

SYSTEM FOR TRACKING MOBILE EQUIPMENT AND ASSOCIATED MOBILE SUBSCRIBERS' IDENTITY

DESCRIPTION

FIELD OF INVENTION

The invention relates to methods and apparatus for recording and utilising mobile terminal usage data for enabling useful functions based on the data to be performed.

BACKGROUND OF THE INVENTION

The following references to and descriptions of prior known or described or proposed systems are not admissions of, and are not to be understood or construed as admissions of, common general knowledge in the relevant technology.

A subscriber connection is usually needed these days for communicating with terminal equipment in an established data communication network. The connection is used to identify, among other things, one or more data transmission networks, wherein communication is permissible, and detailed settings related to the subscriber connection, such as, for example, network/operator-specific data (encryption algorithms, among other things) and subscriber-specific data, such as, for example, the IMSI (International Mobile Subscriber Identity).

According to the known technology, there is currently no way of tracking the current phone number (which is a function of the subscriber connection) associated with a terminal device. While some such information might be maintained by the telecommunication provider providing the subscriber connection, it is impossible to aggregate the information from all service providers to link the mobile device to all subscriber identities that have been used in association with it. There is also no known way to find out the current phone

number associated with a mobile terminal by a party other than the telecommunication provider providing the subscriber connection.

Thus if the subscriber identity (and thus associated phone number) associated with a mobile terminal is changed, it becomes impossible to communicate with it unless the new subscriber identity/associated phone number are known.

It might be desirable to communicate with the mobile terminal irrespective of the subscriber identity currently associated with it. The state of the art currently does not allow this form of communication as communication is always dependent on the subscriber identity and if it changes and the new identity is unknown, communication becomes impossible. This invention as further described later can solve this problem by tracking changes to the subscriber identity and hence it is possible to communicate based on device identity, since by providing the device identity, the currently associated subscriber identity can be identified by this invention.

It might further be desirable to find out all historically associated subscriber identities (phone numbers) with a particular mobile terminal. According to known technology, this is further not possible since there are no techniques in the state of the art of aggregating information from different service providers to determine an audit trail especially if the service providers are themselves not involved (the information is to be determined by a third party).

Known technology relating to the SIM facility is described in the FI-104139B (Nokia Networks Oy), FI-104937 (Sonera Oyj), WO-98/53629 (Motorola, Inc), EP-1037159A2 (Nokia Mobile Phones LTD.) publications. However, these provide no mention of enabling communication with a mobile terminal in the event that the SIM itself has changed.

Besides these, there are proposed solutions for reconfiguration of the SIM facility through the data transmission network. Examples of such are presented, for example, in the EP-0 562 890 B1, U.S. Pat. No. 6,097,967, WO 00/40048 and FI-108390 publications. Such

reconfigurations may include, for example, activation of mobile station services or downloading of so-called value-added services in the terminal equipment. However, again these reconfigurations are rendered meaningless in the context of a change in the subscriber's identity.

Such measures, for example, are also known, which are taken in connection with a change of the subscriber connection in order to transfer subscriber-specific data, such as, for example, *SMS* (Short Data Message) messages and telephone memo data from the old SIM card to the new card. This step may be performed either at the terminal equipment or, for example, at the network operator's service outlet with a special configuration application. However, in both cases, the old and new subscriber identities are known.

Measures are also known to automate management of terminal dependent information by mobile operator. An example of this can be found in WO2004/004390. However, such systems provide a forward mapping between a subscriber identity and a terminal identity. It is unknown for the reverse direction; i.e a mapping between a terminal identity and a subscriber identity. While the system in WO2004/004390 benefits from being able to capture a new device identity when the subscriber changes a device, it does not address the problem of capturing a new subscriber identity in the case of the device is being used by some other subscriber and thus it does not allow communication based on device identity rather than subscriber identity.

