

LOSS PROTECTION SYSTEM FOR PORTABLE MEDIA

Field of the Invention

This invention relates to portable media for storing electronic data. More particularly, this invention relates to a system for protecting the loss of the media and/or data stored by the media. Still more particularly, this invention relates to application stored on the media and loaded into executable memory of a system to cause the system to monitor a triggering event and perform a security function when the triggering event occurs.

Summary of the Prior Art

Since the first use of computers, one of the easiest ways to store and transfer data is by using portable media such as disks, compact disks, memory sticks and the like. However, security of the data has always been an issue for portable media. One specific problem is that a user often forgets to remove the portable media from a computer system after use and leaves the portable media with the computer system after use. The data is then lost to the user and a subsequent user of the system may find the portable media and have access to the data.

To protect the data from being available to subsequent users of the portable media, those skilled in the art began to protect the data with a password. However, this is commonly only a deterrent as many password breaking algorithms are known and can be used to overcome the password protection. Thus, password protection does not provide adequate protection for sensitive data that a user may wish to protect.

Encryption of the stored data has been used in the past. The encryption of the data is a better method for ensuring the data is not accessible by another user that finds

the portable media. However, encryption is only as good as the encryption key used to encrypt the data. Furthermore, data encryption does not address the issue of the user retrieving the data stored on the media.

5 In the past, the size of the portable media has made it problematic to provide any features for loss protection. As technology has advanced, it has become possible to include loss protection features for the media. Most loss protection features previously provided included some circuitry in addition to the portable media that determine the media has been left behind.

10

Some of these features use a transceiver system connected to the media that communicates via Radio Frequency (RF) or other types of signals with a transceiver system in a portable device carried by the user. The signals are used to determine when the portable media is outside of a predetermined range. When the portable media is
15 outside the predetermined range from the portable device of the user, an alarm or other method of alerting the user is activated in the device carried by the user and/or the portable media. These features have several drawbacks. First, the signals may be blocked by the physical features of the connected computer system or the room in which the computer system is housed causing false reporting. A second disadvantage is that
20 the user must carry the portable device at all times the portable media is used. A third disadvantage is the circuitry can either increase the size of the portable media making the media more cumbersome to use or the circuitry takes up valuable space in the media that reduces the amount of memory for storing data in the device.

25 Other security features for portable media include circuitry connected to the portable media that detects whether the media is connected to a computer system. Some portable media having these features include an internal timer that performs a

security function such as erasing the media or encrypting data stored by the media after a predetermined amount of time. Other security features include circuitry that detects power being supplied from the connected system and will erase or encrypt the media if the power is detected for more than a predetermined amount of time. This monitoring system
5 also requires additional circuitry connected to the media which may reduce the amount of media that can be provided to store data.

Thus, those skilled in the art are constantly striving to make improved loss protection systems for portable media device.

10

Summary of the Invention

The above and other problems are solved and an advance in the art is made by a loss protection system for a portable media in accordance with this invention. A first advantage of a system in accordance with this invention is that the system may be
15 installed in any media without additional circuitry. This allows a system in accordance with this invention to be installed on existing devices that have sufficient memory space. Further, no additional manufacturing steps are needed to assemble the devices. A second advantage of a system in accordance with this invention is that, since no additional circuitry is needed, the size and portability of a portable device is not effected.
20 Thus, a portable media device including a loss protection system in accordance with this invention is as portable and easy to carry and use as prior art portable media devices. A third advantage of a loss protection system in accordance with this invention is that the system may protect both against physical loss of the device and loss of data stored by the media when the media is physically lost by a user.

25

In accordance with this invention, a loss protection system is instructions stored as software, hardware, or firmware in a portable media device that operates in the following

manner. The instructions for the system are loaded from the media into a memory of a processing system when the media is connected to the processing systems. The system then monitors the processing system for a first triggering event. When the first triggering event is detected, the processing system then executes a security function. For purposes
5 of this discussion a portable media device is any device that may be connected to a processing system to interact with the system and a processing system is a computer or any other device that includes a processor, volatile memory, a system bus, and interface connected to the bus to allow device to connect to the system.

10 In some embodiments, the first triggering event is a lack of input from a connected device for a specified amount of time. In particular embodiments, the connected device may be a keyboard, a mouse, or other type of I/O device. In other embodiments, the first triggering event may be a lack of activity over the system for a specified amount of time.

