(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
12 December 2024 (12.12.2024)

WIPO | PCT

(10) International Publication Number
WO 2024/253959 A1

(51) International Patent Classification:
H04L 9/40 (2022.01) *H04W 12/60* (2021.01)
H04W 12/30 (2021.01)

(21) International Application Number:
PCT/US2024/031893

(22) International Filing Date:
31 May 2024 (31.05.2024)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
63/470,880 03 June 2023 (03.06.2023) US
18/391,414 20 December 2023 (20.12.2023) US

(71) Applicant: **APPLE INC.** [US/US]; One Apple Park Way, Cupertino, California 95014 (US).

(72) Inventor: **BUGLA, Lukas M.**; c/o Apple Inc., One Apple Park Way, Cupertino, California 95014 (US).

(74) Agent: **OMID, Randy** et al.; DLA Piper LLP US, 555 Mission Street, Suite 2400, San Francisco, California 94105-2933 (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, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MU, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, ME, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

(54) **Title:** USER INTERFACES AND METHODS FOR ENABLING A SECURITY MODE

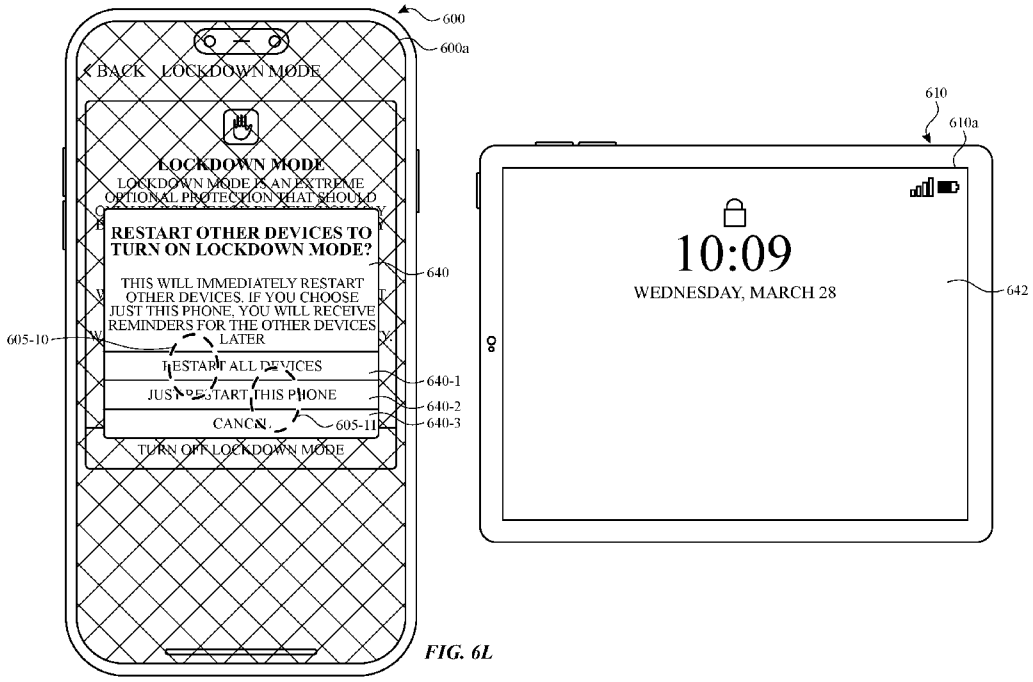


FIG. 6L

(57) **Abstract:** The present disclosure generally relates to enabling a security mode at one or more computer systems. In some embodiments, a security mode can be enabled at a single computer system logged into a user account. In some embodiments, a security mode can be enabled for a plurality of computer systems logged into the user account.

[Continued on next page]

WO 2024/253959 A1

Published:
— *with international search report (Art. 21(3))*

USER INTERFACES AND METHODS FOR ENABLING A SECURITY MODE

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims priority to U.S. Patent Application No. 18/391,414, entitled "USER INTERFACES AND METHODS FOR ENABLING A SECURITY MODE," filed December 20, 2023, and to U.S. Provisional Application No. 63/470,880, entitled "USER INTERFACES AND METHODS FOR ENABLING A SECURITY MODE," filed June 3, 2023. The content of each of which is hereby incorporated by reference in its entirety for all purposes.

FIELD

[0002] The present disclosure relates generally to computer user interfaces, and more specifically to techniques for enabling a security mode at one or more computer systems.

BACKGROUND

[0003] Computer systems can become compromised or experience a security threat. A security mode can be enabled to enhance security of a computer system.

BRIEF SUMMARY

[0004] Some techniques for enabling a security mode at one or more computer systems using electronic devices, however, are generally cumbersome and inefficient. For example, some existing techniques use a complex and time-consuming user interface, which may include multiple key presses or keystrokes. Existing techniques require more time than necessary, wasting user time and device energy. This latter consideration is particularly important in battery-operated devices.

[0005] Accordingly, the present technique provides electronic devices with faster, more efficient methods and interfaces for enabling a security mode at one or more computer systems. Such methods and interfaces optionally complement or replace other methods for enabling a security mode at one or more computer systems. Such methods and interfaces reduce the cognitive burden on a user and produce a more efficient human-machine interface. For battery-operated computing devices, such methods and interfaces conserve power and

increase the time between battery charges. Such methods and interfaces also improve security of computer systems.

[0006] Example methods are described herein. An example method includes, at a computer system that is in communication with a display generation component and one or more input devices: receiving, via the one or more input devices, a request to enable a security mode at the computer system, wherein the computer system is associated with a user account; and in response to receiving the request to enable the security mode at the computer system: in accordance with a determination that a set of one or more electronic devices other than the computer system are associated with the user account, displaying a respective user interface that includes one or more options for enabling the security mode at the set of one or more electronic devices and the computer system; and in accordance with a determination that a set of one or more electronic devices other than the computer system are not associated with the user account, enabling the security mode at the computer system without displaying the respective user interface that includes one or more options for enabling the security mode at the set of one or more electronic devices and the computer system.

[0007] Example non-transitory computer-readable storage media are described herein. An example non-transitory computer-readable storage medium stores one or more programs configured to be executed by one or more processors of a computer system that is in communication with a display generation component and one or more input devices, the one or more programs including instructions for: receiving, via the one or more input devices, a request to enable a security mode at the computer system, wherein the computer system is associated with a user account; and in response to receiving the request to enable the security mode at the computer system: in accordance with a determination that a set of one or more electronic devices other than the computer system are associated with the user account, displaying a respective user interface that includes one or more options for enabling the security mode at the set of one or more electronic devices and the computer system; and in accordance with a determination that a set of one or more electronic devices other than the computer system are not associated with the user account, enabling the security mode at the computer system without displaying the respective user interface that includes one or more options for enabling the security mode at the set of one or more electronic devices and the computer system.

[0008] Example transitory computer-readable storage media are described herein. An example transitory computer-readable storage medium stores one or more programs configured to be executed by one or more processors of a computer system that is in communication with a display generation component and one or more input devices, the one or more programs including instructions for: receiving, via the one or more input devices, a request to enable a security mode at the computer system, wherein the computer system is associated with a user account; and in response to receiving the request to enable the security mode at the computer system: in accordance with a determination that a set of one or more electronic devices other than the computer system are associated with the user account, displaying a respective user interface that includes one or more options for enabling the security mode at the set of one or more electronic devices and the computer system; and in accordance with a determination that a set of one or more electronic devices other than the computer system are not associated with the user account, enabling the security mode at the computer system without displaying the respective user interface that includes one or more options for enabling the security mode at the set of one or more electronic devices and the computer system.

[0009] Example computer systems are described herein. An example computer system is configured to communicate with a display generation component and one or more input devices and includes: one or more processors; and memory storing one or more programs configured to be executed by the one or more processors, the one or more programs including instructions for: receiving, via the one or more input devices, a request to enable a security mode at the computer system, wherein the computer system is associated with a user account; and in response to receiving the request to enable the security mode at the computer system: in accordance with a determination that a set of one or more electronic devices other than the computer system are associated with the user account, displaying a respective user interface that includes one or more options for enabling the security mode at the set of one or more electronic devices and the computer system; and in accordance with a determination that a set of one or more electronic devices other than the computer system are not associated with the user account, enabling the security mode at the computer system without displaying the respective user interface that includes one or more options for enabling the security mode at the set of one or more electronic devices and the computer system.

[0010] An example computer system is configured to communicate with a display generation component and one or more input devices and includes means for receiving, via the one or more input devices, a request to enable a security mode at the computer system, wherein the computer system is associated with a user account; and means for, in response to receiving the request to enable the security mode at the computer system: in accordance with a determination that a set of one or more electronic devices other than the computer system are associated with the user account, displaying a respective user interface that includes one or more options for enabling the security mode at the set of one or more electronic devices and the computer system; and in accordance with a determination that a set of one or more electronic devices other than the computer system are not associated with the user account, enabling the security mode at the computer system without displaying the respective user interface that includes one or more options for enabling the security mode at the set of one or more electronic devices and the computer system.

