August 26, 2019

ERASURE OF DEVICE DATA UPON DETECTION OF UNDERWATER SUBMERSION

Nabil Shahid

Tony Lai

ERASURE OF DEVICE DATA UPON DETECTION OF UNDERWATER SUBMERSION

ABSTRACT

A computing device (e.g. mobile phone, smartphone, tablet computer, etc.) may be configured to delete data in response to detecting that the computing device has been submerged in water or other liquid (or is otherwise irrecoverable). For example, if a user drops a computing device into a lake, after a certain amount of time, the computing device may delete all or a portion of data stored by the device (e.g., user data, system data, etc.). The computing device may detect submersion in water or other liquid by processing data from one or more sensors (e.g., accelerometers and/or pressure sensors) included in the computing device. Upon detecting submersion in liquid, the computing device may start a countdown timer (e.g., with a time selected to be shorter than the water resistance time of the device) to delay the execution of the delete operation. A user may cancel (e.g., abort) the delete operation prior to the expiration of the timer. For example, if a user drops the computing device into the bathtub but retrieves the device within a short period of time, the user may cancel the delete operation. A user may also configure various settings of the delete feature (e.g., opting in or out of the feature, what data to delete, duration of countdown timer, etc.). By providing the ability to delete data in response to detecting submersion, a computing device may protect data stored by the device.

DESCRIPTION

In recent years, computing device hardware robustness has improved, resulting in computing devices that are less likely to break or sustain damage. Computing devices increasingly include safeguards, for example, water resistance, to protect the device from user mishaps (e.g.,

dropping a device in bathtubs, toilets, pools, streams, or on concrete floors, rocks, etc.). For example, many of the major mobile computing devices, such as smartphones, released in 2019 meet the IP68 standard (of IEC standard 60529), meaning the device can withstand submersion in up to five feet of fresh water for thirty minutes. If a user drops one of these computing devices in a shallow body of water, the device remains operable and data stored by the device remains accessible. As long as the computing device is within the user's immediate control, such improvements benefit a user. However, when a user loses the device, such as when they drop their device off a bridge into a shallow stream, someone else may find the device and improperly access the stored user data (e.g., financial records, medical information, passwords, etc.). Thus, it may be desirable for a computing device to execute a process to delete user data when it determines that the device is submerged in water or other liquid. This may reduce the risk of unauthorized usage of user data.

A computing device may be configured to delete user data after detecting it is submerged in water or other liquid. The computing device may be, include, or otherwise be included in a smartphone, tablet computer, laptop computer, computerized watch, computerized eyewear, computerized gloves, personal computer, portable gaming system, portable media player, mobile television platform, or any other type of wearable, non-wearable, mobile, or non-mobile computing device. The computing device may include a user interface. The user interface may include a touch-sensitive display, to utilize various applications, functions, and other features of the computing device. The computing device may include one or more sensors to improve operational performance and ease of use of the device. Example sensors include, but are not limited to, a magnetometer, barometer, one or more accelerometers, infrared sensor, ambient light sensor, gyroscope, fingerprint sensor, GPS sensor, humidity sensor, moisture sensor, and the like.

The computing device may include a pressure sensor, such as a barometer (e.g., to detect ambient pressure to improve location accuracy for the included GPS sensor and/or measure number of stairs climbed). The computing device may also use the pressure sensor to detect whether the device is under water. The computing device may include one or more accelerometers to calculate speed while running or driving, count steps, or detect when the device falls from a height. The computing device may also include one or more output devices, including but not limited to, a flash for an included camera, one or more speakers, auxiliary port, LED indicator light, or other output devices to generate output to a human or machine. The computing device may process data from the described sensors in various ways to improve the functionality, user experience, and security of the computing device.

A computing device may use one or more sensors of the device to detect when it is submerged in water or other liquid to delete user data upon detecting submersion. For example, the computing device may use one or more accelerometers and/or a pressure sensor to determine when the computing device is submerged in water. Upon detecting that the computing device is submerged in water or other liquid (e.g., in response to detecting, via the pressure sensors, a large sudden increase in pressure), the computing device may execute a delete operation to protect user data stored on the device. An example method to detect device submersion and execute this process is shown below in Figure 1. As Figure 1 is only an example, the steps shown in the figure may be carried out in a different order, carried out simultaneously, and/or omitted entirely (e.g., the fall detection steps may be omitted).