15 In accordance with some embodiments of this invention, the security function performed may be the transmission of a message to the user indicating that the portable media device is still connected to the processing system. A message may be sent in the following manner. First, the processing system generates the message. The processing system then reads an address from a memory in either the processing system or the
20 portable media device and transmits the message to the read address. Depending on the embodiment, the message may be an e-mail, short message service (SMS) message to a mobile telephone, and/or a dialog box displayed on a video device connected to the processing system

25 In accordance with other embodiments of the invention, the security function may be encryption of the data stored by the portable media device. The encrypting function begins by the processing system reading the data stored by the media of the portable

media device. The data is then encrypted by the processing system. The encrypted data is then stored by the processing system in the media of the portable media device.

In accordance with other embodiments of the invention, the security function may
5 include the transmission of the data stored by the portable media over a network to a specific network address. In accordance with these embodiments, the processing system reads the data store by the portable media. The processing system then reads a network address from either the portable media device or the memory of processing system; and transmits the data over a connected network, such as the Internet to the read address.

10

In accordance with still other embodiments of this invention the security function may include the processing system erasing the data stored by the portable media.

In accordance with some embodiments of this invention, the system may
15 determine whether the portable media device is currently connected to the processing system in response to a detection of the first triggering event. In these embodiments, the system only executes the security function in response to a determination that the portable media device is connected to the system when the first triggering event occurs.

20 In accordance with some embodiments of the invention, the processing system may monitor for the occurrence of multiple triggering events. A security function is then executed in response to each of the triggering events detected. In accordance with some of these embodiments, different security functions are executed for each one of the triggering events detected. When one of the triggering events is detected, the processing
25 system determines and executes the security function that corresponds to the detected triggering event.

In accordance with other embodiments of this invention, multiple security functions may be executed by the processing system in response to the detection of a single triggering event.

5 In accordance with some embodiments of this invention, a user interface, such as a graphical user interface, may be provided by the processing system to allow a user to enter information to the system and change the parameters of the invention. The received inputs are then stored by the media in the device for use in providing the system. In accordance with some embodiments, the information may include device information
10 that may include data, such as a device name, and/or a device description. In some embodiments, the input information may include host location information. The host location information may include information such as a host system name, a host system network address, and/or indication of a location tracking process for the host system. The system parameters received may include the triggering events to monitor, the timing
15 of the triggering event, and/or a selection of security functions to perform in response to trigger events.

Brief Description of the Drawings

The above and other advantages and features of a loss protection system in
20 accordance with this invention are described in the following detailed description and are shown in the following drawings:

Figure 1 illustrating a processing system and connectable portable media devices in accordance with embodiments of this invention;

Figure 2 illustrating a block diagram of a component of a processing system that
25 connects to portable media devices and executes instructions to provide a loss protection system in accordance with embodiments of this invention;

Figure 3 illustrating a flow diagram of processes performed by a loss protection system in accordance with embodiments of this invention;

Figure 4 illustrating a flow diagram of monitoring processes in accordance with some embodiments of this invention;

5 Figure 5 illustrating a flow diagram for a security function that generates and transmits a message in accordance with embodiments of this invention;

Figure 6 illustrating a flow diagram for a security function that encrypts data stored by a portable media device in accordance with embodiments of this invention;

10 Figure 7 illustrating a flow diagram for a security function that transmits data stored by a portable media device in accordance with embodiments of this invention;

Figure 8 illustrating a flow diagram for a security function that erases data stored by a portable media device in accordance with embodiments of this invention;

Figure 9 illustrating a flow diagram of a process for receiving inputs from a user of a loss protection system in accordance with embodiments of this invention; and

15 Figure 10 illustrating display of a graphical user interface for receiving inputs from a user of a loss protection system in accordance with this invention.

Detailed Description

20 This invention relates to portable media for storing electronic data. More particularly, this invention relates to a system for protecting the loss of the media and/or data stored by the media. Still more particularly, this invention relates to applications stored on the media and loaded into executable memory of a system to cause the system to monitor a triggering event and perform a security function when the triggering event occurs.

25

Figure 1 illustrates a processing system 100 and various portable media device that may include a loss protection system in accordance with this invention. In Figure 1,

processing system 100 is shown as a convention desktop personal computer. However, for purposes of this invention processing system 100 may be a desktop personal computer, a laptop personal computer, a computer terminal, server, router, or any system having a processor, memory, and interfaces for connecting to a device for reading from
5 and writing to a memory media.

In the shown embodiment, processing system 100 includes display 105, keyboard 130, and mouse 140 that are connected to the system as described in Figure 2 to allow user interaction with processing system 100. Processing system 100 also includes
10 optical disk drive 115 and magnetic disk drive 120. Optical disk 155 is inserted into optical disk drive 115 to allow processing system 100 to read data from and write data to optical disk 155. Magnetic disk 150 is inserted into magnetic disk drive 120 to allow processing system 100 to read data from and write data to magnetic disk 150.