[0011] Example computer program products are described herein. An example computer program product includes one or more programs configured to be executed by one or more processors of a computer system that is in communication with a display generation component and one or more input devices, the one or more programs including instructions for: receiving, via the one or more input devices, a request to enable a security mode at the computer system, wherein the computer system is associated with a user account; and in response to receiving the request to enable the security mode at the computer system: in accordance with a determination that a set of one or more electronic devices other than the computer system are associated with the user account, displaying a respective user interface that includes one or more options for enabling the security mode at the set of one or more electronic devices and the computer system; and in accordance with a determination that a set of one or more electronic devices other than the computer system are not associated with the user account, enabling the security mode at the computer system without displaying the respective user interface that includes one or more options for enabling the security mode at the set of one or more electronic devices and the computer system.

[0012] Executable instructions for performing these functions are, optionally, included in a non-transitory computer-readable storage medium or other computer program product configured for execution by one or more processors. Executable instructions for performing

these functions are, optionally, included in a transitory computer-readable storage medium or other computer program product configured for execution by one or more processors.

[0013] Thus, devices are provided with faster, more efficient methods and interfaces for enabling a security mode at one or more computer systems, thereby increasing the effectiveness, efficiency, security, and user satisfaction with such devices. Such methods and interfaces may complement or replace other methods for enabling a security mode at one or more computer systems.

DESCRIPTION OF THE FIGURES

[0014] For a better understanding of the various described embodiments, reference should be made to the Description of Embodiments below, in conjunction with the following drawings in which like reference numerals refer to corresponding parts throughout the figures.

[0015] FIG. 1A is a block diagram illustrating a portable multifunction device with a touch-sensitive display in accordance with some embodiments.

[0016] FIG. 1B is a block diagram illustrating exemplary components for event handling in accordance with some embodiments.

[0017] FIG. 2 illustrates a portable multifunction device having a touch screen in accordance with some embodiments.

[0018] FIG. 3 is a block diagram of an exemplary multifunction device with a display and a touch-sensitive surface in accordance with some embodiments.

[0019] FIG. 4A illustrates an exemplary user interface for a menu of applications on a portable multifunction device in accordance with some embodiments.

[0020] FIG. 4B illustrates an exemplary user interface for a multifunction device with a touch-sensitive surface that is separate from the display in accordance with some embodiments.

[0021] FIG. 5A illustrates a personal electronic device in accordance with some embodiments.

[0022] FIG. 5B is a block diagram illustrating a personal electronic device in accordance with some embodiments.

[0023] FIGS. 6A-6AB illustrate exemplary user interfaces for enabling a security mode at one or more computer systems, in accordance with some embodiments.

[0024] FIG. 7 is a flow diagram illustrating a method for enabling a security mode at one or more computer systems, in accordance with some embodiments.

DESCRIPTION OF EMBODIMENTS

[0025] The following description sets forth exemplary methods, parameters, and the like. It should be recognized, however, that such description is not intended as a limitation on the scope of the present disclosure but is instead provided as a description of exemplary embodiments.

[0026] There is a need for electronic devices that provide efficient methods and interfaces for enabling a security mode at one or more computer systems. For example, computer systems are susceptible to malicious actors and security threats. Accordingly, there is a need to enhance security of such computer systems. Such techniques can reduce the cognitive burden on a user who enables a security mode at one or more computer systems, thereby enhancing productivity. Further, such techniques can reduce processor and battery power otherwise wasted on redundant user inputs.

[0027] Below, FIGS. 1A-1B, 2, 3, 4A-4B, and 5A-5B provide a description of exemplary devices for performing the techniques for enabling a security mode at one or more computer systems. FIGS. 6A-6AB illustrate exemplary user interfaces for enabling a security mode at one or more computer systems. FIG. 7 is a flow diagram illustrating methods of enabling a security mode at one or more computer systems, in accordance with some embodiments. The user interfaces in FIGS. 6A-6AB are used to illustrate the processes described below, including the processes in FIG. 7.

[0028] The processes described below enhance the operability of the devices and make the user-device interfaces more efficient (e.g., by helping the user to provide proper inputs and reducing user mistakes when operating/interacting with the device) through various techniques, including by providing improved visual feedback to the user, reducing the

number of inputs needed to perform an operation, providing additional control options without cluttering the user interface with additional displayed controls, performing an operation when a set of conditions has been met without requiring further user input, increasing security, and/or additional techniques. These techniques also reduce power usage and improve battery life of the device by enabling the user to use the device more quickly and efficiently.

[0029] In addition, in methods described herein where one or more steps are contingent upon one or more conditions having been met, it should be understood that the described method can be repeated in multiple repetitions so that over the course of the repetitions all of the conditions upon which steps in the method are contingent have been met in different repetitions of the method. For example, if a method requires performing a first step if a condition is satisfied, and a second step if the condition is not satisfied, then a person of ordinary skill would appreciate that the claimed steps are repeated until the condition has been both satisfied and not satisfied, in no particular order. Thus, a method described with one or more steps that are contingent upon one or more conditions having been met could be rewritten as a method that is repeated until each of the conditions described in the method has been met. This, however, is not required of system or computer readable medium claims where the system or computer readable medium contains instructions for performing the contingent operations based on the satisfaction of the corresponding one or more conditions and thus is capable of determining whether the contingency has or has not been satisfied without explicitly repeating steps of a method until all of the conditions upon which steps in the method are contingent have been met. A person having ordinary skill in the art would also understand that, similar to a method with contingent steps, a system or computer readable storage medium can repeat the steps of a method as many times as are needed to ensure that all of the contingent steps have been performed.

[0030] Although the following description uses terms “first,” “second,” etc. to describe various elements, these elements should not be limited by the terms. In some embodiments, these terms are used to distinguish one element from another. For example, a first touch could be termed a second touch, and, similarly, a second touch could be termed a first touch, without departing from the scope of the various described embodiments. In some embodiments, the first touch and the second touch are two separate references to the same

touch. In some embodiments, the first touch and the second touch are both touches, but they are not the same touch.

[0031] The terminology used in the description of the various described embodiments herein is for the purpose of describing particular embodiments only and is not intended to be limiting. As used in the description of the various described embodiments and the appended claims, the singular forms "a," "an," and "the" are intended to include the plural forms as well, unless the context clearly indicates otherwise. It will also be understood that the term "and/or" as used herein refers to and encompasses any and all possible combinations of one or more of the associated listed items. It will be further understood that the terms "includes," "including," "comprises," and/or "comprising," when used in this specification, specify the presence of stated features, integers, steps, operations, elements, and/or components, but do not preclude the presence or addition of one or more other features, integers, steps, operations, elements, components, and/or groups thereof.

[0032] The term "if" is, optionally, construed to mean "when" or "upon" or "in response to determining" or "in response to detecting," depending on the context. Similarly, the phrase "if it is determined" or "if [a stated condition or event] is detected" is, optionally, construed to mean "upon determining" or "in response to determining" or "upon detecting [the stated condition or event]" or "in response to detecting [the stated condition or event]," depending on the context.

[0033] Embodiments of electronic devices, user interfaces for such devices, and associated processes for using such devices are described. In some embodiments, the device is a portable communications device, such as a mobile telephone, that also contains other functions, such as PDA and/or music player functions. Exemplary embodiments of portable multifunction devices include, without limitation, the iPhone®, iPod Touch®, and iPad® devices from Apple Inc. of Cupertino, California. Other portable electronic devices, such as laptops or tablet computers with touch-sensitive surfaces (e.g., touch screen displays and/or touchpads), are, optionally, used. It should also be understood that, in some embodiments, the device is not a portable communications device, but is a desktop computer with a touch-sensitive surface (e.g., a touch screen display and/or a touchpad). In some embodiments, the electronic device is a computer system that is in communication (e.g., via wireless communication, via wired communication) with a display generation component (e.g., a display device such as a head-mounted display (HMD), a display, a projector, a touch-

sensitive display, or other device or component that presents visual content to a user, for example on or in the display generation component itself or produced from the display generation component and visible elsewhere). The display generation component is configured to provide visual output, such as display via a CRT display, display via an LED display, or display via image projection. In some embodiments, the display generation component is integrated with the computer system. In some embodiments, the display generation component is separate from the computer system. As used herein, "displaying" content includes causing to display the content (e.g., video data rendered or decoded by display controller 156) by transmitting, via a wired or wireless connection, data (e.g., image data or video data) to an integrated or external display generation component to visually produce the content.

[0034] In the discussion that follows, an electronic device that includes a display and a touch-sensitive surface is described. It should be understood, however, that the electronic device optionally includes one or more other physical user-interface devices, such as a physical keyboard, a mouse, and/or a joystick.