Thus there are currently no known methods of 1) universally tracking subscriber identity (eg: phone number) linked to a particular device identity; 2) externally querying the current and historical subscriber identity(ies) associated with a device identity independent of different mobile service provider networks.

It is an object of the invention to provide a system (including both method and apparatus) to enable useful recording and tracking and retrieval of mobile terminal usage data, and preferably to enable alleviation of inadequacies of the prior art discussed above.

SUMMARY OF THE INVENTION

According to a first aspect of the present invention there is provided a method of recording mobile terminal usage data for subsequent use, the method comprising:

- providing device identity parameters identifying a particular mobile terminal;
- when the operating state of the mobile terminal is active, detecting subscriber identity parameters for a subscriber using the particular mobile terminal;
- determining whether the subscriber identity parameters for the particular mobile terminal have changed over time, and, if so,
- storing changed subscriber identity parameters in a memory together with an association of the changed subscriber identity parameters with the device identity parameters of the particular mobile terminal without losing precedent subscriber identity parameters associated with the particular mobile terminal.

The operating state of the mobile terminal being active may be defined by the existence of at least one of the following operating states:

- when the mobile terminal is first switched on after being in an inactive state,
- when the mobile terminal is first logged onto a mobile communications network,
- and
- when the mobile terminal has been actively logged onto a mobile communications network for a significant period of time (a) after first logging onto the network, or (b) after last detecting of the subscriber identity parameters while the mobile terminal is logged onto the mobile communications network.

In one possible embodiment subscriber identity parameters are stored in a memory of the particular mobile terminal including at least the last detected subscriber identity parameters prior to the performance of the step of detecting current subscriber identity parameters for the subscriber using the particular mobile terminal, and the step of determining whether the current subscriber identity parameters for the particular mobile terminal have changed is preferably carried out by processing means of the mobile terminal which is operative to compare current subscriber identity parameters with the stored last precedent subscriber

identity parameters. In this embodiment, the particular mobile terminal may be operative to generate a flagging signal when it determines that the current subscriber identity parameters have changed compared to the stored last precedent subscriber identity parameters, the flagging signal being generated on a mobile communication network so as to enable the step of storing changed subscriber identity parameters in a memory to be performed externally of the mobile terminal in response to detection of the flagging signal on the communications network.

In a second possible embodiment subscriber identity parameters are stored in a memory of a subscriber monitor external to the mobile terminal and operatively associated with the communication network, the stored subscriber identity parameters including at least the last detected subscriber identity parameters prior to the performance of the step of detecting current subscriber identity parameters for the subscriber using the particular mobile terminal, and the step of determining whether the current subscriber identity parameters for the particular mobile terminal have changed is preferably carried out by processing means of the subscriber monitor external to the mobile terminal and which is operative to compare current subscriber identity parameters with the stored last precedent subscriber identity parameters.

Preferably the step of storing the changed subscriber identity parameters in a memory includes storing such changed subscriber identity parameters in a memory external to the particular mobile terminal by means of a recording sub-system which is operatively associated with the mobile communications network and which extracts device identity parameters and subscriber identity parameters from data communications of the particular mobile terminal over the mobile communications network.

To utilise the mobile terminal usage data recorded, the method may comprise the further steps of:

interrogating the memory of stored subscriber identity parameters for those subscriber identity parameters which have an association in the memory with a particular

target mobile terminal having terminal identifying parameters which are input in the interrogating step, and

retrieving at least one of current and any precedent subscriber identity parameters having an association in the memory with the target mobile terminal.

In one specific utilisation of the usage data where the target mobile terminal comprises one which has been previously been lost or stolen, the method may comprise a further step of communicating with the target mobile terminal in response to the interrogation of the memory and retrieval of the latest stored subscriber identity parameters even if changed subsequent to the loss or theft of the mobile terminal.

In another specific utilisation of the usage data where the target mobile device is one owned by an enterprise, the method may comprise the further step of tracking and logging at least the identities of users of the mobile device for furthering the objectives of the enterprise.

