

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
5 February 2009 (05.02.2009)

PCT

(10) International Publication Number
WO 2009/018125 A1

(51) International Patent Classification:
G06F 1/26 (2006.01)

(21) International Application Number:
PCT/US2008/071135

(22) International Filing Date: 25 July 2008 (25.07.2008)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
11/832,900 2 August 2007 (02.08.2007) US

(71) Applicant (for all designated States except US): **APPLIED MINDS, INC.** [US/US]; 1209 Grand Central Avenue, Glendale, CA 91201 (US).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **FERREN, Bran** [US/US]; 1236 Benedict Canyon Drive, Beverly Hills, CA 90210 (US). **HILLIS, W., Daniel** [US/US]; 4750 Encino Avenue, Encino, CA 91316 (US).

(74) Agents: **GLENN, Michael A.** et al.; Glenn Patent Group, 3475 Edison Way, Ste. L., Menlo Park, CA 94025 (US).

(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, 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, 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, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— with international search report

— with amended claims

(54) Title: METHOD AND APPARATUS FOR PROTECTING DATA IN A PORTABLE ELECTRONIC DEVICE

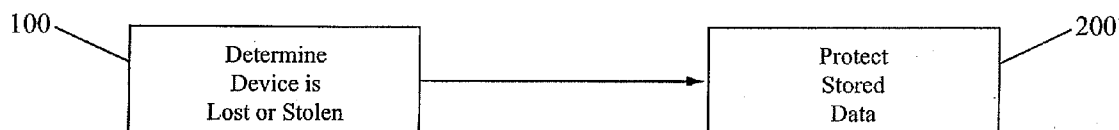


Figure 1

(57) Abstract: Data in a portable electronic device is protected by using external and internal status detection means to determine if the device is misplaced, lost, or stolen. The device then takes, singly or in combination, one of several actions to protect the data on the device, including declaring its location to an owner or service provider, locking the device or specific functions of the device to disable all data retrieval functionality, erasing or overwriting all the stored data in the device or, where the data has been stored in the device in an encrypted format, destroying an internally-stored encryption key, thereby preventing unauthorized access to the encrypted data in the device.

WO 2009/018125 A1

METHOD AND APPARATUS FOR PROTECTING DATA IN A PORTABLE ELECTRONIC DEVICE

5

CROSS-REFERENCES

The present application claims priority to related patent application, serial number 11/832,900 filed August 2, 2007, entitled "Method and Apparatus for Protecting Data in a Portable Electronic Device," which is not admitted to be prior art with respect to the
10 present invention by its mention in the background. This application is incorporated herein in its entirety by this reference thereto.

BACKGROUND OF THE INVENTION

TECHNICAL FIELD

The invention relates to portable electronic devices, and in particular to a system and
15 methods for protecting and safeguarding the privacy of information and data stored on such devices.

DISCUSSION OF THE PRIOR ART

Portable electronic devices, including cell phones, wireless devices, iPods, PDA's and
20 handheld devices, among others, have become ubiquitous in society and are seeing continually increasing widespread use. An October 2004 survey by the Pew Research Center for The People and The Press estimated that 66% of American adults own cell phones. The use of more fully featured portable electronic devices has also become more commonplace.

In response to this increasing usage, designers of portable electronic devices are offering increased functionality, and users are storing an ever-larger volume of private data on the devices. Most portable electronic device users store contact information on the device, and, many users additionally store materials such as confidential communications and proprietary documents. Storage of sensitive data is particularly prevalent in the business community, with some analysts estimating that in the near future as much as 40 percent of corporate data will reside on handheld devices.

As the ability to send, receive, and store data has increased, the risk posed by the potential loss of the data has increased accordingly. The consequences of data falling into the hands of a stranger should a device be lost, temporarily misplaced or stolen are particularly severe.

It is not unusual for persons to lose or misplace their portable electronic devices. Frequently, persons fail to ever recover the device since they cannot determine where and when they actually misplaced the device, or, whether it was stolen. For example, a person might leave the device in the back seat of a cab or in the booth of a restaurant at lunch. Perhaps the device falls out of a jacket or briefcase in an overhead compartment on an airplane. Further, and creating significant embarrassment, one might leave the device at a client's office. Still further, a car might be vandalized and a cell phone stolen. Whatever the case may be, it is quite likely that most people will lose or temporarily misplace their portable electronic device each year. Research shows that 65 percent of Americans lost their cell phones last year -- and it cost \$600 million to replace them.

Losing a phone due to absentmindedness is not just frustrating, though. It also causes great anxiety in the IT departments of many major corporations, because, these days, mobile phones are so powerful that most of them are mini-PCs, containing customer information, phone numbers and pricing schedules. Consequently, a lost phone or PDA may mean a data breach these days, as e-mail isn't the only application found on the devices. More mobile applications are being developed to complement e-mail, such as CRM (customer resource management) and ERP (enterprise resource planning) to

make mobility and the deployment of mobile devices even more valuable for the enterprise.