15 Furthermore, processing system 100 includes Universal Serial Bus (USB) ports 125 that allow a USB compliant device to connect to and interface with processing system 100 via an UBS connector. Examples of USB compliant devices include memory stick 160, digital camera 165, musical playback device 170, and digital video recorder 175. One skilled in the art will recognize many other USB compliant digital devices may
20 connect to processing system 100 via USB ports 125.

Although a transceiver is not shown, processing system 100 may include a RF or other type of signal transceiver that allows devices to connect to and interface with processing system 100 via signalling using a known protocol such as Bluetooth. Thus, in
25 accordance with this invention, a portable media device is any device that connects to a processing system to allow data to be read from and written to a data storage media in a

connected device. The only requirement being that the device has sufficient memory to store the instructions for a loss protection system in accordance with this invention.

Figure 2 illustrates a block diagram of the processing components of processing system 200 that executes instructions to provide applications for use of processing system 100. Processing system 100 includes Central Processing Unit (CPU) 205. CPU 205 is a processor, microprocessor, or any combination of processors and microprocessors that execute instructions to perform the processes in accordance with the present invention. CPU 205 connects to memory bus 210 and Input/Output (I/O) bus 215. Memory bus 210 connects CPU 205 to memories 220 and 225 to transmit data and instructions between the memories and CPU 205. I/O bus 215 connects CPU 205 to peripheral devices to transmit data between CPU 205 and the peripheral devices. One skilled in the art will recognize that I/O bus 215 and memory bus 210 may be combined into one bus or subdivided into many other buses and the exact configuration is left to those skilled in the art.

A non-volatile memory 220, such as a Read Only Memory (ROM), is connected to memory bus 210. Non-volatile memory 220 stores instructions and data needed to operate various sub-systems of processing system 200 and to boot the system at start-up. One skilled in the art will recognize that any number of types of memory may be used to perform this function.

A volatile memory 225, such as Random Access Memory (RAM), is also connected to memory bus 210. Volatile memory 225 stores the instructions and data needed by CPU 205 to perform software instructions for processes such as the processes for providing a system in accordance with this invention. One skilled in the art

will recognize that any number of types of memory may be used to provide volatile memory and the exact type used is left as a design choice to those skilled in the art.

I/O device 230, keyboard 235, display 240, memory 245, network device 250 and
5 any number of other peripheral devices connect to I/O bus 215 to exchange data with CPU 205 for use in applications being executed by CPU 205. I/O device 230 is any device that transmits and/or receives data from CPU 205. Keyboard 235 is a specific type of I/O device that receives user input and transmits the input to CPU 205. Other examples of I/O devices include a mouse, Personal Digital Assistant (PDA) and other
10 USB compliant devices. Display 240 receives display data from CPU 205 and display images on a screen for a user to view. Memory 245 is a device that transmits and receives data to and from CPU 205 for storing data to a media. One skilled in the art will recognize that more than one memory 245 may be connected to system 100. Examples of memory devices include optical disk drive 115 and magnetic disk drive 120 shown in
15 Figure 1; and memory sticks and the like that connect to processing system 100 via USB Ports. Network device 250 connects CPU 205 to a network for transmission of data to and from other processing systems.

In accordance with embodiments of this invention, a loss protection system is a
20 set of instructions for applications stored by a portable media device. The instructions may be stored in the media as software, hardware, or firmware. The instructions are read from the portable media device by a processing system when the portable media device is connected to the processing system. The read instructions are then loaded into an executable memory and performed by the processing system to protect loss of the
25 portable media that is left connected to the processing system when the user leaves.

Figure 3 illustrates an embodiment of a process 300 performed by instructions for a loss protection system in accordance with this invention. Process 300 begins by loading the applications instructions from the portable memory device to executable memory of a processing system when the portable processing device is connected to the processing system in step 305. This is performed by the processing system reading the instructions from the portable media device and writing the instructions to an executable memory such as a RAM connected to a processing unit. One skilled in the art will recognize that this may be provided by the "plug and play" feature of common operating system that allow device to be connected to a processing system and read without the need to initialize the system. Furthermore, an automatic executable application may be stored in the media to cause the application to be loaded into the RAM of processing system to begin execution of the applications by the processing system when the portable media device is connected.