[0035] The device typically supports a variety of applications, such as one or more of the following: a drawing application, a presentation application, a word processing application, a website creation application, a disk authoring application, a spreadsheet application, a gaming application, a telephone application, a video conferencing application, an e-mail application, an instant messaging application, a workout support application, a photo management application, a digital camera application, a digital video camera application, a web browsing application, a digital music player application, and/or a digital video player application.

[0036] The various applications that are executed on the device optionally use at least one common physical user-interface device, such as the touch-sensitive surface. One or more functions of the touch-sensitive surface as well as corresponding information displayed on the device are, optionally, adjusted and/or varied from one application to the next and/or within a respective application. In this way, a common physical architecture (such as the touch-sensitive surface) of the device optionally supports the variety of applications with user interfaces that are intuitive and transparent to the user.

[0037] Attention is now directed toward embodiments of portable devices with touch-sensitive displays. FIG. 1A is a block diagram illustrating portable multifunction device 100

with touch-sensitive display system 112 in accordance with some embodiments. Touch-sensitive display 112 is sometimes called a "touch screen" for convenience and is sometimes known as or called a "touch-sensitive display system." Device 100 includes memory 102 (which optionally includes one or more computer-readable storage mediums), memory controller 122, one or more processing units (CPUs) 120, peripherals interface 118, RF circuitry 108, audio circuitry 110, speaker 111, microphone 113, input/output (I/O) subsystem 106, other input control devices 116, and external port 124. Device 100 optionally includes one or more optical sensors 164. Device 100 optionally includes one or more contact intensity sensors 165 for detecting intensity of contacts on device 100 (e.g., a touch-sensitive surface such as touch-sensitive display system 112 of device 100). Device 100 optionally includes one or more tactile output generators 167 for generating tactile outputs on device 100 (e.g., generating tactile outputs on a touch-sensitive surface such as touch-sensitive display system 112 of device 100 or touchpad 355 of device 300). These components optionally communicate over one or more communication buses or signal lines 103.

[0038] As used in the specification and claims, the term "intensity" of a contact on a touch-sensitive surface refers to the force or pressure (force per unit area) of a contact (e.g., a finger contact) on the touch-sensitive surface, or to a substitute (proxy) for the force or pressure of a contact on the touch-sensitive surface. The intensity of a contact has a range of values that includes at least four distinct values and more typically includes hundreds of distinct values (e.g., at least 256). Intensity of a contact is, optionally, determined (or measured) using various approaches and various sensors or combinations of sensors. For example, one or more force sensors underneath or adjacent to the touch-sensitive surface are, optionally, used to measure force at various points on the touch-sensitive surface. In some implementations, force measurements from multiple force sensors are combined (e.g., a weighted average) to determine an estimated force of a contact. Similarly, a pressure-sensitive tip of a stylus is, optionally, used to determine a pressure of the stylus on the touch-sensitive surface. Alternatively, the size of the contact area detected on the touch-sensitive surface and/or changes thereto, the capacitance of the touch-sensitive surface proximate to the contact and/or changes thereto, and/or the resistance of the touch-sensitive surface proximate to the contact and/or changes thereto are, optionally, used as a substitute for the force or pressure of the contact on the touch-sensitive surface. In some implementations, the substitute measurements for contact force or pressure are used directly to determine whether

an intensity threshold has been exceeded (e.g., the intensity threshold is described in units corresponding to the substitute measurements). In some implementations, the substitute measurements for contact force or pressure are converted to an estimated force or pressure, and the estimated force or pressure is used to determine whether an intensity threshold has been exceeded (e.g., the intensity threshold is a pressure threshold measured in units of pressure). Using the intensity of a contact as an attribute of a user input allows for user access to additional device functionality that may otherwise not be accessible by the user on a reduced-size device with limited real estate for displaying affordances (e.g., on a touch-sensitive display) and/or receiving user input (e.g., via a touch-sensitive display, a touch-sensitive surface, or a physical/mechanical control such as a knob or a button).

[0039] As used in the specification and claims, the term "tactile output" refers to physical displacement of a device relative to a previous position of the device, physical displacement of a component (e.g., a touch-sensitive surface) of a device relative to another component (e.g., housing) of the device, or displacement of the component relative to a center of mass of the device that will be detected by a user with the user's sense of touch. For example, in situations where the device or the component of the device is in contact with a surface of a user that is sensitive to touch (e.g., a finger, palm, or other part of a user's hand), the tactile output generated by the physical displacement will be interpreted by the user as a tactile sensation corresponding to a perceived change in physical characteristics of the device or the component of the device. For example, movement of a touch-sensitive surface (e.g., a touch-sensitive display or trackpad) is, optionally, interpreted by the user as a "down click" or "up click" of a physical actuator button. In some cases, a user will feel a tactile sensation such as an "down click" or "up click" even when there is no movement of a physical actuator button associated with the touch-sensitive surface that is physically pressed (e.g., displaced) by the user's movements. As another example, movement of the touch-sensitive surface is, optionally, interpreted or sensed by the user as "roughness" of the touch-sensitive surface, even when there is no change in smoothness of the touch-sensitive surface. While such interpretations of touch by a user will be subject to the individualized sensory perceptions of the user, there are many sensory perceptions of touch that are common to a large majority of users. Thus, when a tactile output is described as corresponding to a particular sensory perception of a user (e.g., an "up click," a "down click," "roughness"), unless otherwise stated, the generated tactile output corresponds to physical displacement of the device or a

component thereof that will generate the described sensory perception for a typical (or average) user.

[0040] It should be appreciated that device 100 is only one example of a portable multifunction device, and that device 100 optionally has more or fewer components than shown, optionally combines two or more components, or optionally has a different configuration or arrangement of the components. The various components shown in FIG. 1A are implemented in hardware, software, or a combination of both hardware and software, including one or more signal processing and/or application-specific integrated circuits.

[0041] Memory 102 optionally includes high-speed random access memory and optionally also includes non-volatile memory, such as one or more magnetic disk storage devices, flash memory devices, or other non-volatile solid-state memory devices. Memory controller 122 optionally controls access to memory 102 by other components of device 100.

[0042] Peripherals interface 118 can be used to couple input and output peripherals of the device to CPU 120 and memory 102. The one or more processors 120 run or execute various software programs (such as computer programs (e.g., including instructions)) and/or sets of instructions stored in memory 102 to perform various functions for device 100 and to process data. In some embodiments, peripherals interface 118, CPU 120, and memory controller 122 are, optionally, implemented on a single chip, such as chip 104. In some other embodiments, they are, optionally, implemented on separate chips.

[0043] RF (radio frequency) circuitry 108 receives and sends RF signals, also called electromagnetic signals. RF circuitry 108 converts electrical signals to/from electromagnetic signals and communicates with communications networks and other communications devices via the electromagnetic signals. RF circuitry 108 optionally includes well-known circuitry for performing these functions, including but not limited to an antenna system, an RF transceiver, one or more amplifiers, a tuner, one or more oscillators, a digital signal processor, a CODEC chipset, a subscriber identity module (SIM) card, memory, and so forth. RF circuitry 108 optionally communicates with networks, such as the Internet, also referred to as the World Wide Web (WWW), an intranet and/or a wireless network, such as a cellular telephone network, a wireless local area network (LAN) and/or a metropolitan area network (MAN), and other devices by wireless communication. The RF circuitry 108 optionally includes well-known circuitry for detecting near field communication (NFC) fields, such as

by a short-range communication radio. The wireless communication optionally uses any of a plurality of communications standards, protocols, and technologies, including but not limited to Global System for Mobile Communications (GSM), Enhanced Data GSM Environment (EDGE), high-speed downlink packet access (HSDPA), high-speed uplink packet access (HSUPA), Evolution, Data-Only (EV-DO), HSPA, HSPA+, Dual-Cell HSPA (DC-HSPDA), long term evolution (LTE), near field communication (NFC), wideband code division multiple access (W-CDMA), code division multiple access (CDMA), time division multiple access (TDMA), Bluetooth, Bluetooth Low Energy (BTLE), Wireless Fidelity (Wi-Fi) (e.g., IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, and/or IEEE 802.11ac), voice over Internet Protocol (VoIP), Wi-MAX, a protocol for e-mail (e.g., Internet message access protocol (IMAP) and/or post office protocol (POP)), instant messaging (e.g., extensible messaging and presence protocol (XMPP), Session Initiation Protocol for Instant Messaging and Presence Leveraging Extensions (SIMPLE), Instant Messaging and Presence Service (IMPS)), and/or Short Message Service (SMS), or any other suitable communication protocol, including communication protocols not yet developed as of the filing date of this document.