One approach to safeguarding private data is storage of data at a central location. Many portable electronic devices provide an ability to 'synchronize' data stored on the device with data stored on a personal computer. Some wireless providers also provide centralized storage of personal data. For example, the OASYS "VIRTUAL LOCKER" (<http://store.oasysmobile.com/common/about-the-locker>) stores subscriber data at a centralized server. The service offers protection against the nuisance of recreating the lost data in the event of a lost device, and ensures portability of data across future device upgrades. Such approaches, however, do little to safeguard the data cached locally on the portable electronic device, and, in the latter case, the security of the data is blindly entrusted to a third party.

For the foregoing reasons, there is a need for a novel portable electronic device data protection system and methods to confidently protect data stored locally in the device that can be implemented by the owner of the device, the device service provider, or, by the device itself.

SUMMARY OF THE INVENTION

A method and apparatus for protecting data on a lost portable electronic device is discussed, in which external or internal status detection means are used to determine if the device is misplaced, lost, or stolen. The device then takes one or more actions to protect the data on the device, including declaring its location to an owner or service provider, locking the device or specific functions of the device to disable all data retrieval functionality, erasing the stored data in the device or, where the data has been stored in the device in an encrypted format, destroying an internally-stored encryption key, thereby preventing unauthorized access to the encrypted data in the device.

A preferred embodiment of the invention comprises an application, embodied as software or firmware and operating on a portable electronic device, which determines that the portable electronic device is misplaced, lost, or stolen, and that then takes action to safeguard the data stored on the portable electronic device. In a preferred embodiment of the invention, the owner of the device explicitly indicates to the device that it is lost or stolen. In the case of a portable electronic device having cellular phone functionality, the owner may call the device directly and enter a predetermined code that notifies the device that it is lost or stolen. Also in the preferred embodiment of the invention, the device writes data to its internal storage during normal operation in an encrypted format. The device caches the data encryption key within the internal storage of the device during ordinary usage. When it is determined that the device is lost or stolen, the device destroys the encryption key. The owner may then later restore access to the data by providing the encryption key to the device.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a flow chart illustrating the basic operation of an embodiment of the invention;

Figure 2 is an expanded flow chart derivative of the flow chart in Figure 1 illustrating the operation of several embodiments of the invention; and

Figure 3 is a further expanded flow chart derivative of the flow chart in Figure 2 illustrating the operation of additional embodiments of the invention.

DETAILED DESCRIPTION OF A PREFERRED EMBODIMENT

In a preferred embodiment, the invention comprises an application operating on a portable electronic device that (1) determines that the portable electronic device is misplaced, lost or stolen, and (2) takes action to safeguard the data stored on the

portable electronic device. Many embodiments of the invention are possible, based on different techniques for achieving each of the aforementioned functions.

To determine that it is misplaced, lost or stolen, *i.e.*, has an undesirable status, the portable electronic device uses one of several techniques. For purposes herein, the terms, "undesirable status," "misplaced, lost, or stolen," and "lost or stolen" are used in a generic sense to indicate that the portable electronic device is not under control of the owner/user, and therefore, the owner/user is interested protecting the data in the device from access by unauthorized persons.

In the preferred embodiment of the invention, the device receives from the owner an indication that it is misplaced, lost or stolen. For example, in the case of a portable electronic device having cellular phone functionality, the owner may call the device directly and enter a predetermined code that notifies the device that it is lost or stolen. In the case of a portable electronic device that does not have cellular phone functionality, the owner may call a service number operated by the service provider, and the service provider then transmits an appropriate signal to the device using other communication protocols, including other wireless communication systems or landline and network systems.

In an alternative embodiment of the invention, the portable electronic device itself detects that it is misplaced, lost, or stolen. For example, the device may detect that it is misplaced, lost, or stolen based on its current position. The owner of the device defines a region within which he intends to operate the device. If the device leaves the defined region, the device assumes that it has been misplaced, lost, or stolen. An embedded GPS unit, wireless triangulation, or time-of-flight calculations may calculate the position of the device. Alternatively, in areas where service coverage is ordinarily reliable, loss of signal alone may indicate that the device has departed from the intended usage area. The device observes its position and triggers various actions for data protection based upon predetermined location parameters.

Another technique that the portable electronic device may use to detect that it is misplaced, lost, or stolen is observation of a prolonged period of inactivity or activity.

For example, in a device with cellular phone functionality, the device may compare the elapsed time since the owner last placed a call to a threshold value set by the manufacturer or the owner and, depending on the result of the comparison, elect to trigger certain data protection functions. The device observes its own activity levels and triggers various actions for data protection based upon predetermined activity levels.

In yet another technique, a device having cellular phone functionality monitors the phone numbers dialed, and compares them with either or both of a history of previously dialed numbers and numbers within the internally stored contact information. The device observes dialing patterns and triggers various actions for data protection based upon any predetermined events or anomalous dialing patterns.

