art.

The recipient mobile device 14 is adapted to allow the user the option of blocking a caller via a blacklist, with the facility for setting up alerts and flags for certain callers, i.e. watchlisting; or the option to sever social network connections. The recipient device 14 is further configured to allow barring of phone calls.

The embodiment is next described in the context of processing a phone call initiated by the source 12 of the call (from herein on referred to as the caller 12) to a recipient 14 (step 200). The processor 16, via the number resolution database 24, checks whether the dialled number is in the social network of the caller 12 (step 202). The check involves comparing the contact list or electronic phone book of both the caller 12 and recipient 14 on the network address book 27 to verify that the caller 12 and recipient 14 are socially

connected (step 204). Further verification includes determining whether the caller 12 and recipient 14 had prior communication.

If it is determined that the caller 12 and recipient 14 are socially connected based on step 204, the call is established and connected (step 206). On the other hand, if it is determined that the caller 12 and recipient 14 are not socially connected, it could mean that the caller 12 and recipient 14 had no prior communication or the dialled number has just been added, either by a directory download, a business card forward, or manual input. In such a case, the privacy setting of the caller 12 is checked (step 208). The checking involves determining if the calling party 12 is unlisted (step 210) or if the privacy setting prevents the caller's number from being revealed. If the caller's number is unlisted, then the number is masked with system assigned information which has at least the indication that the number is masked (step 212). The masked number then becomes the caller's 12 number which will then be displayed on the recipient device 14.

On the other hand, if the privacy settings of the calling party do not require anonymity, the preferred caller's identity that has been set for the caller 12 is associated with the call (step 214). The preferred identity would then be displayed on the recipient device 14.

Following, step 212 or step 214, the system 10 next checks if the caller 12 and recipient 14 are in the same mobile communication network (step 216). If they are not in the same network, the call is required to be routed to an external network. Such routing networks may be independent of the present invention. In such a situation, the call is routed (step 222) with the caller's identification (step 218) associated with the call. The routing involves passing through a gateway which involves translation of the internal signalling protocol of the system 10 to that which is compatible with the PSTN, ISDN of the external communication network.

If, however, it is established that the caller 12 and recipient 14 are in the same network, the system logs are checked (step 220). The system logs could reside in the recipient device or in an external server. The system logs are checked for the following:

a. whether the caller 12 is in the watch list (step 224), if determined so, an alert or message may be triggered to initiate a call trace or similar options to notify the party which requested for the call trace (step 226). Thereafter, the call is terminated (step 228).

b. if the caller 12 is determined not to be in the watch list, the system logs are checked if the caller 12 is in the black list (step 230). If so, the caller 12 is blocked and the call is terminated (step 228). However, if the caller 12 is determined not to be a blacklisted contact, the privacy settings of the recipient device 14 are checked (step 232) to see if anonymous calls or calls from caller 12 outside the recipient's social network is allowed (step 234). If the privacy settings does not allow anonymous calls or calls from outside the recipient's social network, the call is terminated (step 228). On the other hand, if the recipient allows the anonymous call or calls from outside the recipient's social network, a route is established (step 236) and call is connected (step 206).

The routing of the call (step 236) is a process which comprises the following steps:

The process begins with a check of the attributes of the dialled number (step 302), that is whether the dialled number is forwarded from a friend (step 304) via for example the sharing of an electronic business card, downloaded (step 306), for example from a central directory service, or manual entry (step 308). If from step 304 it is determined by the system 10 that the dialled number was forwarded from a friend, the system 10 transmits the shared information from the friend's phonebook entry (step 310) in the network address book 27. Thereafter, the social network between the parties is created (step 312).

If from step 306 the dialled number is deemed to be downloaded, the default caller identification information entry in the central directory service is used (step 314). Thereafter, the social network between the parties is created (step 312).

If from step 308 it is determined that the dialled number is manually inputted, the system 10 checks for a common node, i.e. an identified common friend in the network address book 27. The system then verifies if the number dialled is unique among the common nodes (step 318), and if it is, that number and the associated call information is used (step 320). On the other hand, if the dialled number is not unique, i.e. there are duplications of numbers, the system uses the default central directory call information to establish the social network connection (step 314).

If from step 308 it is determined that the dialled number if not manually inputted, the system logically assumes that the data had been resident in the recipient device 14 and thus is a result of a previous social network connection with the recipient 14. This indicates that the recipient 14 had severed the social network connection with the caller 12 at some time prior to the call (322). This may be due to one or more of the following reasons:- blacklisting, watchlisting, social withdrawal, or based on mere exigency such as a need to free up space in the electronic phone address book, or even something as mundane as the recipient seeing no perceived need to keep the social connection with the caller, etc.

Based on the above reasons, the system 10 proceeds to check if the caller 12 has been blacklisted (step 324) or watchlisted (step 328). If it is determined to be blacklisted or watchlisted, the call is terminated (step 326) or an alert is triggered (step 330) thereafter terminating the call.