In yet another specific utilisation of the usage of the usage data, the method may comprise the further step of transmitting messages or data to the target mobile device in response to the steps of interrogating the memory and retrieving subscriber identity parameters, the transmission being based on the identity of the target mobile device and independent of the current or latest subscriber identity parameters. In this utilisation method, the data transmission to the target mobile device may include transmission of data processing instructions whereby, in response, the mobile device performs data processing operations selected from data deletion, data manipulation, data backup, and data transmission.

According to a second aspect of the invention there is provided an apparatus for recording mobile terminal usage data for subsequent use, the apparatus including:

means for providing device identity parameters identifying a particular mobile terminal;

means, operative when the operating state of the mobile terminal is active, to detect subscriber identity parameters for a subscriber using the particular mobile terminal;

means for determining whether the subscriber identity parameters for the particular mobile terminal have changed over time, and, if so,

means for storing changed subscriber identity parameters in a memory together with an association of the changed subscriber identity parameters with the device identity parameters of the particular mobile terminal without losing precedent subscriber identity parameters associated with the particular mobile terminal.

The apparatus for utilising the mobile terminal usage data may further comprise:

means for interrogating the memory of stored subscriber identity parameters for those subscriber identity parameters which have an association in the memory with a particular target mobile terminal having terminal identifying parameters which are input to the interrogating means, and

means for retrieving at least one of current and any precedent subscriber identity parameters having an association in the memory with the target mobile terminal.

In use of preferred embodiments of the invention, there will be maintenance of links between physical mobile terminals and their current and historical subscriber identity parameters including but not limited to phone numbers, network identities, location identities etc. The current and historical data are communicated in the event of any change to a remote observing server (*recording sub-system*).

One preferred field of use of the invention has the purpose of *enabling* communication with mobile devices based on their device identities rather than their associated subscriber identity. By tracking subscriber identity associated with a device identity, and making elements of the subscriber identity (such as phone number) available to third parties, communication with the device is enabled regardless of current subscriber identity since the associated phone number of the device in question is made available by the invention.

Many scenarios where such communication is desirable are thus enabled by this invention. Such scenarios include (but are not limited to) the following:

- Remotely communicating with a device when it is lost/stolen even if the associated subscriber identity has been changed by the person who found/stole it.
- Remotely monitoring mobile phone inventory in an enterprise and tracking the associated phone numbers of people using enterprise owned mobile assets.
- Messaging or communication systems based on device identity rather than subscriber identity/phone number.
- Device based (as opposed to subscriber based) value added services including but not limited to VoIP roaming/international roaming etc.
- Communicating with a device based on device identity to remotely update data, to delete data or to backup data.

Another intention of a preferred embodiment of the present invention is to accomplish at least one software product that can be directly loaded and deployed in at least one embodiment of an *observing sub-system* and at least one embodiment of a *recording sub-system*. The software product will enable automatic tracking of subscriber identities associated with registered device identities.

The need for manually tracking or finding out selected parameters (such as but not limited to phone number) pertaining to a current subscriber identity or historical subscriber identities associated with a device identity can thus be eliminated with this product or products.

A further advantage of the present preferred system is that historical data pertaining to subscriber identities associated with a device can be made in a database. This database can then be queried to derive information including but not limited to 1) Previous subscriber identities associated with the device in question. 2) Current status of a device (in terms of selected subscriber identity parameters) .

It should be pointed out that when the terms “comprises/comprising” are used in this description, it should be taken to mean the specified properties, steps or components are included, but it does not exclude the presence of one or more other properties, parts, steps, components or groups of these.

