July 2021

PRIVACY DASHBOARD

Jingyu Wu

Dave Chung

Joyaa Lin

Sara N-Marandi

PRIVACY DASHBOARD

ABSTRACT

A computing device may display a graphical user interface (GUI) of a privacy dashboard showing permission usage of sensor data (e.g., location, microphone, camera, etc.) and content provider data (e.g., files, media, contacts, calendar, short message service (SMS), call log, etc.) by applications for a given time period (e.g., the past 24 hours, the past 7 days, etc.). The privacy dashboard may include graphs, lists, and other visual indicators for displaying information about the permission usage per sensor and/or per application in a clear, concise, and comprehensible way. In the privacy dashboard, the computing device may include certain types of privacy information, such as sensor data usage, within the initial screen while omitting other types of privacy information, such as content provider data usage, from the initial screen. The computing device may display information about other types of privacy information in response to a user input (e.g., touch input). In some examples, the privacy dashboard may enable a user to see detailed information about permission usage of an application and manage permissions for each application via the privacy dashboard. As such, the privacy dashboard may improve user awareness and comprehension of data access by increasing transparency with respect to permission usage by applications.

DESCRIPTION

FIG. 1 below is a conceptual diagram illustrating a computing device 100 that executes a graphical user interface module 102 (“GUI module 102”) to display a graphical user interface (GUI) of a privacy dashboard showing permission usage of sensor data (e.g., location, microphone, camera, etc.) and content provider data (e.g., files, media, contacts, calendar, short

message service (SMS), call log, etc.) by applications for a given time period (e.g., the past 24 hours, the past 7 days, the past month, etc.). Computing device 100 may be any mobile or non-mobile computing device, such as a cellular phone, a smartphone, a desktop computer, a laptop computer, a tablet computer, a portable gaming device, a portable media player, an e-book reader, a watch (including a so-called smartwatch), a gaming controller, and/or the like. As shown in FIG. 1, computing device 100 may include a presence-sensitive display 104, one or more processors 106, one or more storage devices 108, one or more communication components 110 ("COMM components 110"). Storage devices 108 may include GUI module 102, a system application 112, one or more application(s) 114, a device data repository 116, and a data access repository 118.