[0044] Audio circuitry 110, speaker 111, and microphone 113 provide an audio interface between a user and device 100. Audio circuitry 110 receives audio data from peripherals interface 118, converts the audio data to an electrical signal, and transmits the electrical signal to speaker 111. Speaker 111 converts the electrical signal to human-audible sound waves. Audio circuitry 110 also receives electrical signals converted by microphone 113 from sound waves. Audio circuitry 110 converts the electrical signal to audio data and transmits the audio data to peripherals interface 118 for processing. Audio data is, optionally, retrieved from and/or transmitted to memory 102 and/or RF circuitry 108 by peripherals interface 118. In some embodiments, audio circuitry 110 also includes a headset jack (e.g., 212, FIG. 2). The headset jack provides an interface between audio circuitry 110 and removable audio input/output peripherals, such as output-only headphones or a headset with both output (e.g., a headphone for one or both ears) and input (e.g., a microphone).

[0045] I/O subsystem 106 couples input/output peripherals on device 100, such as touch screen 112 and other input control devices 116, to peripherals interface 118. I/O subsystem 106 optionally includes display controller 156, optical sensor controller 158, depth camera controller 169, intensity sensor controller 159, haptic feedback controller 161, and one or

more input controllers 160 for other input or control devices. The one or more input controllers 160 receive/send electrical signals from/to other input control devices 116. The other input control devices 116 optionally include physical buttons (e.g., push buttons, rocker buttons, etc.), dials, slider switches, joysticks, click wheels, and so forth. In some embodiments, input controller(s) 160 are, optionally, coupled to any (or none) of the following: a keyboard, an infrared port, a USB port, and a pointer device such as a mouse. The one or more buttons (e.g., 208, FIG. 2) optionally include an up/down button for volume control of speaker 111 and/or microphone 113. The one or more buttons optionally include a push button (e.g., 206, FIG. 2). In some embodiments, the electronic device is a computer system that is in communication (e.g., via wireless communication, via wired communication) with one or more input devices. In some embodiments, the one or more input devices include a touch-sensitive surface (e.g., a trackpad, as part of a touch-sensitive display). In some embodiments, the one or more input devices include one or more camera sensors (e.g., one or more optical sensors 164 and/or one or more depth camera sensors 175), such as for tracking a user's gestures (e.g., hand gestures and/or air gestures) as input. In some embodiments, the one or more input devices are integrated with the computer system. In some embodiments, the one or more input devices are separate from the computer system. In some embodiments, an air gesture is a gesture that is detected without the user touching an input element that is part of the device (or independently of an input element that is a part of the device) and is based on detected motion of a portion of the user's body through the air including motion of the user's body relative to an absolute reference (e.g., an angle of the user's arm relative to the ground or a distance of the user's hand relative to the ground), relative to another portion of the user's body (e.g., movement of a hand of the user relative to a shoulder of the user, movement of one hand of the user relative to another hand of the user, and/or movement of a finger of the user relative to another finger or portion of a hand of the user), and/or absolute motion of a portion of the user's body (e.g., a tap gesture that includes movement of a hand in a predetermined pose by a predetermined amount and/or speed, or a shake gesture that includes a predetermined speed or amount of rotation of a portion of the user's body).

[0046] A quick press of the push button optionally disengages a lock of touch screen 112 or optionally begins a process that uses gestures on the touch screen to unlock the device, as described in U.S. Patent Application 11/322,549, "Unlocking a Device by Performing Gestures on an Unlock Image," filed December 23, 2005, U.S. Pat. No. 7,657,849, which is

hereby incorporated by reference in its entirety. A longer press of the push button (e.g., 206) optionally turns power to device 100 on or off. The functionality of one or more of the buttons are, optionally, user-customizable. Touch screen 112 is used to implement virtual or soft buttons and one or more soft keyboards.

[0047] Touch-sensitive display 112 provides an input interface and an output interface between the device and a user. Display controller 156 receives and/or sends electrical signals from/to touch screen 112. Touch screen 112 displays visual output to the user. The visual output optionally includes graphics, text, icons, video, and any combination thereof (collectively termed "graphics"). In some embodiments, some or all of the visual output optionally corresponds to user-interface objects.

[0048] Touch screen 112 has a touch-sensitive surface, sensor, or set of sensors that accepts input from the user based on haptic and/or tactile contact. Touch screen 112 and display controller 156 (along with any associated modules and/or sets of instructions in memory 102) detect contact (and any movement or breaking of the contact) on touch screen 112 and convert the detected contact into interaction with user-interface objects (e.g., one or more soft keys, icons, web pages, or images) that are displayed on touch screen 112. In an exemplary embodiment, a point of contact between touch screen 112 and the user corresponds to a finger of the user.

[0049] Touch screen 112 optionally uses LCD (liquid crystal display) technology, LPD (light emitting polymer display) technology, or LED (light emitting diode) technology, although other display technologies are used in other embodiments. Touch screen 112 and display controller 156 optionally detect contact and any movement or breaking thereof using any of a plurality of touch sensing technologies now known or later developed, including but not limited to capacitive, resistive, infrared, and surface acoustic wave technologies, as well as other proximity sensor arrays or other elements for determining one or more points of contact with touch screen 112. In an exemplary embodiment, projected mutual capacitance sensing technology is used, such as that found in the iPhone® and iPod Touch® from Apple Inc. of Cupertino, California.

[0050] A touch-sensitive display in some embodiments of touch screen 112 is, optionally, analogous to the multi-touch sensitive touchpads described in the following U.S. Patents: 6,323,846 (Westerman et al.), 6,570,557 (Westerman et al.), and/or 6,677,932 (Westerman),

and/or U.S. Patent Publication 2002/0015024A1, each of which is hereby incorporated by reference in its entirety. However, touch screen 112 displays visual output from device 100, whereas touch-sensitive touchpads do not provide visual output.

[0051] A touch-sensitive display in some embodiments of touch screen 112 is described in the following applications: (1) U.S. Patent Application No. 11/381,313, "Multipoint Touch Surface Controller," filed May 2, 2006; (2) U.S. Patent Application No. 10/840,862, "Multipoint Touchscreen," filed May 6, 2004; (3) U.S. Patent Application No. 10/903,964, "Gestures For Touch Sensitive Input Devices," filed July 30, 2004; (4) U.S. Patent Application No. 11/048,264, "Gestures For Touch Sensitive Input Devices," filed January 31, 2005; (5) U.S. Patent Application No. 11/038,590, "Mode-Based Graphical User Interfaces For Touch Sensitive Input Devices," filed January 18, 2005; (6) U.S. Patent Application No. 11/228,758, "Virtual Input Device Placement On A Touch Screen User Interface," filed September 16, 2005; (7) U.S. Patent Application No. 11/228,700, "Operation Of A Computer With A Touch Screen Interface," filed September 16, 2005; (8) U.S. Patent Application No. 11/228,737, "Activating Virtual Keys Of A Touch-Screen Virtual Keyboard," filed September 16, 2005; and (9) U.S. Patent Application No. 11/367,749, "Multi-Functional Hand-Held Device," filed March 3, 2006. All of these applications are incorporated by reference herein in their entirety.

[0052] Touch screen 112 optionally has a video resolution in excess of 100 dpi. In some embodiments, the touch screen has a video resolution of approximately 160 dpi. The user optionally makes contact with touch screen 112 using any suitable object or appendage, such as a stylus, a finger, and so forth. In some embodiments, the user interface is designed to work primarily with finger-based contacts and gestures, which can be less precise than stylus-based input due to the larger area of contact of a finger on the touch screen. In some embodiments, the device translates the rough finger-based input into a precise pointer/cursor position or command for performing the actions desired by the user.

[0053] In some embodiments, in addition to the touch screen, device 100 optionally includes a touchpad for activating or deactivating particular functions. In some embodiments, the touchpad is a touch-sensitive area of the device that, unlike the touch screen, does not display visual output. The touchpad is, optionally, a touch-sensitive surface that is separate from touch screen 112 or an extension of the touch-sensitive surface formed by the touch screen.

[0054] Device 100 also includes power system 162 for powering the various components. Power system 162 optionally includes a power management system, one or more power sources (e.g., battery, alternating current (AC)), a recharging system, a power failure detection circuit, a power converter or inverter, a power status indicator (e.g., a light-emitting diode (LED)) and any other components associated with the generation, management and distribution of power in portable devices.

[0055] Device 100 optionally also includes one or more optical sensors 164. FIG. 1A shows an optical sensor coupled to optical sensor controller 158 in I/O subsystem 106. Optical sensor 164 optionally includes charge-coupled device (CCD) or complementary metal-oxide semiconductor (CMOS) phototransistors. Optical sensor 164 receives light from the environment, projected through one or more lenses, and converts the light to data representing an image. In conjunction with imaging module 143 (also called a camera module), optical sensor 164 optionally captures still images or video. In some embodiments, an optical sensor is located on the back of device 100, opposite touch screen display 112 on the front of the device so that the touch screen display is enabled for use as a viewfinder for still and/or video image acquisition. In some embodiments, an optical sensor is located on the front of the device so that the user's image is, optionally, obtained for video conferencing while the user views the other video conference participants on the touch screen display. In some embodiments, the position of optical sensor 164 can be changed by the user (e.g., by rotating the lens and the sensor in the device housing) so that a single optical sensor 164 is used along with the touch screen display for both video conferencing and still and/or video image acquisition.