Where the caller 12 is within the same mobile communication network, the system 10 performs the following, as illustrated in Fig. 4, to establish or route the call.

When such a call is made (step 402), the social network associated with the intended recipient 14 device is checked whether the called number is a node in the social network of the intended recipient 14 (step 404). By default, the call is routed to the identified node in the social network. If the intended recipient 14 number is not in the social network of the calling party, the phone network is then checked whether the intended recipient 14 is within the same network (step 406). If the intended recipient 14 is within the same network, the phone number of the calling party 12 is masked (step 408) as specified by the calling party 12 and the call is connected (step 410).

If the intended recipient 14 is determined to be in a different network, the system 10 checks if the recipient 14 is an unlisted number (step 412), and if so, sends the network ID information (step 416) and routes the call (step 418). If the recipient 14 is not an unlisted number, the caller ID information is sent in-lieu of the network ID information (step 420) and the call is routed (step 418).

It is to be appreciated that even if the caller 12 specifies a mask for his or her number, if he or she has previously connected with the intended recipient 14, the specified mask will be overridden by the information from the previously established connection. As an example, if caller 12 has prior contact (i.e. established a social connection) with recipient 14 where caller 12 used the number n; and caller 12 subsequently severed his or her connection with recipient 14 and then caller 12 tries to re-connect with recipient 14 using another different specified number x, this number x will be overridden by n and recipient 14 will still see caller 12 number as n instead of the new number x. It is to be appreciated that the caller 12 number will be different to another recipient C in social group AC as their social grouping is different.

In the case where the originating caller 12 is from an external network and the recipient device 14 is within the network, the system 10 performs the

following, as illustrated in Fig. 4, to establish, terminate or perform any optional action pertaining to the call.

Upon initiating the call (step 502), the privacy setting of the caller 12 is checked (step 504). An example of the way of checking the privacy setting of the caller 12 involves checking if the caller 12 is publicly listed (step 506). If the caller 12 discloses caller identification or is publicly listed, the call is connected (step 522). However, if the caller 12 withholds caller identification, such that it is not publicly listed, the system logs are checked (step 508) to determine if the caller 12 is on the blacklist (step 510). If the number of caller 12 is blacklisted, the call is terminated (step 512) and the system 10 has the option to perform further actions such as initiating a call trace or sending out an alert (step 514) to the nominated emergency contacts (i.e. social contacts). Upon determining that the number of caller 12 is not blacklisted, the privacy setting of the recipient is checked (step 516). The called party 14 is checked and if anonymous calls are accepted (step 518), the call is logged by the system (step 520) and subsequently connected (step 522). On the other hand, if the called party does not accept anonymous calls, the call is terminated immediately (step 512). Again, the system has to option to perform certain further actions, such as initiating a call trace or sending out an alert (step 514).

When a call is logged in step 520, the system pairs the calling number with the called number. This pairing becomes a virtual social network connection such that in a subsequent call from the same caller and in the absence of derogatory information found upon checking of the logs, i.e. being in the blacklist, the call is already connected to the called party. The intended recipient 14, which is inside the network using this invention, has the option, however, at any time, to put the calling party on a blacklist and disconnect, or sever the social network connection.

The embodiment as described above may also be used in conjunction with a Location Based Service (LBS) in the case of an emergency (ICE) tool. In an illustrative example as depicted in Fig. 6, it is assumed that certain users signed up to volunteer with an Emergency HELP service. The business rules for this can be defined by the organization which oversees the HELPline.

The HELPline process is started by an end user in distress. This end user which becomes the caller or calling party 12, calls the designated HELPline number, which in this example is 4357 corresponding to HELP in a regular phone keypad (step 602). It is to be appreciated that if it were a 911 call, the call would be routed to the 911 call center. The system then invokes the LBS and determines the location of the calling party 12 (step 604).

The processing server 16 proceeds to check its volunteer database (known as a HELP group) and acquires their locations (step 606). In case of a closed HELP group, i.e. the user defines which numbers are to be associated with a HELP call, the system and LBS checks the location of the volunteer pool. The system identifies the volunteer nearest in location to the calling party 12 (step 608). The calling party 12 may be in the company of others who are part of the volunteer pool. If a call for help is routed to them, it would defeat the purpose of the distress call as the caller 12 is requesting for help. Hence, the system shall see to it that the relative location of the calling party and the target volunteer are not identical to such degree of error associated with the LBS.

Upon determining the nearest volunteer, the system 10 routes the call to the nearest volunteer (step 610). If a volunteer receives the call (step 612), then a conversation is established (step 614).

On the other hand, a volunteer may not receive a call, either because the volunteer failed to notice the call, for example a missed call (step 615), or because the volunteer is not interested to respond to the distress call. If the volunteer inadvertently missed the call, a reattempt to call is made by the

system 10 (step 616). On the other hand, if the call is intentionally rejected, the phone number of the rejecting party is removed from the pool of volunteers (step 618). The system then determines who among the others in the pool is nearest the distressed party and tries to route the call to that volunteer, i.e. a retry with excluded party (step 616). The steps 610 to 618 may be repeated as discussed.