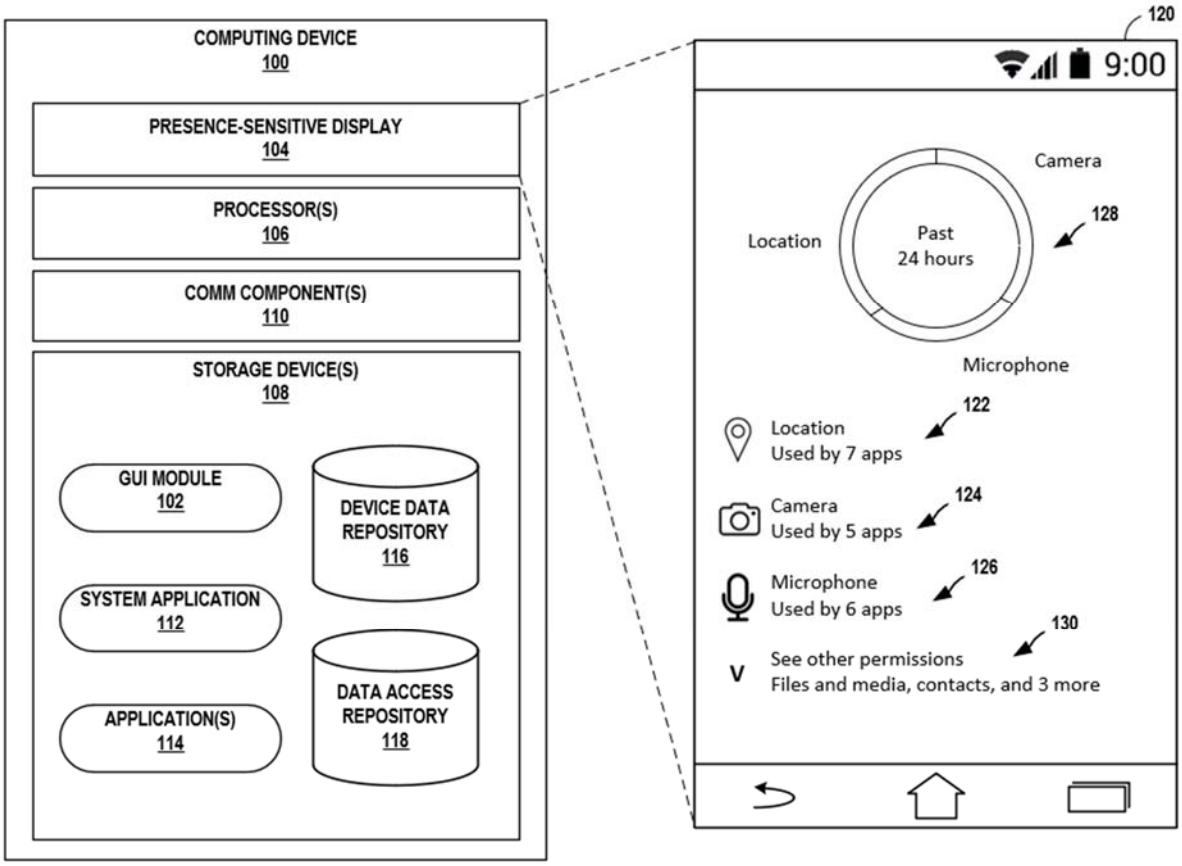

FIG. 1

Presence-sensitive display 104 of computing device 100 may be a presence-sensitive display that functions as an input device and as an output device. For example, presence-sensitive display 104 may function as an input device using a presence-sensitive input component, such as a resistive touchscreen, a surface acoustic wave touchscreen, a capacitive touchscreen, a projective capacitance touchscreen, a pressure sensitive screen, an acoustic pulse recognition touchscreen, or another presence-sensitive display technology. Additionally, presence-sensitive display 104 may function as an output (e.g., display) device using any of one or more display components, such as a liquid crystal display (LCD), dot matrix display, light emitting diode (LED) display, microLED display, organic light-emitting diode (OLED) display, e-ink, active-matrix organic light-emitting diode (AMOLED) display, or similar monochrome or color display capable of outputting visible information to a user of computing device 100.

Processors 106 may implement functionality and/or execute instructions associated with computing device 100. Examples of processors 106 may include one or more of an application specific integrated circuit (ASIC), a field programmable gate array (FPGA), an application processor, a display controller, an auxiliary processor, a central processing unit (CPU), a graphics processing unit (GPU), one or more sensor hubs, and any other hardware configure to function as a processor, a processing unit, or a processing device. System application 102 may be operable by processors 106 to perform various actions, operations, or functions of computing device 100.

Storage devices 108 may include one or more computer-readable storage media. For example, storage devices 108 may be configured for long-term, as well as short-term storage of information, such as instructions, data, or other information used by computing device 100. In some examples, storage devices 108 may include non-volatile storage elements. Examples of

such non-volatile storage elements include magnetic hard discs, optical discs, solid state discs, and/or the like. In other examples, in place of, or in addition to the non-volatile storage elements, storage devices 108 may include one or more so-called “temporary” memory devices, meaning that a primary purpose of these devices may not be long-term data storage. For example, the devices may comprise volatile memory devices, meaning that the devices may not maintain stored contents when the devices are not receiving power. Examples of volatile memory devices include random-access memories (RAM), dynamic random-access memories (DRAM), static random-access memories (SRAM), etc.

Computing device 100 may include communication components 110 (“COMM components 110”). COMM components 110 may receive and transmit various types of information over a network, such as a cellular radio, a third-generation (3G) radio, a fourth-generation (4G) radio, a fifth-generation (5G) radio, a Bluetooth® radio (or any other personal area network (PAN) radio), a near-field communication (NFC) radio, a WiFi® radio (or any other wireless local area network (WLAN) radio), and/or the like. Additionally or alternatively, computing device 110 may include wired communication devices capable of transmitting and/or receiving communication signals via a direct link over a wired communication medium (e.g., a Universal Serial Bus (USB) cable).

In general, computing device 100 may use a permission system to control access to device data in device data repository 116, which can include sensitive information. Under these permission systems, an application, such as application 114, that requires device data to perform a function first needs to request permission and then receive it to access the device data. For example, application 114 may be a map application that requires location data in order to function properly; consequently, application 114 may need to request such permission from the

user, which the user may grant or deny. If the user grants application 114 the requested permission, the user may have no insight into how application 114 is actually using the permission. While system application 112 of computing device 100 may record permission usage to a ledger stored in data access repository 118 that is viewable by the user, the ledger may contain a large amount of technical information and therefore be difficult for a user to understand.

In accordance with techniques of this disclosure, GUI module 102 may display a GUI of a privacy dashboard 120 ("privacy dashboard 120") showing permission usage of sensor data and content provider data by applications 114 for a certain period (e.g., the past 24 hours, the past week, the past month, etc.) to provide better transparency to users about when device data stored in device data repository 116 is accessed by applications 114. Privacy dashboard 120 may include graphs, charts, tables, lists, and other graphical elements for displaying information about the permission usage per sensor and/or per application in a clear, concise, and comprehensible way. The information may be based on a ledger (e.g., a record) of data access by applications 114 in data access repository 118. The ledger may be created by system application 112, which in some examples may be a module responsible for revoking and granting permissions and providing basic information about the permissions.

Privacy dashboard 120 may be designed to provide relevant information to the user while reducing the amount of distracting information displayed to a user. For instance, GUI module 102 may cluster (e.g., group, collect, etc.) data accesses by application 114 into a single access. For example, if application 114 (e.g., a social networking application) accesses data access repository 118 multiple times (e.g., 2, 5, 10, etc.) in a time period (e.g., one minute, one hour, etc.), privacy dashboard 120 may indicate only one access during that same time period.