[0056] Device 100 optionally also includes one or more depth camera sensors 175. FIG. 1A shows a depth camera sensor coupled to depth camera controller 169 in I/O subsystem 106. Depth camera sensor 175 receives data from the environment to create a three dimensional model of an object (e.g., a face) within a scene from a viewpoint (e.g., a depth camera sensor). In some embodiments, in conjunction with imaging module 143 (also called a camera module), depth camera sensor 175 is optionally used to determine a depth map of different portions of an image captured by the imaging module 143. In some embodiments, a depth camera sensor is located on the front of device 100 so that the user's image with depth information is, optionally, obtained for video conferencing while the user views the other video conference participants on the touch screen display and to capture

selfies with depth map data. In some embodiments, the depth camera sensor 175 is located on the back of device, or on the back and the front of the device 100. In some embodiments, the position of depth camera sensor 175 can be changed by the user (e.g., by rotating the lens and the sensor in the device housing) so that a depth camera sensor 175 is used along with the touch screen display for both video conferencing and still and/or video image acquisition.

[0057] Device 100 optionally also includes one or more contact intensity sensors 165. FIG. 1A shows a contact intensity sensor coupled to intensity sensor controller 159 in I/O subsystem 106. Contact intensity sensor 165 optionally includes one or more piezoresistive strain gauges, capacitive force sensors, electric force sensors, piezoelectric force sensors, optical force sensors, capacitive touch-sensitive surfaces, or other intensity sensors (e.g., sensors used to measure the force (or pressure) of a contact on a touch-sensitive surface). Contact intensity sensor 165 receives contact intensity information (e.g., pressure information or a proxy for pressure information) from the environment. In some embodiments, at least one contact intensity sensor is collocated with, or proximate to, a touch-sensitive surface (e.g., touch-sensitive display system 112). In some embodiments, at least one contact intensity sensor is located on the back of device 100, opposite touch screen display 112, which is located on the front of device 100.

[0058] Device 100 optionally also includes one or more proximity sensors 166. FIG. 1A shows proximity sensor 166 coupled to peripherals interface 118. Alternately, proximity sensor 166 is, optionally, coupled to input controller 160 in I/O subsystem 106. Proximity sensor 166 optionally performs as described in U.S. Patent Application Nos. 11/241,839, "Proximity Detector In Handheld Device"; 11/240,788, "Proximity Detector In Handheld Device"; 11/620,702, "Using Ambient Light Sensor To Augment Proximity Sensor Output"; 11/586,862, "Automated Response To And Sensing Of User Activity In Portable Devices"; and 11/638,251, "Methods And Systems For Automatic Configuration Of Peripherals," which are hereby incorporated by reference in their entirety. In some embodiments, the proximity sensor turns off and disables touch screen 112 when the multifunction device is placed near the user's ear (e.g., when the user is making a phone call).

[0059] Device 100 optionally also includes one or more tactile output generators 167. FIG. 1A shows a tactile output generator coupled to haptic feedback controller 161 in I/O subsystem 106. Tactile output generator 167 optionally includes one or more electroacoustic devices such as speakers or other audio components and/or electromechanical devices that

convert energy into linear motion such as a motor, solenoid, electroactive polymer, piezoelectric actuator, electrostatic actuator, or other tactile output generating component (e.g., a component that converts electrical signals into tactile outputs on the device). Contact intensity sensor 165 receives tactile feedback generation instructions from haptic feedback module 133 and generates tactile outputs on device 100 that are capable of being sensed by a user of device 100. In some embodiments, at least one tactile output generator is collocated with, or proximate to, a touch-sensitive surface (e.g., touch-sensitive display system 112) and, optionally, generates a tactile output by moving the touch-sensitive surface vertically (e.g., in/out of a surface of device 100) or laterally (e.g., back and forth in the same plane as a surface of device 100). In some embodiments, at least one tactile output generator sensor is located on the back of device 100, opposite touch screen display 112, which is located on the front of device 100.

[0060] Device 100 optionally also includes one or more accelerometers 168. FIG. 1A shows accelerometer 168 coupled to peripherals interface 118. Alternately, accelerometer 168 is, optionally, coupled to an input controller 160 in I/O subsystem 106. Accelerometer 168 optionally performs as described in U.S. Patent Publication No. 20050190059, "Acceleration-based Theft Detection System for Portable Electronic Devices," and U.S. Patent Publication No. 20060017692, "Methods And Apparatuses For Operating A Portable Device Based On An Accelerometer," both of which are incorporated by reference herein in their entirety. In some embodiments, information is displayed on the touch screen display in a portrait view or a landscape view based on an analysis of data received from the one or more accelerometers. Device 100 optionally includes, in addition to accelerometer(s) 168, a magnetometer and a GPS (or GLONASS or other global navigation system) receiver for obtaining information concerning the location and orientation (e.g., portrait or landscape) of device 100.

[0061] In some embodiments, the software components stored in memory 102 include operating system 126, communication module (or set of instructions) 128, contact/motion module (or set of instructions) 130, graphics module (or set of instructions) 132, text input module (or set of instructions) 134, Global Positioning System (GPS) module (or set of instructions) 135, and applications (or sets of instructions) 136. Furthermore, in some embodiments, memory 102 (FIG. 1A) or 370 (FIG. 3) stores device/global internal state 157, as shown in FIGS. 1A and 3. Device/global internal state 157 includes one or more of: active

application state, indicating which applications, if any, are currently active; display state, indicating what applications, views or other information occupy various regions of touch screen display 112; sensor state, including information obtained from the device's various sensors and input control devices 116; and location information concerning the device's location and/or attitude.

[0062] Operating system 126 (e.g., Darwin, RTXC, LINUX, UNIX, OS X, iOS, WINDOWS, or an embedded operating system such as VxWorks) includes various software components and/or drivers for controlling and managing general system tasks (e.g., memory management, storage device control, power management, etc.) and facilitates communication between various hardware and software components.

[0063] Communication module 128 facilitates communication with other devices over one or more external ports 124 and also includes various software components for handling data received by RF circuitry 108 and/or external port 124. External port 124 (e.g., Universal Serial Bus (USB), FIREWIRE, etc.) is adapted for coupling directly to other devices or indirectly over a network (e.g., the Internet, wireless LAN, etc.). In some embodiments, the external port is a multi-pin (e.g., 30-pin) connector that is the same as, or similar to and/or compatible with, the 30-pin connector used on iPod® (trademark of Apple Inc.) devices.

[0064] Contact/motion module 130 optionally detects contact with touch screen 112 (in conjunction with display controller 156) and other touch-sensitive devices (e.g., a touchpad or physical click wheel). Contact/motion module 130 includes various software components for performing various operations related to detection of contact, such as determining if contact has occurred (e.g., detecting a finger-down event), determining an intensity of the contact (e.g., the force or pressure of the contact or a substitute for the force or pressure of the contact), determining if there is movement of the contact and tracking the movement across the touch-sensitive surface (e.g., detecting one or more finger-dragging events), and determining if the contact has ceased (e.g., detecting a finger-up event or a break in contact). Contact/motion module 130 receives contact data from the touch-sensitive surface. Determining movement of the point of contact, which is represented by a series of contact data, optionally includes determining speed (magnitude), velocity (magnitude and direction), and/or an acceleration (a change in magnitude and/or direction) of the point of contact. These operations are, optionally, applied to single contacts (e.g., one finger contacts) or to multiple

simultaneous contacts (e.g., "multitouch"/multiple finger contacts). In some embodiments, contact/motion module 130 and display controller 156 detect contact on a touchpad.

[0065] In some embodiments, contact/motion module 130 uses a set of one or more intensity thresholds to determine whether an operation has been performed by a user (e.g., to determine whether a user has "clicked" on an icon). In some embodiments, at least a subset of the intensity thresholds are determined in accordance with software parameters (e.g., the intensity thresholds are not determined by the activation thresholds of particular physical actuators and can be adjusted without changing the physical hardware of device 100). For example, a mouse "click" threshold of a trackpad or touch screen display can be set to any of a large range of predefined threshold values without changing the trackpad or touch screen display hardware. Additionally, in some implementations, a user of the device is provided with software settings for adjusting one or more of the set of intensity thresholds (e.g., by adjusting individual intensity thresholds and/or by adjusting a plurality of intensity thresholds at once with a system-level click "intensity" parameter).