In step 310, the processing system begins performing a triggering event monitoring application. The monitoring application monitors for one or more triggering events to occur. A triggering event can be any action and/or inaction of an application performed by or a device connected to the processing system. Some examples of triggering events include a lack of input received from an I/O device, such as keyboard or mouse, for a specified period of time; lack of read and/or write operations to a device connected to processing system; lack of response for a software application; and detection of a user logging off the processing system. One skilled in the art will recognize that any other detectable event may be used without departing from this invention.

In step 315, the monitoring application determines whether one of the triggering events occurred. If a trigger event occurred, the processing system executes the applications that provide a security function in step 325. Some examples of security

functions that may be performed include transmitting a message to a stored address as shown in Figure 5 and described below; encrypting the data stored by the media as shown in Figure 6 and described below; transmitting the data stored by the media to a stored network address as shown in Figure 7 and described below; and erasing the data
5 stored by the media as shown in Figure 8 and described below. One skilled in the art will recognize that any number of security functions may be performed in addition to the functions previously recited without departing from this invention. After the security function is performed, process 300 ends.

10 If the event is not detected, process 300 may determine whether there is any information for the loss protection system that must be updated in step 335. In some embodiments, the determination may be made by determining whether a Graphical User Interface (GUI) has received an input of information from a user. An example of the information that may be received is show in Figure 9 and described below. However, one
15 skilled in the art will recognize that other detection and input methods may be used without departing from this invention.

If there is no information to update, process 300 repeats from step 315 to monitor the system for the triggering events. If there is information to be updated, the update
20 information is received in step 340 and stored to either the media or a memory in the processing system in step 345. Process 300 then repeats from 315 to monitor the system for triggering events.

Figure 4 illustrates a process 400 for performing monitoring by the processing
25 system to detect occurrences of triggering events and executing security functions in accordance with some embodiments of this invention. Process 400 begins in step 405 by initializing any timers that are needed for monitoring for specific triggering events. In step

410, the timers begin timing. The system then monitors the processing system for the occurrence of one or more trigger events in step 415. As described above, a triggering event can be any action and/or inaction of an application performed by or a device connected to the processing system. Some examples of triggering events include a lack
5 of input received from an I/O device, such as keyboard or mouse, for a specified period of time; lack of read and/or write operations to a device connected to processing system; lack of response for a software application; and detection of a user logging off the processing system. One skilled in the art will recognize that any other detectable event may be used without departing from this invention.

10

In step 420, process 400 determines whether a triggering event has occurred. If a triggering event has not occurred, process 400 increments the timers in step 435 and repeats from step 415. If a triggering event has occurred, process 400 may proceed directly to step 440 or monitor the portable media device to determine whether the device
15 is connected in step 425. If the device is determined not to be connected to the processing system in step 427, process 400 ends.

If the device is determined to still be connected in step 427 or in response to the detection of an occurrence of a triggering event in step 420, process 400 determines one
20 or more security functions to be performed in step 440. The one or security functions to perform may be determined by the specific triggering event that was detected. For example, if keyboard inactivity for 600 seconds is detected, a message generating security function may be performed. However, if system inactivity for 1200 seconds is detected a data encryption security function and a second type of message generating
25 security function may be performed. The number of triggering events monitored and specific security functions to be performed being left as either a design choice of those skilled in the art or to a user of the system.

The security functions determined in step 440 are then executed in step 445. Process then determines whether to continue monitoring for triggering events in step 450. If process 400 is to continue monitoring, process 400 returns to step 435 and increments
5 the timers. Process 400 then repeats from step 415. Alternatively, process 400 may proceed to repeat from step 405 after step 445 if process 400 is to monitor the processing system for the occurrence of the same event. If process 400 is not to continue monitoring, process 400 ends.

10 Figure 5 illustrates a process 500 that is a message generating security function in accordance with some embodiments of this invention. Process 500 may be used to generate many different types of messages including, but not limited to, Short Message Service (SMS) messages, e-mails, and dialog boxes. Process 500 begins in step 505 by generating a message in the proper format. An address to receive the message is then
15 read from either the portable media device or the memory of the processing system. The message is then transmitted to the read address by the processing system in a conventional manner in step 515 and process 500 ends.

Figure 6 illustrates a process 600 that is a media data encryption security function
20 provided in accordance with some embodiments of this invention. One skilled in the art will recognize that the steps of this process may be performed iteratively on portions of the data stored by the portable media device if the amount of data stored is too great. Process 600 begins by reading the data from the media in step 605. In step 610, the data is then encrypted either using an encryption technique provided by the processing system
25 or an encryption method downloaded from the portable media device. Process 600 then ends by storing the encrypted data onto the media in the portable media device in step 615.