Finally, the device may combine two or more of the above techniques to provide a more sophisticated determination of when it has been misplaced, lost, or stolen.

Once the device determines that it is likely misplaced, lost, or stolen, the device may take one or more of several actions, each providing an additional level of security. In one embodiment of the invention, the device enters a beacon mode in which it transmits its location. For example, if the device is equipped with a GPS unit, it may transmit its location to a central server operated by the service provider. The owner of the device may then access the location of the device, e.g. via a web page that adequately authenticates the identity of the owner. Alternatively, the portable electronic device may call a predetermined number, e.g. the land line of the owner, and report, e.g. with a synthesized voice, its current location to either a message recorder or directly to the owner.

In another embodiment of the invention, the portable electronic device provides a higher level of protection by entering a non-functional lock-down mode after determining it is misplaced, lost, or stolen. Once in lock-down mode, the device does not allow data retrieval therefrom. The device returns to full operation only when the owner can be reliably authenticated, for example via a predetermined password or biometric identification.

However, as a skilled hacker may still defeat the authentication process, the preferred embodiment of the invention provides an even higher level of security. In a preferred embodiment of the invention, during normal operation the device writes data to the internal storage in an encrypted format. The device caches the encryption key within the storage during ordinary usage, so that the encryption and decryption processes do not inconvenience the user. When it is determined that the device is misplaced, lost, or stolen, the device destroys the encryption key. The owner may restore access to the data by providing the encryption key, which he has presumably recorded in a safe location.

In yet another embodiment of the invention, the portable electronic device completely erases the contents of its on board data storage. If the storage incorporates volatile memory, the device may cut the power to the memory. If the storage incorporates non-volatile memory, the device may overwrite the data, preferably multiple times. The device may use a file utility such as "GNU SHRED" to perform the overwriting. While providing essentially complete security, this approach does prevent direct recovery of the data by the owner.

In a further embodiment of the invention, the portable electronic device implements the actions described above in sequence, entering beacon mode immediately upon determination that it is misplaced, lost, or stolen. If more time passes before the owner recovers the device, the remaining actions are undertaken in sequence, with each action providing and increased level of security.

As illustrated in Figure 1, a preferred embodiment of, the invention comprises a method and apparatus for protecting data in a portable electronic device. The invention further comprises method comprising a first step 100 of determining that the device is misplaced, lost, or stolen; and a second step 200 of protecting the data stored in the device. A portable electronic device can include any such device which has data storage and the ability to send and receive communications or to automatically act on indicators of status and trigger actions to protect data on the device whenever a certain status has developed. Portable electronic devices include cell phones, pagers, PDA's,

memory sticks, portable hard drives, iPod's, MP3 players, and any other such device which is mobile, stores data for its user, and includes sufficient memory and logic to implement the functions of the invention.

Figure 2 is a more detailed diagram that shows a procedure for determining that the device is lost or stolen 100 and that may be accomplished by the device either (1) receiving external notification 110 of the loss or theft or (2) using internal means 120 to detect loss or theft.

In Figure 2, to implement the step of protecting stored data 200, the invention may employ several different approaches, either singly or in combination, as follows. First, the device may declare its location 210. Second, the device may lock data retrieval functionality 220. Third, where data on the device has been encrypted, the device may destroy an encryption key 230, thereby preventing unauthorized access to the data. Fourth, the device may erase the stored data 240.

As illustrated in Figure 3, the invention may employ additional status detection 100 and data protection 200 means. Where certain means are described in a singular fashion, the invention provides that any of the means may be used either singly or in combination. First, the device may receive a call and code from its owner 112 to alert the device that it is lost or stolen. Either singly or in combination with a call from an owner 112, the device may also receive notice communicated directly from a service provider 114. Either singly or in combination, the device may also use its own internal status detection means including observing its position 122, observing device activity levels 124 or observing dialing patterns on the device 126, among other things.

Further, in response to the determination that the device has been misplaced, lost, or stolen, to protect its stored data, either singly or in combination, the device can declare its location 210 by transmitting its location to a service provider 212 or by announcing its location to an owner 214. The device may announce its location to an owner 214 using several different approaches, either singly or in combination, including: triggering an automated call to the owner on another designated number, triggering an instant

message to the owner, sending an email to the owner, paging the owner on another designated number, sounding an audible alarm, or by triggering some other form of communication to the owner, such as placing an indication of the device location on a website accessible by the owner.

- 5 Once the portable electronic device has determined or been alerted that it has an undesirable status and has been either misplaced, lost, or stolen, the device can also choose to take the additional following steps to protect its data, either singly or combination, including locking down data retrieval functionality 220, destroying an encryption key 230, or erasing the stored data 240.
- 10 In a preferred embodiment, the invention comprises a data protection system for a portable electronic device having an owner. The portable electronic device has data storage, means for determining a status of the portable electronic device, and means for protecting data on the portable electronic device whenever a status of the portable electronic device is undesirable. For present purposes, an "owner" is defined as
- 15 someone who actually either owns the device or is an authorized user of the device and, hence, entitled to protect the data on the device. This definition of owner is not intended to prescribe or prevent the use of the invention in other circumstances, where use of the device may be temporary, on lease, or otherwise.