[0066] Contact/motion module 130 optionally detects a gesture input by a user. Different gestures on the touch-sensitive surface have different contact patterns (e.g., different motions, timings, and/or intensities of detected contacts). Thus, a gesture is, optionally, detected by detecting a particular contact pattern. For example, detecting a finger tap gesture includes detecting a finger-down event followed by detecting a finger-up (liftoff) event at the same position (or substantially the same position) as the finger-down event (e.g., at the position of an icon). As another example, detecting a finger swipe gesture on the touch-sensitive surface includes detecting a finger-down event followed by detecting one or more finger-dragging events, and subsequently followed by detecting a finger-up (liftoff) event.

[0067] Graphics module 132 includes various known software components for rendering and displaying graphics on touch screen 112 or other display, including components for changing the visual impact (e.g., brightness, transparency, saturation, contrast, or other visual property) of graphics that are displayed. As used herein, the term "graphics" includes any object that can be displayed to a user, including, without limitation, text, web pages, icons (such as user-interface objects including soft keys), digital images, videos, animations, and the like.

[0068] In some embodiments, graphics module 132 stores data representing graphics to be used. Each graphic is, optionally, assigned a corresponding code. Graphics module 132 receives, from applications etc., one or more codes specifying graphics to be displayed along with, if necessary, coordinate data and other graphic property data, and then generates screen image data to output to display controller 156.

[0069] Haptic feedback module 133 includes various software components for generating instructions used by tactile output generator(s) 167 to produce tactile outputs at one or more locations on device 100 in response to user interactions with device 100.

[0070] Text input module 134, which is, optionally, a component of graphics module 132, provides soft keyboards for entering text in various applications (e.g., contacts module 137, e-mail client module 140, IM module 141, browser module 147, and any other application that needs text input).

[0071] GPS module 135 determines the location of the device and provides this information for use in various applications (e.g., to telephone module 138 for use in location-based dialing; to camera module 143 as picture/video metadata; and to applications that provide location-based services such as weather widgets, local yellow page widgets, and map/navigation widgets).

[0072] Applications 136 optionally include the following modules (or sets of instructions), or a subset or superset thereof:

- Contacts module 137 (sometimes called an address book or contact list);
- Telephone module 138;
- Video conference module 139;
- E-mail client module 140;
- Instant messaging (IM) module 141;
- Workout support module 142;
- Camera module 143 for still and/or video images;

- Image management module 144;
- Video player module;
- Music player module;
- Browser module 147;
- Calendar module 148;
- Widget modules 149, which optionally include one or more of: weather widget 149-1, stocks widget 149-2, calculator widget 149-3, alarm clock widget 149-4, dictionary widget 149-5, and other widgets obtained by the user, as well as user-created widgets 149-6;
- Widget creator module 150 for making user-created widgets 149-6;
- Search module 151;
- Video and music player module 152, which merges video player module and music player module;
- Notes module 153;
- Map module 154; and/or
- Online video module 155.

[0073] Examples of other applications 136 that are, optionally, stored in memory 102 include other word processing applications, other image editing applications, drawing applications, presentation applications, JAVA-enabled applications, encryption, digital rights management, voice recognition, and voice replication.

[0074] In conjunction with touch screen 112, display controller 156, contact/motion module 130, graphics module 132, and text input module 134, contacts module 137 are, optionally, used to manage an address book or contact list (e.g., stored in application internal state 192 of contacts module 137 in memory 102 or memory 370), including: adding name(s) to the address book; deleting name(s) from the address book; associating telephone number(s), e-mail address(es), physical address(es) or other information with a name;

associating an image with a name; categorizing and sorting names; providing telephone numbers or e-mail addresses to initiate and/or facilitate communications by telephone module 138, video conference module 139, e-mail client module 140, or IM module 141; and so forth.

[0075] In conjunction with RF circuitry 108, audio circuitry 110, speaker 111, microphone 113, touch screen 112, display controller 156, contact/motion module 130, graphics module 132, and text input module 134, telephone module 138 are optionally, used to enter a sequence of characters corresponding to a telephone number, access one or more telephone numbers in contacts module 137, modify a telephone number that has been entered, dial a respective telephone number, conduct a conversation, and disconnect or hang up when the conversation is completed. As noted above, the wireless communication optionally uses any of a plurality of communications standards, protocols, and technologies.

[0076] In conjunction with RF circuitry 108, audio circuitry 110, speaker 111, microphone 113, touch screen 112, display controller 156, optical sensor 164, optical sensor controller 158, contact/motion module 130, graphics module 132, text input module 134, contacts module 137, and telephone module 138, video conference module 139 includes executable instructions to initiate, conduct, and terminate a video conference between a user and one or more other participants in accordance with user instructions.

[0077] In conjunction with RF circuitry 108, touch screen 112, display controller 156, contact/motion module 130, graphics module 132, and text input module 134, e-mail client module 140 includes executable instructions to create, send, receive, and manage e-mail in response to user instructions. In conjunction with image management module 144, e-mail client module 140 makes it very easy to create and send e-mails with still or video images taken with camera module 143.

[0078] In conjunction with RF circuitry 108, touch screen 112, display controller 156, contact/motion module 130, graphics module 132, and text input module 134, the instant messaging module 141 includes executable instructions to enter a sequence of characters corresponding to an instant message, to modify previously entered characters, to transmit a respective instant message (for example, using a Short Message Service (SMS) or Multimedia Message Service (MMS) protocol for telephony-based instant messages or using XMPP, SIMPLE, or IMPS for Internet-based instant messages), to receive instant messages,

and to view received instant messages. In some embodiments, transmitted and/or received instant messages optionally include graphics, photos, audio files, video files and/or other attachments as are supported in an MMS and/or an Enhanced Messaging Service (EMS). As used herein, "instant messaging" refers to both telephony-based messages (e.g., messages sent using SMS or MMS) and Internet-based messages (e.g., messages sent using XMPP, SIMPLE, or IMPS).

[0079] In conjunction with RF circuitry 108, touch screen 112, display controller 156, contact/motion module 130, graphics module 132, text input module 134, GPS module 135, map module 154, and music player module, workout support module 142 includes executable instructions to create workouts (e.g., with time, distance, and/or calorie burning goals); communicate with workout sensors (sports devices); receive workout sensor data; calibrate sensors used to monitor a workout; select and play music for a workout; and display, store, and transmit workout data.

[0080] In conjunction with touch screen 112, display controller 156, optical sensor(s) 164, optical sensor controller 158, contact/motion module 130, graphics module 132, and image management module 144, camera module 143 includes executable instructions to capture still images or video (including a video stream) and store them into memory 102, modify characteristics of a still image or video, or delete a still image or video from memory 102.

[0081] In conjunction with touch screen 112, display controller 156, contact/motion module 130, graphics module 132, text input module 134, and camera module 143, image management module 144 includes executable instructions to arrange, modify (e.g., edit), or otherwise manipulate, label, delete, present (e.g., in a digital slide show or album), and store still and/or video images.

[0082] In conjunction with RF circuitry 108, touch screen 112, display controller 156, contact/motion module 130, graphics module 132, and text input module 134, browser module 147 includes executable instructions to browse the Internet in accordance with user instructions, including searching, linking to, receiving, and displaying web pages or portions thereof, as well as attachments and other files linked to web pages.

[0083] In conjunction with RF circuitry 108, touch screen 112, display controller 156, contact/motion module 130, graphics module 132, text input module 134, e-mail client

module 140, and browser module 147, calendar module 148 includes executable instructions to create, display, modify, and store calendars and data associated with calendars (e.g., calendar entries, to-do lists, etc.) in accordance with user instructions.

[0084] In conjunction with RF circuitry 108, touch screen 112, display controller 156, contact/motion module 130, graphics module 132, text input module 134, and browser module 147, widget modules 149 are mini-applications that are, optionally, downloaded and used by a user (e.g., weather widget 149-1, stocks widget 149-2, calculator widget 149-3, alarm clock widget 149-4, and dictionary widget 149-5) or created by the user (e.g., user-created widget 149-6). In some embodiments, a widget includes an HTML (Hypertext Markup Language) file, a CSS (Cascading Style Sheets) file, and a JavaScript file. In some embodiments, a widget includes an XML (Extensible Markup Language) file and a JavaScript file (e.g., Yahoo! Widgets).

[0085] In conjunction with RF circuitry 108, touch screen 112, display controller 156, contact/motion module 130, graphics module 132, text input module 134, and browser module 147, the widget creator module 150 are, optionally, used by a user to create widgets (e.g., turning a user-specified portion of a web page into a widget).

[0086] In conjunction with touch screen 112, display controller 156, contact/motion module 130, graphics module 132, and text input module 134, search module 151 includes executable instructions to search for text, music, sound, image, video, and/or other files in memory 102 that match one or more search criteria (e.g., one or more user-specified search terms) in accordance with user instructions.