Figure 7 illustrates a process 700 that is a security function for transmitting data stored by the portable media device to a network address in accordance with some embodiments of this invention. One skilled in the art will recognize that the steps of this process may be performed iteratively on portions of the data stored by the portable media device if the amount of data stored is too great. Process 700 begins in step 705 by reading data from the portable media device. In step 710, a network address, such as an IP Internet address is read from either the portable media device or the memory of the processing system. The data is then transmitted over a network to the read address in conventional manner by step 715 and process 700 ends when all of the data is transmitted.

Figure 8 illustrates process 800 that provides a data erase security function on the portable media device in accordance with some embodiments of this invention. Process 800 is performed in a conventional data erase function of the media in portable media device to erase all of the data stored by the media that is either stored in the processing system or downloaded from the portable media device in step 805. Preferably, the erase function writes over the media multiple times to ensure that the data cannot be recovered. After the data stored by the media is erased, process 800 ends.

Figure 9 illustrates a process that receives user inputs to update a configuration of the loss protection system to user preferences in accordance with some embodiments of this invention. Process 900 begins in step 905 by determining if device information is received. In some embodiments, the device information includes a device name and/or a device description that allows a user to identify a portable media device and data stored by the device. If device information is received in step 905, the data is stored into a

proper space in a configuration file or other data structure either in the device and/or in the processing system in step 910.

After any device information is stored, process 900 determines if location
5 information is received. In some embodiments, location information may include a host system name, a host system network address, and/or a location determine method for locating the host system. If location information is received in step 915, the location information is stored into a proper space in a configuration file or other data structure stored by the device and/or the processing system in step 920.

10

After any location information is stored, process 900 determines if trigger
information is received. In some embodiments, trigger information may include a system to monitor for a particular event and a time and/or duration of the event. For example, the event may be inactivity of the keyboard and the duration may be 500 seconds. If trigger
15 information is received in step 925, the trigger information is stored into a proper space in a configuration file or other data structure stored by the device and/or the processing system in step 930.

After any trigger information is stored, process 900 determines if notification
20 information is received. In some embodiments, notification information may include a selection of a type of message to sent, and/or a recipient address to receive the message. If notification information is received in step 935, the notification information is stored into a proper space in a configuration file or other data structure stored by the device and/or the processing system in step 940.

25

After any notification information is stored, process 900 determines if protection
information is received. In some embodiments, protection information may include an

indication of a type of security function to perform in response to a particular triggering event. If protection information is received in step 945, the protection information is stored into a proper space in a configuration file or other data structure stored by the device and/or the processing system in step 950 and process 900 ends.

5

Figure 10 illustrates a Graphical User Interface (GUI) 1000 provided in accordance with some embodiments of this invention to allow a user to provide information to a loss protection system; and change the configuration and/or parameters of the system. GUI 1000 is a conventional GUI that is provided in a conventional manner
10 based upon the operating system used and other system requirements. One skilled in the art will recognize that other GUIs and other types of interfaces may be used to display and receive information from a user.

GUI 1000 has four display sections: device identification section 1010, location
15 tracking section 1020, triggering method section 1030, notification method section 1040 and data protection section 1050. Each of these sections displays options that a user may use to provide information to a loss protection system.

Device identification section 1010 includes name dialog box 1012 and description
20 dialog box 1015. Name dialog box 1012 allows a user to input a title for the portable media device. The title is then stored in a configuration file or other data structure by the portable media device and/or processing system. The title is then used in message to identify the portable media device to the user. Description dialog box 1015 allows a user to input a description of the portable media device and/or content of data stored by the
25 device. The description is then stored in a configuration file or other data structure by the portable media device and/or processing system. The description may then be used in message to further identify the device to the user.

Location tracking section 1020 includes host name dialog box 1022, host address dialog box 1024, Global Positioning System (GPS) check box 1026, Access Point triangulation check box 1027, cellular triangulation check box 1028 and base station triangulation check box 1029. Host name dialog box 1022 allows a user to input a name identifying the processing system to which the portable media device is connected. The host name is then stored in a configuration file or other data structure by the portable media device and/or processing system. The host name is then used in message to help identify the location of the portable media device and processing system to the user.

Host address dialog box 1024 allows a user to input an IP or other network address identifying the processing system to which the portable media device is connected. The host address is then stored in a configuration file or other data structure by the portable media device and/or processing system. One skilled in the will recognize some embodiments may include a network address read from the configuration information of the processing system in this display automatically for the user. The host address is then used in message to help identify the location of the portable media device and the processing system to the user.