In a first version, the means for determining status of the portable electronic device may

20 be external to the portable electronic device. The owner of the device subjectively or objectively determines that the device has an undesirable status. An undesirable status includes being misplaced, lost, or stolen. An undesirable status further includes knowing the location of the device, not having current access to the device, but wishing to prevent access to data on the device by others while it is in the known, but undesirable

25 location. Generally, when the device is in a known but undesirable location, the owner has inadvertently temporarily left the device at a known location such as a restaurant, an airplane, at another person's office, at a friend's house, at a business, or some other similar circumstance.

External status communication may occur via any of at least two methods. The first method consists of an owner making a determination that the portable electronic device has an undesirable status. The owner communicates a status code to the device to indicate the undesirable status, and the device receives the status code from the owner.

5 The second method consists of a service provider determining that the portable electronic device has an undesirable status. The service provider communicates with the device to provide a notice to the device of status, and the device receives the notice.

Alternatively, in another embodiment, the data protection system may use internal means in the portable electronic device for determining status of the device. These
10 means may include any of the following, either singly or in combination: observing a position of the portable electronic device; observing an activity level of the portable electronic device; or observing a dialing pattern of the portable electronic device.

Once the data protection system has used either external or internal means to determine a status of the portable electronic device, various means for protecting data
15 on the device are triggered by the device. These means for protecting data stored on the device include, singly or in combination: (1) the device declaring its own location to its owner or a service provider; (2) the device locking data retrieval functionality; (3) where data is stored in an encrypted format, destroying an encryption key stored in the device to prevent further access to the data; or (4) erasing the data in the device.

20 A preferred embodiment, of the invention for protecting data in a lost portable electronic device, wherein the data is encrypted with an encryption key stored in the device, comprises the steps of: (1) an owner of the device determining that the device has an undesirable status; (2) the owner calling the device and transmitting a code to the device indicating the undesirable status; (3) the device receiving the code; and (4) the
25 device destroying the stored encryption key, thereby preventing access to the data on the device.

The previously described versions of the invention have many advantages, including simple implementation, flexible methods of implementation, varying levels of security, varying means for notification, automated determination of device status, and universal

applicability to any portable electronic device, wireless and otherwise, among other things. The invention does not require that all the advantageous features and all the advantages need to be incorporated into every embodiment of the invention.

Although the invention has been described in considerable detail with reference to
5 certain preferred versions thereof, other versions are possible. For example, in addition to GPS, other forms of device locating technology can be used, such as RFID, WiFi triangulation, microwave or broadcast triangulation, ultrawideband triangulation, and other location and position detection systems that might evolve in the future. Further, other access inhibitors can be triggered upon determination that the device has an
10 undesirable status, such as the requirement for a thumb-print, retinal scan or other bio-identification input. Additionally, such features as power-disconnect, screen blanking, and other interruptions to device functionality may be triggered upon determination that the device has an undesirable status. Additionally, although an undesirable status is described as misplaced, lost, or stolen, the invention may be easily adapted to address
15 other status circumstances, such as presence within certain distrusted wireless networks, presence within certain geographical regions, and any other status circumstances which might be of interest to a user or owner of the device. In addition, although described as having external and internal means for determining status and triggering data protection actions, in additional embodiments, a device can be enabled
20 with any of the described features in an automated fashion, thereby creating a smart implementation which is triggered automatically based upon the device's detection of certain events or activities, as previously described.

Although the invention is described herein with reference to the preferred embodiment, one skilled in the art will readily appreciate that other applications may be substituted for
25 those set forth herein without departing from the spirit and scope of the present invention. Accordingly, the invention should only be limited by the Claims included below.

CLAIMS

1. A method for protecting data in a portable electronic device, comprising the steps of:

determining that the device is misplaced, lost, or stolen; and

protecting the data in the device if it is determined that the device is misplaced,
lost, or stolen.

2. The method of Claim 1, wherein the step of determining that the device is misplaced, lost, or stolen takes place external to the device.

3. The method of Claim 2, wherein the external determination step further comprises the steps of:

an owner determining that the device is misplaced, lost, or stolen; and

the owner notifying the device using wireless means.

4. The method of Claim 3, wherein the step of notifying the device further comprises the steps of:

the device receiving a call from the owner; and

the device receiving a code from the owner during the call that informs the device that the device is misplaced, lost, or stolen.

5. The method of Claim 2, wherein the external determination step further comprises the step of:

the device receiving notice from a service provider that the device is misplaced, lost, or stolen.

6. The method of Claim 1, wherein the step of determining that the device is misplaced, lost, or stolen further comprises the step of:

the device using internal self-detection to determine the device is misplaced, lost, or stolen.

7. The method of Claim 6, wherein the step of using internal self-detection further comprises the step of:

5 observing a position of the device.