The embodiments of the invention shall now be described with reference to the attached drawings where:

BRIEF DESCRIPTION OF THE DRAWINGS

- Figure 1 shows a block diagram of some parts in a first embodiment of the invention
- Figure 2 shows a block diagram of a first embodiment of an *observing sub-system*.
- Figure 3 shows a block diagram of a second embodiment of an *observing sub-system*.
- Figure 4 shows a block diagram of an embodiment of a *recording sub-system*.
- Figure 5 shows a block diagram of a second embodiment of the invention.
- Figure 6 shows a flow diagram of a first embodiment for a method for tracking association of mobile equipment with mobile subscribers' identity; according to the present invention
- Figure 7 shows a flow diagram of a second embodiment of the method; according to the present invention
- Figure 8 shows a flow diagram of a third embodiment of the method; according to the present invention
- Figure 9 shows a flow diagram of a fourth embodiment of the method; according to the present invention
- Figure 10 shows a schematic diagram of some software products; according to the present invention

DETAILED DESCRIPTION OF EMBODIMENTS

A list of abbreviations that are used in this description is given in order to facilitate an understanding of the present invention

ABBREVIATIONS

API	Application Programming Interface
CL	Communication Link
CMA	Change Monitoring Agent
CN	Cellular Network
CPU	Central Processing Unit
CRA	Change Recording Agent
EPROM	Erasable Programmable Read Only Memory
EEPROM	Electrically Erasable Programmable Read Only Memory
GPRS	General Packet Radio Service
HTTP	Hypertext Transport Protocol
IQA	Identity Querying Agent
IS	Identity Store
MT	Mobile Terminal
MTOS	Mobile Terminal Operating System
MTPE	Mobile Terminal Programming Environment
OS	Operating System
SIH	Subscriber Identity History
SMSC	Short Message Service Centre
TP	Transport Package

Figure 1 shows a block diagram of some of the components in an embodiment of the invention. The *observing sub-system* in Figure 1 is denoted by reference number 9. It consists of a mobile terminal 1, an identity Change Monitoring Agent 2 and an Identity Store 3. The CMA 2 functions as means, operative when the operating state of the mobile

terminal is active, to detect subscriber identity parameters for a subscriber using the particular mobile terminal; and as means for determining whether the subscriber identity parameters for the particular mobile terminal have changed over time.

The *recording sub-system* 10 consists of an identity Change Recording Agent 6, a Subscriber Identities History persistent store 7 and an Identity Querying Agent 8. The CRA 6 functions as means for storing changed subscriber identity parameters in the memory or store 7 together with an association of the changed subscriber identity parameters with the device identity parameters of the particular mobile terminal without losing precedent subscriber identity parameters associated with the particular mobile terminal. The IQA 8 functions as means for interrogating the store 7 having stored subscriber identity parameters for those subscriber identity parameters which have an association in the memory 7 with a particular target mobile terminal 1 having terminal identifying parameters which are input to the interrogating means, and as means for retrieving at least one of current and any precedent subscriber identity parameters having an association in the memory 7 with the target mobile terminal 1.

The observing sub-system and the recording sub-system communicate via the Cellular Network 5 using one or more Transport Packages 4. The embodiment of the Transport Package 4 is dependent on the communication protocol used by the embodiment of the invention. As an example, if an embodiment of the invention uses HTTP over the GPRS bearer provided by the Cellular Network 5, the Transport Package 4 would be an HTTP packet. Similarly, if the communication protocol used by another embodiment of the invention was the SMS bearer, the Transport Package 4 would be according to the GSM PDU specification.