GPS check box 1026, Access Point triangulation check box 1027, cellular triangulation check box 1028 and base station triangulation check box 1029 provide boxes that a user may use a mouse click to select a particular locating security functions that may be provided by the loss protection system. The selected locating security functions are then enabled in a configuration file or other data structure stored on the media device and/or processing system. The selected locating security functions are then used to locate the processing system when a trigger event occurs and provide the location to the user in a generated message. One skilled in the art will recognize that

these are conventional location methods and a description of each is omitted from the application for brevity.

Triggering method section 1030 provides device /media inactivity check box 1031,
5 keyboard inactivity check box 1032, system inactivity check box 1033, mouse inactivity
check box 1034, and inactivity duration dialog box 1036. Device /media inactivity check
box 1031, keyboard inactivity check box 1032, system inactivity check box 1033, and
mouse inactivity check box 1034 allow a user to use a mouse click to select the specific
triggering events for the loss protection system to monitor. One skilled in the art will
10 recognize that any number of additional events may be added without departing from this
invention. The selected triggering events are then enabled in a configuration file or other
data structure stored on the media device and/or processing system. The loss protection
system then monitors processing system for these events to occur.

15 Inactivity duration dialog box 1036 allows a user to input a specific amount of time
for inactivity to occur in the specified triggering events. The time is then stored in a
configuration file or other data structure stored by the portable media device and/or
processing system and is used to determine if a triggering event occurs.

20 Notification method section 1040 includes message box check box 1041, phone
message check box 1042, SMS check box 1043, e-mail check box 1044, telephone
number dialog box 1045, mobile telephone number dialog box 1046, e-mail address
dialog box 1047, and message dialog box 1048. Message box check box 1041, phone
message check box 1042, SMS check box 1043, and e-mail check box 1044 provide
25 boxes that a user may use a mouse click to select a particular type of message that a
message security function provided by the loss protection system may generate and
transmit in response to a triggering event. The selected message types functions are

then enabled in a configuration file or other data structure stored on the media device and/or processing system. The message types are then used by the processing system to generate and transmit messages in the selected format when a triggering event occurs. One skilled in the art will recognize that other messaging formats may be added and any
5 of these formats may be removed from a loss protection system without departing from this invention.

Telephone number dialog box 1045 allows a user to input a telephone number of a particular telephone number to receive a voice telephone message when a telephone
10 message type is selected. The input telephone number is then stored in a configuration file or other data structure stored by the portable media device and/or processing system and is used to transmit a generated telephone message when a triggering event occurs.

Mobile telephone number dialog box 1046 allows a user to input a mobile
15 telephone number of a particular mobile telephone to receive a SMS message when a SMS message type is selected. The input mobile telephone number is then stored in a configuration file or other data structure stored by the portable media device and/or processing system and is used to transmit a generated SMS message when a triggering event occurs.

20

E-mail address dialog box 1047 allows a user to input an e-mail address to receive an e-mail message when an e-mail message type is selected. The input e-mail address is then stored in a configuration file or other data structure stored by the portable media device and/or processing system and is used to transmit a generated e-mail
25 message when a triggering event occurs.

Message dialog box 1048 allows a user to input a message to receive in the selected format(s) when a message type is selected. The input message is then stored in a configuration file or other data structure stored by the portable media device and/or processing system and is used to generate the content of a message in the selected
5 type(s) when a triggering event occurs.

Data protection section 1050 includes data encryption check box 1051, data recovery check box 1052, data erase check box 1053, data encryption time dialog box 1056, data recovery time dialog box 1057 and data erase time dialog box 158. Data
10 encryption check box 1051, data recovery check box 1052, and data erase check box 1053 provide boxes that a user may use a mouse click to select a particular type of data security function provided by the loss protection system to execute in response to a triggering event. Data encryption time dialog box 1056, data recovery time dialog box 1057 and data erase time dialog box 158 allow a user to input a time that acts as a trigger
15 event for the corresponding data security function. The input times are then stored in a configuration file or other data structure stored by the portable media device and/or processing system and are used by the triggering events to monitor and cause the corresponding data security functions to be executed when the input times expire.

20 Update box 1060 allows a user to mouse click on the box to cause an update function to be executed to update the configuration file or other data structure stored by the portable media device and/or processing system. Minimize box 1070 allows a user to minimize the screen display of GUI 1000 to view other display screens. Exit check box 1080 stops execution of GUI 1000.

25

The above describe particular embodiments of a loss protection system for a portable media device in accordance with this invention. It is foreseen that those skilled

in the art can and will design alternative embodiments that infringe on this invention as set forth in the following claims for the description of these embodiments.