8. The method of Claim 6, wherein the step of using internal self-detection further comprises the step of:

 observing an activity level of the device.

9. The method of Claim 6, wherein the step of using internal self-detection further
10 comprises the step of:

 observing dialing patterns of the device.

10. The method of Claim 1, wherein the step of protecting the data in the device further comprises the step of:

 declaring a location of the device.

15 11. The method of Claim 10, wherein the step of declaring a location further comprises the step of:

 transmitting the location of the device to a service provider.

20 12. The method of Claim 10, wherein the step of declaring a location further comprises the step of:

communicating the location of the device to a device owner.

13. The method of Claim 1, wherein the step of protecting the data in the device further comprises the step of:

locking the device to eliminate data retrieval functionality.

5 14. The method of Claim 1, wherein data in the device is encrypted with an encryption key and the step of protecting the data in the device further comprises the step of:

destroying the data encryption key, thereby preventing unauthorized access to the data in the device.

10 15. The method of Claim 1, wherein the step of protecting the data in the device further comprises the step of:

erasing the data.

16. A data protection apparatus comprising:

a portable electronic device having data storage;

15 means associated with said portable electronic device for determining status of the portable electronic device; and

means associated with said portable electronic device for protecting data on the portable electronic device whenever the status of the portable electronic device is determined to be undesirable.

20 17. The data protection apparatus of Claim 16, wherein the means for determining status of the portable electronic device is external to the portable electronic device.

18. The data protection apparatus of Claim 17, wherein the external status determination means comprises:

means for allowing an owner to make a determination that the portable electronic device has an undesirable status;

means for allowing the owner to communicate a status code to the portable electronic device to indicate the undesirable status; and,

5 means in the portable electronic device for receiving the status code from the owner.

19. The data protection apparatus of Claim 17, wherein the external status determination means comprises:

10 means for a service provider, to determine that the portable electronic device has an undesirable status;

means for the service provider to communicate with the portable electronic device to provide a notice to the portable electronic device of the undesirable status; and

means within the portable electronic device for receiving the notice.

15 20. The data protection apparatus of Claim 16, wherein the means for determining status of the portable electronic device is internal to the portable electronic device.

21. The data protection apparatus of Claim 20, wherein the internal means for determining status of the portable electronic device comprises:

20 means within the portable electronic device for observing a position of the portable electronic device.

22. The data protection apparatus of Claim 20, wherein the internal means for determining status of the portable electronic device comprises:

25 means within the portable electronic device for observing an activity level of the portable electronic device.

23. The data protection apparatus of Claim 20, wherein the internal means for determining status of the portable electronic device comprises:

5 means within the portable electronic device for observing a dialing pattern of the portable electronic device.

24. The data protection apparatus of Claim 16, wherein the means for protecting data on the portable electronic device comprises:

10 means within the portable electronic device for declaring a location of the portable electronic device.

25. The data protection apparatus of Claim 24, wherein the portable electronic device declares the location by transmitting the location to a service provider.

15 26. The data protection apparatus of Claim 24, wherein the portable electronic device declares its location by transmitting the location to an owner.

27. The data protection apparatus of Claim 16, wherein the means for protecting data on the portable electronic device comprises:

means within the portable electronic device for locking data retrieval functionality.

20 28. The data protection apparatus of Claim 16, further comprising:

means for encrypting the data in the portable electronic device with an encryption key; and

where the means for protecting data on the portable electronic device comprises:

means within the portable electronic device for destroying the data encryption key.

29. The data protection apparatus of Claim 16, wherein the means for protecting data in the portable electronic device comprises:

5 means within the portable electronic device erasing the data in the portable electronic device.

30. The data protection apparatus of Claim 16, wherein the means for determining status of the portable electronic device is both external and internal.

10

31. The data protection apparatus of Claim 30, wherein the internal means for determining status of the portable electronic device comprises any of means for observing portable electronic device position, means for observing portable electronic device activity level and means for observing portable electronic device dialing patterns.

15

32. A method for protecting data in a portable electronic device, wherein the data is encrypted with an encryption key stored in the portable electronic device, the method comprising the steps of:

20 an owner of the portable electronic device determining that the device has an undesirable status,;

the owner calling the portable electronic device and transmitting a code to the portable electronic device indicating the undesirable status;

the portable electronic device receiving the code; and

25 upon receipt of the code, the portable electronic device destroying the stored encryption key;

wherein access to the data on the portable electronic device is prevented.

**AMENDED CLAIMS received by the International Bureau on
02 December 2008**

1. A method for protecting data in a portable electronic device, comprising the steps of:

determining that the device is misplaced, lost, or stolen, wherein the device uses internal self-detection to determine the device is misplaced, lost, or stolen; and

protecting the data in the device if it is determined that the device is displaced, lost, or stolen.

2. The method of Claim 1, wherein the step of using internal self-detection further comprises the step of observing an activity level of the device.