Figure 2 shows a block diagram of a first embodiment of an *observing sub-system* of the invention. In this embodiment the *observing sub-system* is implemented as a software/hardware or combination of both software and hardware addition to the mobile terminal. Thus the component of a Mobile Terminal OS 4 is added to the schematic in addition to the components of a Mobile Terminal 1, an identity Change Monitoring Agent 2

and a Identity Store 3. In general, in this embodiment, subscriber identity parameters are stored in a memory 3 of the particular mobile terminal 1 including at least the last detected subscriber identity parameters prior to the detection of current subscriber identity parameters for the subscriber using the particular mobile terminal, and the determination whether the current subscriber identity parameters for the particular mobile terminal 1 have changed is carried out by processing means of the mobile terminal OS 4 which is operative to compare current subscriber identity parameters with the stored last precedent subscriber identity parameters. In this embodiment the MTOS 4 may be operative to generate a flagging signal when it determines that the current subscriber identity parameters have changed compared to the stored last precedent subscriber identity parameters, the flagging signal being generated and transmitted in a transport package 4 on a mobile communication network 5 so as to enable the storage of changed subscriber identity parameters in memory 7 to be performed externally of the mobile terminal 1 in response to detection of the flagging signal on the communications network.

It is worthwhile to mention that the Mobile Terminal OS could be embodied by a variety of Mobile Operating Systems including but not limited to Symbian OS, Windows Mobile, Linux and also proprietary OS' such as Nokia OS, and also other OS' that might be available at a later date.

It is also worthwhile to mention that the CMA could be embodied by either software or hardware implementations or a combination thereof.

In the case of it being a software implementation, the implementation could be further embodied by software written in programming languages including but not limited to C++, Symbian C++, MFC C++, C#, VB, VB.NET or any other programming language in the known state of art or, as of the present day, not invented or not yet in use. The only prerequisite of such a language would be that the Mobile Operating System and the Mobile Terminal Hardware provide support for software development in such a programming language and it is possible in such a programming language to at least:

- 1) programmatically query the device identity and subscriber identity parameters of a Mobile Terminal
- 2) programmatically initiate communication over a wireless network using any known or future available communication protocol in the art
- 3) programmatically initiate storage/retrieval of identity information to an Identity Store which might be embodied by a form of storage media including but not limited to files, databases, flash memory, EEPROM, EPROM etc.
- 4) programmatically compare differences in at least two instances of identity information.

In the case of it being a hardware implementation, the implementation could be further embodied by hardware involving but not limited to any CPU, Microprocessor, Architecture, Instruction Set, Memory Components, Circuits, Interfaces, Interrupts etc provided that the aforementioned hardware is compatible with the Mobile Terminal Hardware and Operating System and (in conjunction with the aforementioned Mobile Terminal Hardware and MTOS) is able to at least:

- 1) query the device identity and subscriber identity parameters of the Mobile Terminal
- 2) initiate communication over a wireless network using any known or future available communication protocol in the art
- 3) initiate storage/retrieval of identity information to an Identity Store 3 which might be embodied by a form of storage media including but not limited to files, databases, flash memory, EEPROM, EPROM etc.
- 4) compare differences in at least two instances of identity information.

In the case of it being an implementation involving both software and hardware, the embodiments discussed in the previous two paragraphs would apply provided the combination of this hardware and software is able to at least:

- 1) query the device identity and subscriber identity parameters of a Mobile Terminal
- 2) initiate communication over a wireless network using any known or future available communication protocol in the art

- 3) initiate storage/retrieval of identity information to an Identity Store which might be embodied by a form of storage media including but not limited to files, databases, flash memory, EEPROM, EPROM etc.
- 4) compare differences in at least two instances of identity information.

Figure 3 shows a block diagram of a second embodiment of an *observing sub-system* or subscriber monitor. In this embodiment the *observing sub-system* is implemented as an addition/enhancement to a Cellular Network. Thus Figure 3 introduces an addition element of a Probe 4 and a CL 9 in addition to the already discussed elements of Figure 2.

In general terms, in this embodiment, subscriber identity parameters are stored in a memory 3 of a subscriber monitor external to the mobile terminal 1 and operatively associated with the communication network 5, the stored subscriber identity parameters including at least the last detected subscriber identity parameters prior to the detection of current subscriber identity parameters for the subscriber using the particular mobile terminal. The determination whether the current subscriber identity parameters for the particular mobile terminal have changed is carried out by processing means of the CMA 2 which is operative to compare current subscriber identity parameters with the stored last precedent subscriber identity parameters.