[0087] In conjunction with touch screen 112, display controller 156, contact/motion module 130, graphics module 132, audio circuitry 110, speaker 111, RF circuitry 108, and browser module 147, video and music player module 152 includes executable instructions that allow the user to download and play back recorded music and other sound files stored in one or more file formats, such as MP3 or AAC files, and executable instructions to display, present, or otherwise play back videos (e.g., on touch screen 112 or on an external, connected display via external port 124). In some embodiments, device 100 optionally includes the functionality of an MP3 player, such as an iPod (trademark of Apple Inc.).

[0088] In conjunction with touch screen 112, display controller 156, contact/motion module 130, graphics module 132, and text input module 134, notes module 153 includes

executable instructions to create and manage notes, to-do lists, and the like in accordance with user instructions.

[0089] In conjunction with RF circuitry 108, touch screen 112, display controller 156, contact/motion module 130, graphics module 132, text input module 134, GPS module 135, and browser module 147, map module 154 are, optionally, used to receive, display, modify, and store maps and data associated with maps (e.g., driving directions, data on stores and other points of interest at or near a particular location, and other location-based data) in accordance with user instructions.

[0090] In conjunction with touch screen 112, display controller 156, contact/motion module 130, graphics module 132, audio circuitry 110, speaker 111, RF circuitry 108, text input module 134, e-mail client module 140, and browser module 147, online video module 155 includes instructions that allow the user to access, browse, receive (e.g., by streaming and/or download), play back (e.g., on the touch screen or on an external, connected display via external port 124), send an e-mail with a link to a particular online video, and otherwise manage online videos in one or more file formats, such as H.264. In some embodiments, instant messaging module 141, rather than e-mail client module 140, is used to send a link to a particular online video. Additional description of the online video application can be found in U.S. Provisional Patent Application No. 60/936,562, "Portable Multifunction Device, Method, and Graphical User Interface for Playing Online Videos," filed June 20, 2007, and U.S. Patent Application No. 11/968,067, "Portable Multifunction Device, Method, and Graphical User Interface for Playing Online Videos," filed December 31, 2007, the contents of which are hereby incorporated by reference in their entirety.

[0091] Each of the above-identified modules and applications corresponds to a set of executable instructions for performing one or more functions described above and the methods described in this application (e.g., the computer-implemented methods and other information processing methods described herein). These modules (e.g., sets of instructions) need not be implemented as separate software programs (such as computer programs (e.g., including instructions)), procedures, or modules, and thus various subsets of these modules are, optionally, combined or otherwise rearranged in various embodiments. For example, video player module is, optionally, combined with music player module into a single module (e.g., video and music player module 152, FIG. 1A). In some embodiments, memory 102

optionally stores a subset of the modules and data structures identified above. Furthermore, memory 102 optionally stores additional modules and data structures not described above.

[0092] In some embodiments, device 100 is a device where operation of a predefined set of functions on the device is performed exclusively through a touch screen and/or a touchpad. By using a touch screen and/or a touchpad as the primary input control device for operation of device 100, the number of physical input control devices (such as push buttons, dials, and the like) on device 100 is, optionally, reduced.

[0093] The predefined set of functions that are performed exclusively through a touch screen and/or a touchpad optionally include navigation between user interfaces. In some embodiments, the touchpad, when touched by the user, navigates device 100 to a main, home, or root menu from any user interface that is displayed on device 100. In such embodiments, a "menu button" is implemented using a touchpad. In some other embodiments, the menu button is a physical push button or other physical input control device instead of a touchpad.

[0094] FIG. 1B is a block diagram illustrating exemplary components for event handling in accordance with some embodiments. In some embodiments, memory 102 (FIG. 1A) or 370 (FIG. 3) includes event sorter 170 (e.g., in operating system 126) and a respective application 136-1 (e.g., any of the aforementioned applications 137-151, 155, 380-390).

[0095] Event sorter 170 receives event information and determines the application 136-1 and application view 191 of application 136-1 to which to deliver the event information. Event sorter 170 includes event monitor 171 and event dispatcher module 174. In some embodiments, application 136-1 includes application internal state 192, which indicates the current application view(s) displayed on touch-sensitive display 112 when the application is active or executing. In some embodiments, device/global internal state 157 is used by event sorter 170 to determine which application(s) is (are) currently active, and application internal state 192 is used by event sorter 170 to determine application views 191 to which to deliver event information.

[0096] In some embodiments, application internal state 192 includes additional information, such as one or more of: resume information to be used when application 136-1 resumes execution, user interface state information that indicates information being displayed or that is ready for display by application 136-1, a state queue for enabling the user to go

back to a prior state or view of application 136-1, and a redo/undo queue of previous actions taken by the user.

[0097] Event monitor 171 receives event information from peripherals interface 118. Event information includes information about a sub-event (e.g., a user touch on touch-sensitive display 112, as part of a multi-touch gesture). Peripherals interface 118 transmits information it receives from I/O subsystem 106 or a sensor, such as proximity sensor 166, accelerometer(s) 168, and/or microphone 113 (through audio circuitry 110). Information that peripherals interface 118 receives from I/O subsystem 106 includes information from touch-sensitive display 112 or a touch-sensitive surface.

[0098] In some embodiments, event monitor 171 sends requests to the peripherals interface 118 at predetermined intervals. In response, peripherals interface 118 transmits event information. In other embodiments, peripherals interface 118 transmits event information only when there is a significant event (e.g., receiving an input above a predetermined noise threshold and/or for more than a predetermined duration).

[0099] In some embodiments, event sorter 170 also includes a hit view determination module 172 and/or an active event recognizer determination module 173.

[0100] Hit view determination module 172 provides software procedures for determining where a sub-event has taken place within one or more views when touch-sensitive display 112 displays more than one view. Views are made up of controls and other elements that a user can see on the display.

[0101] Another aspect of the user interface associated with an application is a set of views, sometimes herein called application views or user interface windows, in which information is displayed and touch-based gestures occur. The application views (of a respective application) in which a touch is detected optionally correspond to programmatic levels within a programmatic or view hierarchy of the application. For example, the lowest level view in which a touch is detected is, optionally, called the hit view, and the set of events that are recognized as proper inputs are, optionally, determined based, at least in part, on the hit view of the initial touch that begins a touch-based gesture.

[0102] Hit view determination module 172 receives information related to sub-events of a touch-based gesture. When an application has multiple views organized in a hierarchy, hit

view determination module 172 identifies a hit view as the lowest view in the hierarchy which should handle the sub-event. In most circumstances, the hit view is the lowest level view in which an initiating sub-event occurs (e.g., the first sub-event in the sequence of sub-events that form an event or potential event). Once the hit view is identified by the hit view determination module 172, the hit view typically receives all sub-events related to the same touch or input source for which it was identified as the hit view.

[0103] Active event recognizer determination module 173 determines which view or views within a view hierarchy should receive a particular sequence of sub-events. In some embodiments, active event recognizer determination module 173 determines that only the hit view should receive a particular sequence of sub-events. In other embodiments, active event recognizer determination module 173 determines that all views that include the physical location of a sub-event are actively involved views, and therefore determines that all actively involved views should receive a particular sequence of sub-events. In other embodiments, even if touch sub-events were entirely confined to the area associated with one particular view, views higher in the hierarchy would still remain as actively involved views.

[0104] Event dispatcher module 174 dispatches the event information to an event recognizer (e.g., event recognizer 180). In embodiments including active event recognizer determination module 173, event dispatcher module 174 delivers the event information to an event recognizer determined by active event recognizer determination module 173. In some embodiments, event dispatcher module 174 stores in an event queue the event information, which is retrieved by a respective event receiver 182.

[0105] In some embodiments, operating system 126 includes event sorter 170. Alternatively, application 136-1 includes event sorter 170. In yet other embodiments, event sorter 170 is a stand-alone module, or a part of another module stored in memory 102, such as contact/motion module 130.

[0106] In some embodiments, application 136-1 includes a plurality of event handlers 190 and one or more application views 191, each of which includes instructions for handling touch events that occur within a respective view of the application's user interface. Each application view 191 of the application 136-1 includes one or more event recognizers 180. Typically, a respective application view 191 includes a plurality of event recognizers 180. In other embodiments, one or more of event recognizers 180 are part of a separate module, such

as a user interface kit or a higher level object from which application 136-1 inherits methods and other properties. In some embodiments, a respective event handler 190 includes one or more of: data updater 176, object updater 177, GUI updater 178, and/or event data 179 received from event sorter 170. Event handler 190 optionally utilizes or calls data updater 176, object updater 177, or GUI updater 178 to update the application internal state 192. Alternatively, one or more of the application views 191 include one or more respective event handlers 190. Also, in some embodiments, one or more of data updater 176, object updater 177, and GUI updater 178 are included in a respective application view 191.