3. The method of claim 1, wherein the step of using internal self-detection comprises observing dialing patterns of the device.

4. The method of Claim 1, wherein the step of using internal self-detection further comprises the step of observing a position of the device.

5. The method of Claim 1, wherein the step of protecting the data in the device comprises the step of declaring a location of the device.

6. The method of Claim 5, wherein the step of declaring a location comprises the step of transmitting the location of the device to a service provider.

7. The method of Claim 5, wherein the step of declaring a location comprises the step of communicating the location of the device to a device owner.

8. The method of Claim 1, wherein the step of protecting the data in the device comprises the step of locking the device to eliminate data retrieval functionality.

9. The method of Claim 1, wherein data in the device is encrypted with an encryption key and the step of protecting the data in the device comprises the step of destroying the encryption key, thereby preventing unauthorized access to the data in the device.

10. The method of Claim 1, wherein the step of protecting the data in the device further comprising erasing the data.

11. The method of claim 4 further comprising the steps of:
establishing an area of frequent usage; and
determining whether the position is outside the area of frequent usage, wherein the determination that the position is outside the area of frequent usage provides evidence that the device is misplaced, lost or stolen.

12. A data protection apparatus comprising:
a portable electronic device having data storage;
means associated with said portable electronic device for determining status of the portable electronic device, wherein said means for determines status is internal to the portable electronic device;
means associated with said portable electronic device for protecting data on the portable electronic device whenever the status of the portable electronic device is determined to be undesirable.

13. The data protection apparatus of Claim 12, wherein the internal means for determining status of the portable electronic device further comprises:
means within the portable electronic device for observing an activity level of the portable electronic device.

14. The data protection apparatus of Claim 12, wherein the internal means for determining status of the portable electronic device further comprises:

means within the portable electronic device for observing a dialing pattern of the portable electronic device.

15. The data protection apparatus of Claim 12, wherein the internal means for determining status of the portable electronic device further comprises:

means within the portable electronic device for observing a position of the portable electronic device.

16. The data protection apparatus of Claim 12, wherein the means for protecting data on the portable electronic device comprises:

means within the portable electronic device for declaring a location of the portable electronic device.

17. The data protection apparatus of Claim 16, wherein the portable electronic device declares the location by transmitting the location to a service provider.

18. The data protection apparatus of Claim 16, wherein the portable electronic device declares its location by transmitting the location to an owner.

19. The data protection apparatus of Claim 12, wherein the means for protecting data on the portable electronic device comprises:

means within the portable electronic device for locking data retrieval functionality.

20. The data protection apparatus of Claim 12, further comprising:

means for encrypting the data in the portable electronic device with an encryption key;

wherein the means for protecting data on the portable electronic device comprises:

means within the portable electronic device for destroying the encryption key.

21. The data protection apparatus of Claim 12, wherein the means for protecting data in the portable electronic device comprises:

means within the portable electronic device erasing the data in the portable electronic device.

22. The data protection apparatus of Claim 15 further comprising:

a means for establishing an area of frequent; and

a means for determining whether the position is outside the area of frequent usage, wherein the determination that the position is outside the area of frequent usage provides evidence that the device is misplaced, lost or stolen.

23. A data protection apparatus comprising:

a portable electronic device having data storage;

means for encrypting the data in the portable electronic device with an encryption key; and

means associated with said portable electronic device for determining status of the portable electronic device;

means associated with said portable electronic device for protecting data on the portable electronic device whenever the status of the portable electronic device is determined to be undesirable, said means comprising destroying the encryption key.

24. The data protection apparatus of Claim 23, wherein the means for determining status of the portable electronic device further comprises means for observing an activity level of the portable electronic device.

25. The data protection apparatus of Claim 23, wherein the means for determining status of the portable electronic device further comprises means for observing a dialing pattern of the portable electronic device.

26. The data protection apparatus of Claim 23, wherein the means for protecting data on the portable electronic device comprises means for declaring a location of the portable electronic device.

27. The data protection apparatus of Claim 26, wherein the portable electronic device declares the location by transmitting the location to a service provider.

28. The data protection apparatus of Claim 26, wherein the portable electronic device declares its location by transmitting the location to an owner.

29. The data protection apparatus of Claim 23, wherein the means for determining status takes place external to the device, said means for determining selected from among:

- an owner determining that the device is misplaced, lost, or stolen, and the owner notifying the device using wireless means; and

- the device receiving notice from a service provider that the device is misplaced, lost, or stolen.

30. The data protection apparatus of Claim 29, wherein the step of the owner notifying the device further comprises the steps of:

- the device receiving a call from the owner; and

- the device receiving a code from the owner during the call that informs the device that the device is misplaced, lost, or stolen.

31. The data protection apparatus of Claim 23, wherein the means for determining status of the portable electronic device further comprises:

- means within the portable electronic device for observing a position of the portable electronic device.