The Probe 4 could be embodied by any combination of software or hardware provided that it is able to interface with the CN 5 to derive information from signaling which allows mobile subscribers to be tracked via any of their identities. There are many embodiments of readily available probes available on the market today.

In some embodiments of an observing sub-system, such an aforementioned Probe might not even be required provided a CMA 2 is directly able to interface with a CN 5 and perform the aforementioned functions of a Probe 4.

A CL 9 shown in the figure is further linked to a CN 5, however, this is not necessary in all embodiments. If a CMA 2 uses a mode of communication that is not dependent on a CN 5,

this link would not be required. It is required in those cases when a CMA 2 uses a CN 5 dependent mode of communication such as but not limited to SMS etc. In such an embodiment, a CL 9 would link to an appropriate part of a CN 5 such as a SMSC.

In this embodiment of the invention, the CMA 2 is embodied by any combination of software and hardware that, with or without interfacing with a Probe 4, is able to

- 1) query the device identity and subscriber identity parameters of a Mobile Terminal
- 2) initiate communication over a wireless or wired network using any known or future communication protocol in the art
- 3) initiate storage/retrieval of identity information to an Identity Store which might be embodied by a form of storage media including but not limited to files, databases, flash memory, EEPROM, EPROM etc.
- 4) compare differences in at least two instances of identity information.

Figure 4 shows a block diagram of an embodiment of a *recording sub-system*. In general terms, in this embodiment, the storage of the changed subscriber identity parameters in memory 7 which is external to the particular mobile terminal 1 is performed by means of a recording sub-system or CRA 6 which is operatively associated with the mobile communications network 5 and which extracts device identity parameters and subscriber identity parameters from data communications of the particular mobile terminal 1 over the mobile communications network 5. Components 5 and 9 of this embodiment need not be discussed here as they have been previously discussed in the context of Figure 3.

The CRA 6 may be embodied by any combination of hardware and/or software that is capable of

- 1) Interfacing with a CL 9
- 2) Initiating data storage and/or retrieval requests to/from a Subscriber Identity History memory store which might be embodied by a form of storage media including but not limited to files, databases, flash memory, EEPROM, EPROM etc.
- 3) Receiving and interpreting *transport packages* determined by the interface in 1)

An IQA 8 is operative to interrogate the memory 7 of stored subscriber identity parameters for those subscriber identity parameters which have an association in the memory with a particular target mobile terminal having terminal identifying parameters which are input to the IQA 8 and is operative to retrieve the current and precedent subscriber identity parameters having an association in the memory with the target mobile terminal. The IQA 8 may be embodied by any combination of hardware and/or software that is capable of

- 1) Reading/analyzing information stored in the Subscriber Identity History store 7.
 - 2) Displaying such information in a human readable form
- AND/OR
- 3) Allowing such information to be used programmatically

Figure 5 shows a second embodiment of the invention. In this embodiment, the CMA and the CRA have been merged depicted in the figure by CMA/CRA 2. Furthermore, IS and the SIH have been merged depicted in the figure by IS/SIH 3. The embodiment functions like the embodiments discussed earlier except that there is no need for communication between the *observing sub-system* and the *recording sub-system* as they have been merged.

Figure 6 shows a flow diagram for a method for tracking association of mobile equipment with mobile subscribers' identity. The method starts at block 1. The method continues, via block 2, by detecting the MT identities. It checks whether the identities have undergone a change (block 3) and continues, via block 4, by recording changes if this is the case. The method terminates at block 5.

Figure 7 shows a flow diagram for a second embodiment of the method. This embodiment adds steps to detail the method when it is applicable to the CMA being an extension of the MT software as discussed with reference to Figure 2. The method starts at block 1.