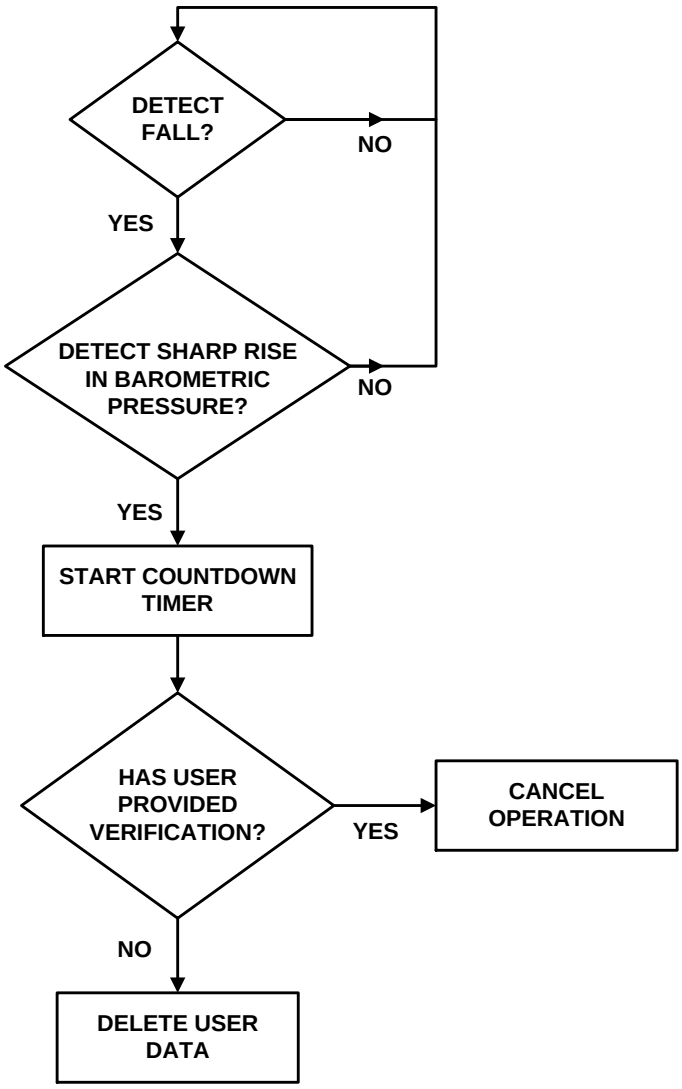

Figure 1

As shown in Figure 1, the computing device may first detect whether the device has fallen. The computing device may use the one or more accelerometers of the device to detect such a fall. A fall may indicate a user accidentally dropped the device and is unable to retrieve it. For example, if the user knocks the computing device from a bridge ledge to a road below, the computing device may detect the device fell. If the device detects a fall, the computing device may then use the included pressure sensor (e.g., barometer) to determine whether the device is submerged in water or other liquid. Because the pressure under water is much higher than atmospheric air, the

computing device may determine that it is submerged when the included pressure sensor detects a sharp rise in pressure.

If the device determines that it is not submerged, the device may resume normal operation. However, if the computing device determines that it both fell and is submerged, the computing device may begin a countdown timer. Upon determining the device is submerged, the computing device may start a countdown timer. When the countdown timer expires the computing device may then execute the delete operation. The countdown timer duration may be configured so that it is shorter in duration than the water resistance time of the computing device (e.g., amount of time the internal components are protected from the ingress of water). For example, if the water resistance time of a device is 30 minutes, the countdown timer duration may be set at 25 minutes. While the timer is counting down, the computing device may allow the user to cancel the delete operation. This can protect the user from inadvertently deleting device data. Upon expiration of the timer, the computing device may execute the delete operation and delete user data from the device.

The computing device may output notifications to alert a user that the device will soon execute the delete operation. For example, the computing device may display via the user interface a time-decaying bar to indicate an amount of time remaining before the device data is deleted. The computing device may also output an audible tone via the included one or more speakers to alert the user that the countdown timer has started. The computing device may also blink (e.g., turn on and off repeatedly) the flash of the device camera or the LED indicator light. Such an output provides a user a perceivable indication, even when under water, that the computing device may execute the delete operation upon expiration of the countdown timer. The described examples alert the user that the computing device may soon delete device data.

The computing device may also allow a user to cancel the delete operation. This may require the user cancel the delete operation before a countdown timer expires to ensure no device data is deleted. In one example, the user interface may display a "Cancel" button. The user may press this button to cancel the operation. The computing device may ask the user to verify their identity or other information before canceling the delete operation. For example, the computing device may ask a user to enter their security lock passcode, pattern lock, password, or other device security information, or use the fingerprint sensor or other biometric verification device to verify the user's identity. If the user successfully verifies their identity, the computing device may cancel the delete operation and resume normal operation.

The computing device may also allow a user to configure various delete operation settings. For example, when setting up the device for the first time, the computing device may ask the user whether they want to opt-in or opt-out of the delete feature. The computing device may recommend a user enable the feature if the user does not secure access to the device with a passcode, password, fingerprint, or other security verification. Alternatively, or additionally, a user may access various settings of the delete feature by navigating the various menus presented by the user interface of the computing device. Example configurable settings include selecting the type of data to delete during the delete operation, the duration of the countdown timer, or opting in or out of the feature, among others. The computing device may allow a user to select the specific type of data to delete during a delete operation. For example, a user may only want to delete certain data files which contain sensitive information, such as financial institution records, healthcare records, passwords, etc. Alternatively, a user may choose to delete all device data during a delete operation. For example, upon expiry of the countdown timer, the computing device

may execute a factory reset. Configurable settings, such as the described examples, provide a user increased control of the security of their personal information.

As the robustness of computing devices to user mishaps improves (e.g., dropping the device from a boat into a shallow lake), user data is increasingly at risk to unauthorized use when the user is unable to retrieve the device. Configuring a computing device to execute a delete process upon detecting submersion in water may improve the privacy and security of user data. This may secure user data from unauthorized use by someone who retrieves the device. Upon detecting submersion, the computing device may start a countdown timer shorter in duration than the water resistance time of the device. During this time a user may cancel the delete operation. The user may configure various settings of the delete feature to ensure confidential and sensitive data is protected from unauthorized use. This may improve the privacy and security of user data.

It is noted that the techniques of this disclosure may be combined with any other suitable technique or combination of techniques. As one example, the techniques of this disclosure may be combined with the techniques described in US Patent Application Publication 2007/0254697A1. As another example, the techniques of this disclosure may be combined with the techniques described in US Patent Application Publication US20150312754A1. As another example, the techniques of this disclosure may be combined with the techniques described in US Patent Application Publication US20160334294A1.