What is claimed is:

1. A loss protection system for a portable media device connectable to a processing system comprising:

a memory in said portable media device; and

5 instructions stored in said memory for directing a processing unit to:

load said instructions into a memory of said processing system,
monitor said processing system for a first triggering event, and
execute a security function in response to detection of said first
triggering event.

10

2. The loss protection system of claim 1 wherein said first triggering event is lack of input from a connected device for a specified amount of time.

3. The loss protection system of claim 2 wherein said connected device is a
15 keyboard.

4. The loss protection system of claim 2 wherein said connected device is a mouse.

5. The loss protection system of claim 1 wherein said first triggering event is a lack of
20 system activity in said processing system for a specified amount of time.

6. The loss protection system of claim 1 wherein said instructions include said security function comprising:

instructions for directing a processing unit to:

25

generate a message,
read an address to receive said message, and
transmit said message to said address.

7. The loss protection system of claim 6 wherein said message is an e-mail.

8. The loss protection system of claim 6 wherein said message is a short message
5 service message to mobile telephone.

9. The loss protection system of claim 6 wherein said message is a dialog box on a
display device.

10 10. The loss protection system of claim 1 wherein said instructions include said
security function comprising:

instructions for directing said processing unit to:

read data stored in said memory of said portable media device,
encrypt said data, and

15 store said encrypted data in said memory of said portable media
device.

11. The loss protection system of claim 1 wherein said instructions include said
security function comprising:

20 instructions for directing said processing unit to:

read data from said memory of said portable media device,
read an address from said memory of said portable media device,
and
transmit said data to said address.

25

12. The loss protection system of claim 1 wherein said instructions include said
security function comprising:

instructions for directing said processing unit to:

erase data stored in said memory of said portable media device.

13. The loss protection system of claim 1 wherein said instructions further comprise:

5 instructions for directing said processing unit to:

determine whether said portable media device is connected to said processing system in response to detection of said first trigger event and said executing of said security function being responsive to a determination that said device is connected to said system.

10

14. The loss protection system of claim 1 wherein said instructions further comprise:

instructions for directing said processing unit to:

monitor said processing system for a plurality of trigger events including said first triggering event, and

15 execute a security function in response to each detection of an occurrence of one of said plurality of trigger events.

15. The loss protection system of claim 14 wherein said instructions further comprise:

instructions for directing said processing unit to:

20 execute a different security function in response to detection of each of said plurality of trigger events.

16. The loss protection system of claim 14 wherein said instructions further comprise:

25 instructions for directing said processing unit to determine one of plurality of security functions to execute from said one of said plurality of trigger events detected.

17. The loss protection system of claim 1 wherein said instructions further comprise:

instructions for directing said processing unit to:

execute a plurality of security functions including said security
function in response to detection of said first triggering event.

5

18. The loss protection system of claim 1 wherein said instructions further comprise:

instructions for directing said processing unit to:

receive an input of device information, and

store said input of device information in said memory of said portable

10

media device.

19. The loss protection system of claim 18 wherein said device information includes a
device name.

15

20. The loss protection system of claim 18 wherein said device information includes a
device description.

21. The loss protection system of claim 1 wherein said instructions further comprise:

instructions for direction said processing unit to:

20

receive an input host location information, and

store said host location information in said memory of said device.

22. The loss protection system of claim 21 wherein host location information includes
name for said processing system.

25

23. The loss protection system of claim 21 wherein said host location information
includes a network address for said processing system.

24. The loss protection system of claim 21 where said host location information includes an indication of a location tracking process to determine said location of said processing system.

5

25. The loss protection system of claim 1 wherein said instructions further comprise:

instructions for directing said processing unit to:

receive an input of a triggering event information, and

store said trigger event information in said memory of said portable

10

media device.

26. The loss protection system of claim 25 wherein said triggering event information includes an indication of a device to monitor for inactivity.

15

27. The loss protection system of claim 25 wherein said triggering event information includes an amount of time of inactivity.

28. The loss protection system of claim 1 wherein said instructions further comprise:

instructions for directing said processing unit:

20

receive an input for receiving a selection of a security function to

perform in response to detection of said triggering event, and

store an indication of said security function to perform in said memory of said portable media device.

25

29. The loss protection system of claim 1 wherein said instructions further comprise:

instructions for directing said processing unit to:

receive an input of a notification address, and

store said notification address in said memory of said portable media device.

30. The loss protection system of claim 1 wherein said instructions further comprise:

5 instructions for directing said processing unit to:

provide a graphical user interface to request and receive information from a user.