In addition, there may be a time out feature wherein if the calls are being routed to the same numbers and calls remain unanswered, the call by default is routed to the central HELPline which could be a facility similar to 911 or to such other implementation as may be adopted by the locality, the mobile network operator, or such other concerned party.

The volunteer database may be user-defined, i.e. defined by the user who is in distress. It could also be system generated, based on an existing directory service, which is a centralized database for all subscribers as well as an online white/yellow page service and a social network roster. It could also be social, based on the entries in the caller's contact list or phone book, or based on the frequency or duration of interaction between the caller and those in his or her contact list, phone book, call or message log file.

The present invention provides a number masking feature that extends the mere hiding or spoofing or a source identifier. Through the processing of the calls as described above, the number masking feature of the invention is a conscious effort to make phone numbers relevant, or irrelevant, to parties using a secure infrastructure that prevents fraud.

Compared to prior art standards such as RFC 3325, which enables a network of trusted servers to assert the identity of authenticated users, where users have to be within the network of trust, the present invention contemplates a situation beyond the definition of RFC 3325, where one party may be outside the trusted network.

An advantage associated with the present invention is that the MIN is never exposed providing controllable privacy due to checkings performed on the privacy settings of both the source and recipient devices.

The caller and recipient device could be mobile phones or any electronic gadget or device with network connectivity.
The caller and recipient device could be in wireless communication via mobile network, i.e. 3G, EDGE, GSM, radio etc.; through wireless networks, i.e. WiFi, WiMax, IrDa, Bluetooth, NFC, or through wired connectivity.

In additional to the above, the fundamental functionality of fun numbers can also be configured through other interfaces like an IVR and web site.
In light of the social network address book 27 which is maintained within the system's network, number spoofing is not possible from the mobile caller or recipient as only the operator has knowledge of the identification mapping at all times.

It is to be understood that the above embodiments have been provided only by way of exemplification of this invention, such as those detailed below, and that further modifications and improvements thereto, as would be apparent to persons skilled in the relevant art, are deemed to fall within the broad scope and ambit of the present invention described. Furthermore although individual embodiments of the invention may have been described it is intended that the invention also covers combinations of the embodiments discussed:

Claims

1. A system for displaying an identifier of a source on a recipient device in communication with the source, the system comprising

an association database defining a list of sources associated with the recipient device; and

a processing manager arranged to process communications from the source to the recipient device and arranged to access the association database to determine if the source is associated with the recipient device and, if so, to display an established identifier of the source, otherwise to determine the privacy settings of the source and display a further identifier on the recipient device in accordance with the determined privacy settings.

2. A system according to claim 1 wherein the processing manager is integrated with the source or recipient device.

3. A system according to claim 1 or 2, wherein the recipient device is a mobile device configured to allow barring of phone calls.

4. A system according to claim 1, wherein the system further comprises a Location Based Service (LBS) to determine the location of the calling party.

5. A system according to claim 4, wherein the LBS is further configured to determine the number of registered users of the LBS nearest to the location of the calling party.

6. A system according to claim 3, wherein the recipient device comprises a system log for determining whether the source is watchlisted or blacklisted.

7. A system according to claim 1, wherein the processing manager is adapted to be in data communication with an external gateway for routing

calls if it is determined that the source and recipient devices are not within the same communication network.

8. A system according to claim 1, wherein the the processing manager is arranged to access a network address book to determine if the source is associated with the recipient device.

9. A method for displaying an identifier of a source on a recipient device, the recipient device adapted to receive calls from the source, comprising the following steps:

a. determining whether a link exists between the source and recipient device and display an existing identifier of the source on the recipient device if the link exist; and

b. checking the privacy settings of the source to determine the identifier to be displayed on the recipient device where there is no existing link.

10. A method of claim 9, wherein the step of checking the privacy settings of the source includes determining if the source is unlisted or has its caller ID masked.

11. A method of claim 9, wherein if it is determined that the source and recipient device are within the same communication network, the method further includes the step of checking if the source is blacklisted or watchlisted within the communication network.

12. A method of claim 11, wherein if the source is not blacklisted and watchlisted, privacy settings of the recipient device is checked to determine if the identifier of the source may be displayed on the recipient device.

13. A method of claim 11, wherein if the source is watchlisted within the communication network, an alert is triggered and the call is terminated.

14. A method of claim 11, wherein if the source is blacklisted within the communication network, the call is terminated.

15. A method of claim 12, the method including a step of establishing the route between the source and recipient device, wherein the route establishment step includes checking the identifier attribute of the source to determine how the identifier is derived.

16. A method of claim 15 wherein the step of checking the identifier attribute includes determining if the identifier was forwarded, downloaded or manually inputted to the source.

17. A method of claim 9 including the step of determining if the source and recipient device are within the same communication network, and routing calls from the source if it is determined that the source and recipient devices are not within the same communication network.

18. A method of claim 9 wherein the step of determining whether a link exists between the source and recipient device includes accessing a network address book.