32. The data protection apparatus of Claim 31, wherein the means for determining status of the portable electronic device further comprises:

a means for establishing an area of frequent usage; and

a means for determining whether the position is outside the area of frequent usage, wherein the determination that the position is outside the area of frequent usage provides evidence that the device is misplaced, lost or stolen.

1/3

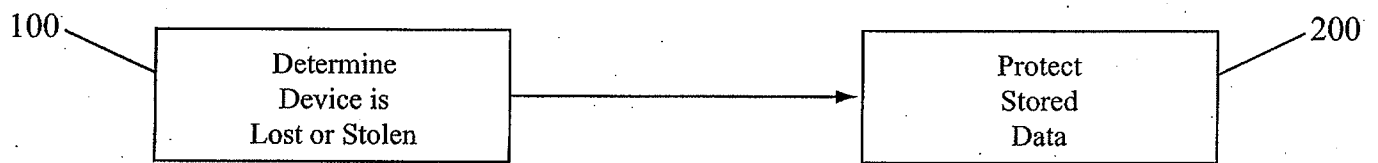


Figure 1

2/3

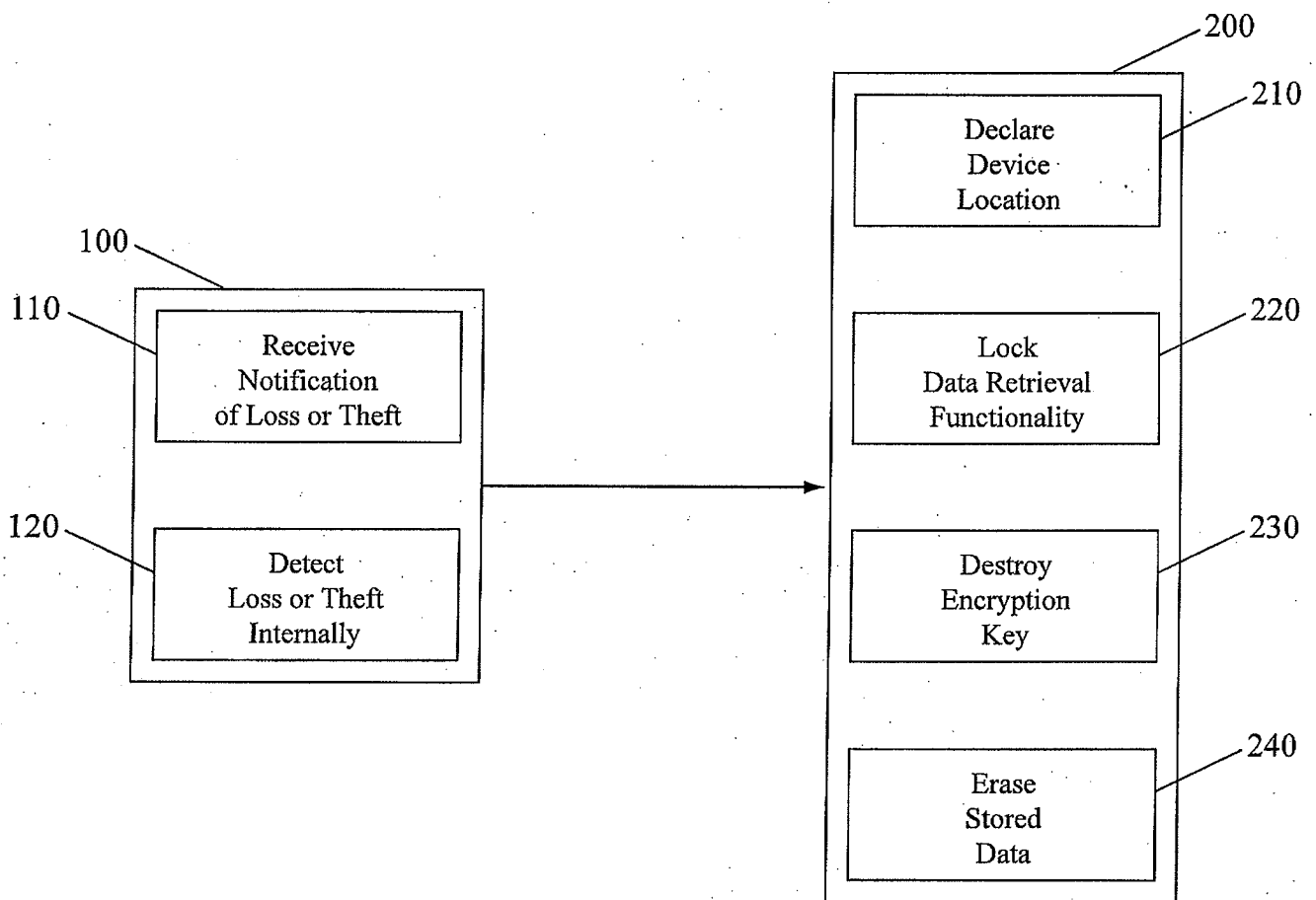


Figure 2

3/3

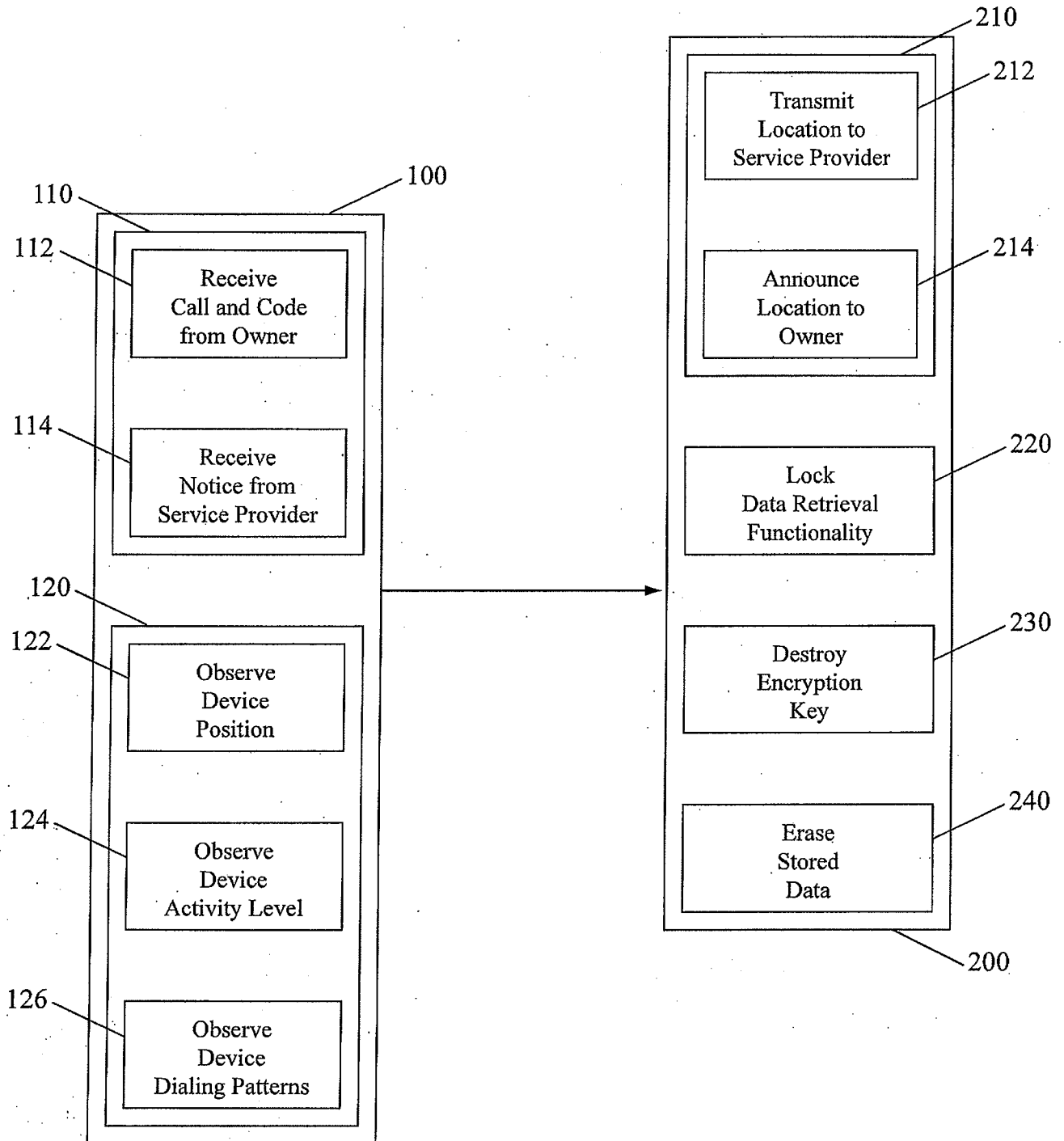


Figure 3

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US2008/071135

A. CLASSIFICATION OF SUBJECT MATTER

IPC(8) - G06F 01/26 (2008.04)

USPC - 726/035

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC(8) - G06F 01/26 (2008.04)

USPC - 726/035

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 practicable, search terms used)

MicroPatent

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X --- Y	US 2005/0073389 A1 (CHANDLEY) 07 April 2005 (07.04.2005) entire document	1-8, 10-22, 24-32 ----- 9, 23
Y	WO 97/38521 A1 (STODDARD) 16 October 1997 (16.10.1997) entire document	9, 23

☐ Further documents are listed in the continuation of Box C.

* Special categories of cited documents:

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search

23 September 2008

Date of mailing of the international search report

03 OCT 2008

Name and mailing address of the ISA/US

Mail Stop PCT, Attn: ISA/US, Commissioner for Patents
P.O. Box 1450, Alexandria, Virginia 22313-1450

Facsimile No. 571-273-3201

Authorized officer:

Blaine R. Copenheaver

PCT Helpdesk: 571-272-4300

PCT OSP: 571-272-7774