31. A method of protecting loss of a portable media device connectable to a

10 processing system comprising:

loading instructions for said method stored in said portable media device into said processing system;

monitoring said processing system for a first triggering event; and

executing a security function by said processing system in response to a

15 detection said first triggering event.

32. The method of protecting loss of a portable media device of claim 31 wherein said first triggering event is lack of input from a connected device to said processing system for a specified amount of time.

20

33. The method of protecting loss of a portable media device of claim 32 wherein said connected device is a keyboard.

34. The method of protecting loss of a portable media device of claim 32 wherein said
25 connected device is a mouse.

35. The method of protecting loss of a portable media device of claim 31 wherein said first triggering event is a lack of system activity in said processing system for a specified amount of time.

5 36. The method of protecting loss of a portable media device of claim 31 wherein said step of executing said security function comprises:

generating a message in said processing system;

reading an address to receive said message by said processing system;

and

10 transmitting said message to said address from said processing system.

37. The method of protecting loss of a portable media device of claim 36 wherein said message is an e-mail.

15 38. The method of protecting loss of a portable media device of claim 36 wherein said message is a short message service message.

39. The method of protecting loss of a portable media device of claim 36 wherein said message is a dialog box on a display device.

20

40. The method of protecting loss of a portable media device of claim 31 wherein said step of executing said security function comprises:

reading data stored in said memory of said portable media device by said processing system;

25 encrypting said data in said processing device; and

storing said encrypted data from said processing system to said memory of said portable media device.

41. The method of protecting loss of a portable media device of claim 31 wherein step of executing said security function comprises:

5 reading data in said memory of said portable media device by said processing system;
 reading an address from said memory of said portable media device by said processing system; and
 transmitting said data to said address from said processing system.

10 42. The method of protecting loss of a portable media device of claim 31 wherein said step of executing security function comprises:

 erasing data stored in said memory of said portable media device by said processing system.

15 43. The method of protecting loss of a portable media device of claim 31 further comprising:

 determining whether said portable media device is connected to said processing system in response to a detection of said first trigger event and wherein said executing of said security function is responsive to a
20 determination that said device is connected to said system.

44. The method of protecting loss of a portable media device of claim 31 further comprising:

25 monitoring by said processing system for a plurality of trigger events including said first triggering event; and
 executing a security function by said processing system in response to each detection of an occurrence of one of said plurality of triggering events.

45. The method of protecting loss of a portable media device of claim 44 further comprising:

5. executing a different security function by said processing system in response to detection of each of said plurality of triggering events.

46. The method of protecting loss of a portable media device of claim 44 further comprising:

10 determining one of plurality of security functions to execute from said one of said plurality of triggering events detected.

47. The method of protecting loss of a portable media device of claim 31 further comprising:

15 executing a plurality of security functions including said security function by said processing system in response to detection of said first trigger event.

48. The method of protecting loss of a portable media device of claim 31 further comprising:

20 receiving an input of device information in said processing system; and storing said input of device information from said processing system into said memory of said portable media device.

49. The method of protecting loss of a portable media device of claim 48 wherein said device information includes a device name.

25

50. The method of protecting loss of a portable media device of claim 48 wherein said device information includes a device description.

51. The method of protecting loss of a portable media device of claim further comprising:

5 receiving an input host location information in said processing device; and
storing said host location information from said processing device into said
memory of said device.

52. The method of protecting loss of a portable media device of claim 51 wherein said
host location information includes name for said processing device.

10

53. The method of protecting loss of a portable media device of claim 51 wherein said
host location information includes a network address for said processing device.

54. The method of protecting loss of a portable media device of claim 51 where said
15 host location information includes an indication of a location tracking process to
determine said location of said processing system.

55. The method of protecting loss of a portable media device of claim 51 further
comprising:

20 receiving an input of triggering event information in said processing system;
and
storing said triggering event information in said memory of said device.

56. The method of protecting loss of a portable media device of claim 55 wherein said
25 triggering event information includes an indication of a device to monitor for
inactivity.

57. The method of protecting loss of a portable media device of claim 55 wherein said triggering event information includes an amount of time of inactivity.

58. The method of protecting loss of a portable media device of claim 31 further comprising:

receiving an input for receiving a selection of a security function to perform in response to detection of a triggering event in said processing system; and

storing an indication of said security function to perform from said processing device into said memory of said portable media device.

59. The method of protecting loss of a portable media device of claim 31 further comprising:

receiving an input of a notification address in said processing system; and storing said notification request from said processing device into said memory of said portable media device.

60. The method of protecting loss of a portable media device of claim 31 further comprising:

providing a graphical user interface to request and receive information from a user by said processing system.