It continues via blocks 2,3 and 4 detecting MT identities, retrieving old MT identities and comparing them. It checks whether the identities have changed (block 5). If they have not changed, the method terminates in block 10. If they have changed, the method continues via blocks 6,7,8 and 9 successively updating the local IS on the MT, communicating changed

identities over a network, receiving this information over the network in the *recording sub-system* and storing the new values in the SIH. The method then terminates in block 10.

Figure 8 shows a flow diagram for a third embodiment of the method. This differs from Figure 7 only in block 2 hence only this block shall be discussed here.

Block 2 in figure 8 detects MT identities based on a Probe as discussed in the embodiment of figure 3. This step is activated either when the MT logs on to the cellular network, or by periodically *polling* the Probe for identity information.

Figure 9 shows a flow diagram for a fourth embodiment of the method. This flow diagram corresponds to the second embodiment of the invention as depicted in figure 5. It differs from figure 8 only because it lacks certain steps. This is due to the fact that in the second embodiment of the invention, the observing sub-system and the recording sub-system are combined.

Figure 10 shows a schematic of some software products according to the present invention. A total of n different software products 102(1), 102(2),...,102(n) are shown in figure 10, where n is an integer. The software products 102(1), 102(2),...,102(n) can be directly loaded into the internal memory of at least one digital computer 100(1), 100(2),...,100(n). Figure 10 also shows a total of n computers. Each software product 102(1), 102(2),...,102(n) comprises software modules in order to carry out one part or all of the steps according to figure 6 when the product or products 102(1), 102(2),...,102(n) are run on the computer or computers 100(1),...,100(n). The software products 102(1), 102(2),...,102(n) may, for example, be in the form of diskettes, RAM-disks, magnetic tapes, CD-ROMs or any other suitable products.

In addition the figure shows a total of m different software products 103(1), 103(2),...,103(m), where m is an integer. The software products 103(1), 103(2),...,103(m) can be directly loaded into the internal memory of at least one mobile terminal 101(1), 101(2),...,101(m). Figure 10 also shows a total of m mobile terminals. Each software

product 103(1), 103(2),...,103(m) comprises software modules in order to carry out one part or all of the steps according to figure 6 when the product or products 103(1), 103(2),...,103(n) are run on the mobile terminal or terminals 101(1),...,101(m). The software products 103(1), 103(2),...,103(n) may, for example, be in the form of diskettes, RAM-disks, magnetic tapes, CD-ROMs or any other suitable products.

The invention is not limited to the embodiments described above. It will be clear that many different modifications will be possible within the scope of the attached claims.

CLAIMS

1. A method of recording mobile terminal usage data for subsequent use, the method comprising:

providing device identity parameters identifying a particular mobile terminal;

when the operating state of the mobile terminal is active, detecting subscriber identity parameters for a subscriber using the particular mobile terminal;

determining whether the subscriber identity parameters for the particular mobile terminal have changed over time, and, if so,

storing changed subscriber identity parameters in a memory together with an association of the changed subscriber identity parameters with the device identity parameters of the particular mobile terminal without losing precedent subscriber identity parameters associated with the particular mobile terminal.

2. A method as claimed in claim 1 wherein the operating state of the mobile terminal being active is defined by the existence of at least one of the following operating states:

when the mobile terminal is first switched on after being in an inactive state,

when the mobile terminal is first logged onto a mobile communications network,
and

when the mobile terminal has been actively logged onto a mobile communications network for a significant period of time (a) after first logging onto the network, or (b) after last detecting of the subscriber identity parameters while the mobile terminal is logged onto the mobile communications network.

3. A method as claimed in claim 1 or 2 wherein subscriber identity parameters are stored in a memory of the particular mobile terminal including at least the last detected subscriber identity parameters prior to the performance of the step of detecting current subscriber identity parameters for the subscriber using the particular mobile terminal, and wherein the step of determining whether the current subscriber identity parameters for the particular mobile terminal have changed is carried out by processing means of the mobile

terminal which is operative to compare current subscriber identity parameters with the stored last precedent subscriber identity parameters.