Similarly, if application 114 (e.g., an application package (APK)) accesses data access repository 118 in each time period of a series of consecutive time periods (e.g., for 2 consecutive minutes, 5 consecutive minutes, 10 consecutive minutes, etc.), privacy dashboard 120 may indicate only one access during the series of consecutive time periods (while indicating the length of the series of consecutive time periods). As indicated above, a time period may have a fixed length, such as one minute, one hour, etc. In some instances, a time period may be an amount of time starting with the first access by an application and ending with the last access. Other definitions of a time period are contemplated by this disclosure. In some examples, privacy dashboard 120 may uncluster data accesses by application 114 (e.g., in response to user input) to show each data access by application 114.

Privacy dashboard 120 may provide an overview of permissive usage of sensor data and content provider data by applications during a certain period (e.g., past 24 hours). For example, as shown in FIG. 1, privacy dashboard may include a location graphical element 122 indicating the number of applications using location data, a camera graphical element 124 indicating the number of applications using camera data, a microphone graphical element 126 indicating the number of applications using microphone data, etc. In some examples, privacy dashboard 120 may further include a visual indicator 128 that changes based on the sensors that were used during the certain period. For example, if the location and camera sensors were used during the past 24 hours but not the microphone sensor, location and camera sensors may be (e.g., equally) represented in visual indicator 128, but the microphone sensor may not be represented at all.

Privacy dashboard 120 may include certain types of privacy information, such as sensor data usage, within the initial screen while omitting other types of privacy information, such as content provider data usage, from the initial screen. For example, as shown in FIG. 1, privacy

dashboard 120 may show location graphical element 122, camera graphical element 124, microphone graphical element 126, etc., but only show graphical elements for the content provider data in response to actuation of expansion graphical element 130.

FIG. 2 is a conceptual diagram illustrating a sensor-specific GUI 132 of privacy dashboard 120 ("sensor-specific privacy dashboard 132") listing which of applications 114 used the corresponding sensor during the certain period and an application-specific GUI 134 of privacy dashboard 120 ("application-specific privacy dashboard 134") displaying detailed information about permission usage of one of applications 114. GUI module 102 may display sensor-specific privacy dashboard 132 in response to a user actuating one of graphical elements 122-126. GUI module 102 may display application-specific privacy dashboard 134 in response

to a user actuating one of application graphical elements 136A-136F (collectively, "application graphical elements 136").

Sensor-specific privacy dashboard 132 may show when (e.g., the time of day) and how (e.g., in the foreground, in the background, etc.) applications 114 used a specific sensor. Application-specific privacy dashboard 134 may include detailed information about the permissions for application 114, such as permissions that are always allowed, the permissions that need to be asked for every time, the permissions that are not allowed, etc.

In some examples, sensor-specific privacy dashboard 132 and/or application-specific privacy dashboard 134 may include a permission graphical element 138 associated with managing permissions for applications 114. Actuating permission graphical element 138 may result in invocation of a corresponding function for managing permissions, which may include presenting (e.g., via presence-sensitive display 104) graphical elements associated with allowing or denying permissions for that application on presence-sensitive display 104. The user may allow or deny one or more permissions by actuating these graphical elements. In examples where the user denies one or more permissions, computing device 100 may deny application 114 access to the corresponding one or more sensors.

In some examples, application 114 may call an application programming interface (API) that uses device data to perform a function on behalf of application 114. In such cases, the API, not application 114, may request permission from the user to access device data repository 116. To ensure that privacy dashboard 120 accurately identifies (e.g., from the perspective of the user) the program responsible for accessing device data repository 116, GUI module 102 (e.g., in coordination with system application 112) may attribute the data access to both the API that

directly accessed device data repository 116 and application 114 that effectively indirectly accessed device data repository 116 using the API.

One or more advantages of the techniques described in this disclosure include improving user awareness and comprehension of data access by increasing transparency with respect to permission usage by applications. By visually communicating data usage per sensor and/or per application in a clear, concise, and comprehensible way, the privacy dashboard informs and users about which applications have access to the device data. This may lead to the discovery of, for example, overprivileged applications during a certain period, such as the past 24 hours. Providing this information may help a user make decisions regarding whether the user wants to allow permission for a particular application and under what circumstances.

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 Derks, "Fair Privacy: Improving Usability of the Android Permission System," Centre for International Development Issues, August 2015. In another example, the techniques of this disclosure may be combined with the techniques described in Tsai et al., "Turtle Guard: Helping Android Users Apply Contextual Privacy Preference," USENIX Association, May 10, 2017. In yet another example, the techniques of this disclosure may be combined with the techniques described in U.S. Patent Application Publication No. 2019/0108353A1. In yet another example, the techniques of this disclosure may be combined with the techniques described in Schoon, "Android 12 DP1: Privacy toggles can block camera and microphone with a tap," 9 to 5 Google, February 18, 2021.