4. A method as claimed in claim 3 wherein the particular mobile terminal is operative to generate a flagging signal when it determines that the current subscriber identity parameters have changed compared to the stored last precedent subscriber identity parameters, the flagging signal being generated on a mobile communication network so as to enable the step of storing changed subscriber identity parameters in a memory to be performed externally of the mobile terminal in response to detection of the flagging signal on the communications network.

5. A method as claimed in claim 1 or 2 wherein subscriber identity parameters are stored in a memory of a subscriber monitor external to the mobile terminal and operatively associated with the communication network, the stored subscriber identity parameters including at least the last detected subscriber identity parameters prior to the performance of the step of detecting current subscriber identity parameters for the subscriber using the particular mobile terminal, and wherein the step of determining whether the current subscriber identity parameters for the particular mobile terminal have changed is carried out by processing means of the subscriber monitor external to the mobile terminal and which is operative to compare current subscriber identity parameters with the stored last precedent subscriber identity parameters.

6. A method as claimed in any one of claims 1 to 5 wherein the step of storing the changed subscriber identity parameters in a memory includes storing such changed subscriber identity parameters in a memory external to the particular mobile terminal by means of a recording sub-system which is operatively associated with the mobile communications network and which extracts device identity parameters and subscriber identity parameters from data communications of the particular mobile terminal over the mobile communications network.

7. A method of utilising mobile terminal usage data comprising the method of recording mobile terminal usage data as claimed in any one of claims 1 to 6, and comprising the further steps of:

interrogating the memory of stored subscriber identity parameters for those subscriber identity parameters which have an association in the memory with a particular target mobile terminal having terminal identifying parameters which are input in the interrogating step, and

retrieving at least one of current and any precedent subscriber identity parameters having an association in the memory with the target mobile terminal.

8. A method as claimed in claim 7 wherein the target mobile terminal comprises one which has been previously been lost or stolen, the method comprising a further step of communicating with the target mobile terminal in response to the interrogation of the memory and retrieval of the latest stored subscriber identity parameters even if changed subsequent to the loss or theft of the mobile terminal.

9. A method as claimed in claim 7 wherein the target mobile device is one owned by an enterprise and wherein the method comprises the further step of tracking and logging at least the identities of users of the mobile device for furthering the objectives of the enterprise.

10. A method as claimed in claim 7 and further comprising the step of transmitting messages or data to the target mobile device in response to the steps of interrogating the memory and retrieving subscriber identity parameters, the transmission being based on the identity of the target mobile device and independent of the current or latest subscriber identity parameters.

11. A method as claimed in claim 10 wherein the data transmission to the target mobile device includes transmission of data processing instructions whereby, in response, the mobile device performs data processing operations selected from data deletion, data manipulation, data backup, and data transmission.

12. Apparatus for recording mobile terminal usage data for subsequent use, the apparatus including:

means for providing device identity parameters identifying a particular mobile terminal;

means, operative when the operating state of the mobile terminal is active, to detect subscriber identity parameters for a subscriber using the particular mobile terminal;

means for determining whether the subscriber identity parameters for the particular mobile terminal have changed over time, and, if so,

means for storing changed subscriber identity parameters in a memory together with an association of the changed subscriber identity parameters with the device identity parameters of the particular mobile terminal without losing precedent subscriber identity parameters associated with the particular mobile terminal.

13. Apparatus as claimed in claim 12 for utilising mobile terminal usage data, the apparatus further comprising:

means for interrogating the memory of stored subscriber identity parameters for those subscriber identity parameters which have an association in the memory with a particular target mobile terminal having terminal identifying parameters which are input to the interrogating means, and

means for retrieving at least one of current and any precedent subscriber identity parameters having an association in the memory with the target mobile terminal.