[0107] A respective event recognizer 180 receives event information (e.g., event data 179) from event sorter 170 and identifies an event from the event information. Event recognizer 180 includes event receiver 182 and event comparator 184. In some embodiments, event recognizer 180 also includes at least a subset of: metadata 183, and event delivery instructions 188 (which optionally include sub-event delivery instructions).

[0108] Event receiver 182 receives event information from event sorter 170. The event information includes information about a sub-event, for example, a touch or a touch movement. Depending on the sub-event, the event information also includes additional information, such as location of the sub-event. When the sub-event concerns motion of a touch, the event information optionally also includes speed and direction of the sub-event. In some embodiments, events include rotation of the device from one orientation to another (e.g., from a portrait orientation to a landscape orientation, or vice versa), and the event information includes corresponding information about the current orientation (also called device attitude) of the device.

[0109] Event comparator 184 compares the event information to predefined event or sub-event definitions and, based on the comparison, determines an event or sub-event, or determines or updates the state of an event or sub-event. In some embodiments, event comparator 184 includes event definitions 186. Event definitions 186 contain definitions of events (e.g., predefined sequences of sub-events), for example, event 1 (187-1), event 2 (187-2), and others. In some embodiments, sub-events in an event (e.g., 187-1 and/or 187-2) include, for example, touch begin, touch end, touch movement, touch cancellation, and multiple touching. In one example, the definition for event 1 (187-1) is a double tap on a displayed object. The double tap, for example, comprises a first touch (touch begin) on the displayed object for a predetermined phase, a first liftoff (touch end) for a predetermined

phase, a second touch (touch begin) on the displayed object for a predetermined phase, and a second liftoff (touch end) for a predetermined phase. In another example, the definition for event 2 (187-2) is a dragging on a displayed object. The dragging, for example, comprises a touch (or contact) on the displayed object for a predetermined phase, a movement of the touch across touch-sensitive display 112, and liftoff of the touch (touch end). In some embodiments, the event also includes information for one or more associated event handlers 190.

[0110] In some embodiments, event definitions 186 include a definition of an event for a respective user-interface object. In some embodiments, event comparator 184 performs a hit test to determine which user-interface object is associated with a sub-event. For example, in an application view in which three user-interface objects are displayed on touch-sensitive display 112, when a touch is detected on touch-sensitive display 112, event comparator 184 performs a hit test to determine which of the three user-interface objects is associated with the touch (sub-event). If each displayed object is associated with a respective event handler 190, the event comparator uses the result of the hit test to determine which event handler 190 should be activated. For example, event comparator 184 selects an event handler associated with the sub-event and the object triggering the hit test.

[0111] In some embodiments, the definition for a respective event (187) also includes delayed actions that delay delivery of the event information until after it has been determined whether the sequence of sub-events does or does not correspond to the event recognizer's event type.

[0112] When a respective event recognizer 180 determines that the series of sub-events do not match any of the events in event definitions 186, the respective event recognizer 180 enters an event impossible, event failed, or event ended state, after which it disregards subsequent sub-events of the touch-based gesture. In this situation, other event recognizers, if any, that remain active for the hit view continue to track and process sub-events of an ongoing touch-based gesture.

[0113] In some embodiments, a respective event recognizer 180 includes metadata 183 with configurable properties, flags, and/or lists that indicate how the event delivery system should perform sub-event delivery to actively involved event recognizers. In some embodiments, metadata 183 includes configurable properties, flags, and/or lists that indicate

how event recognizers interact, or are enabled to interact, with one another. In some embodiments, metadata 183 includes configurable properties, flags, and/or lists that indicate whether sub-events are delivered to varying levels in the view or programmatic hierarchy.

[0114] In some embodiments, a respective event recognizer 180 activates event handler 190 associated with an event when one or more particular sub-events of an event are recognized. In some embodiments, a respective event recognizer 180 delivers event information associated with the event to event handler 190. Activating an event handler 190 is distinct from sending (and deferred sending) sub-events to a respective hit view. In some embodiments, event recognizer 180 throws a flag associated with the recognized event, and event handler 190 associated with the flag catches the flag and performs a predefined process.

[0115] In some embodiments, event delivery instructions 188 include sub-event delivery instructions that deliver event information about a sub-event without activating an event handler. Instead, the sub-event delivery instructions deliver event information to event handlers associated with the series of sub-events or to actively involved views. Event handlers associated with the series of sub-events or with actively involved views receive the event information and perform a predetermined process.

[0116] In some embodiments, data updater 176 creates and updates data used in application 136-1. For example, data updater 176 updates the telephone number used in contacts module 137, or stores a video file used in video player module. In some embodiments, object updater 177 creates and updates objects used in application 136-1. For example, object updater 177 creates a new user-interface object or updates the position of a user-interface object. GUI updater 178 updates the GUI. For example, GUI updater 178 prepares display information and sends it to graphics module 132 for display on a touch-sensitive display.

[0117] In some embodiments, event handler(s) 190 includes or has access to data updater 176, object updater 177, and GUI updater 178. In some embodiments, data updater 176, object updater 177, and GUI updater 178 are included in a single module of a respective application 136-1 or application view 191. In other embodiments, they are included in two or more software modules.

[0118] It shall be understood that the foregoing discussion regarding event handling of user touches on touch-sensitive displays also applies to other forms of user inputs to operate

multifunction devices 100 with input devices, not all of which are initiated on touch screens. For example, mouse movement and mouse button presses, optionally coordinated with single or multiple keyboard presses or holds; contact movements such as taps, drags, scrolls, etc. on touchpads; pen stylus inputs; movement of the device; oral instructions; detected eye movements; biometric inputs; and/or any combination thereof are optionally utilized as inputs corresponding to sub-events which define an event to be recognized.

[0119] FIG. 2 illustrates a portable multifunction device 100 having a touch screen 112 in accordance with some embodiments. The touch screen optionally displays one or more graphics within user interface (UI) 200. In this embodiment, as well as others described below, a user is enabled to select one or more of the graphics by making a gesture on the graphics, for example, with one or more fingers 202 (not drawn to scale in the figure) or one or more styluses 203 (not drawn to scale in the figure). In some embodiments, selection of one or more graphics occurs when the user breaks contact with the one or more graphics. In some embodiments, the gesture optionally includes one or more taps, one or more swipes (from left to right, right to left, upward and/or downward), and/or a rolling of a finger (from right to left, left to right, upward and/or downward) that has made contact with device 100. In some implementations or circumstances, inadvertent contact with a graphic does not select the graphic. For example, a swipe gesture that sweeps over an application icon optionally does not select the corresponding application when the gesture corresponding to selection is a tap.

[0120] Device 100 optionally also include one or more physical buttons, such as "home" or menu button 204. As described previously, menu button 204 is, optionally, used to navigate to any application 136 in a set of applications that are, optionally, executed on device 100. Alternatively, in some embodiments, the menu button is implemented as a soft key in a GUI displayed on touch screen 112.

[0121] In some embodiments, device 100 includes touch screen 112, menu button 204, push button 206 for powering the device on/off and locking the device, volume adjustment button(s) 208, subscriber identity module (SIM) card slot 210, headset jack 212, and docking/charging external port 124. Push button 206 is, optionally, used to turn the power on/off on the device by depressing the button and holding the button in the depressed state for a predefined time interval; to lock the device by depressing the button and releasing the button before the predefined time interval has elapsed; and/or to unlock the device or initiate

an unlock process. In an alternative embodiment, device 100 also accepts verbal input for activation or deactivation of some functions through microphone 113. Device 100 also, optionally, includes one or more contact intensity sensors 165 for detecting intensity of contacts on touch screen 112 and/or one or more tactile output generators 167 for generating tactile outputs for a user of device 100.

[0122] FIG. 3 is a block diagram of an exemplary multifunction device with a display and a touch-sensitive surface in accordance with some embodiments. Device 300 need not be portable. In some embodiments, device 300 is a laptop computer, a desktop computer, a tablet computer, a multimedia player device, a navigation device, an educational device (such as a child's learning toy), a gaming system, or a control device (e.g., a home or industrial controller). Device 300 typically includes one or more processing units (CPUs) 310, one or more network or other communications interfaces 360, memory 370, and one or more communication buses 320 for interconnecting these components. Communication buses 320 optionally include circuitry (sometimes called a chipset) that interconnects and controls communications between system components. Device 300 includes input/output (I/O) interface 330 comprising display 340, which is typically a touch screen display. I/O interface 330 also optionally includes a keyboard and/or mouse (or other pointing device) 350 and touchpad 355, tactile output generator 357 for generating tactile outputs on device 300 (e.g., similar to tactile output generator(s) 167 described above with reference to FIG. 1A), sensors 359 (e.g., optical, acceleration, proximity, touch-sensitive, and/or contact intensity sensors similar to contact intensity sensor(s) 165 described above with reference to FIG. 1A). Memory 370 includes high-speed random access memory, such as DRAM, SRAM, DDR RAM, or other random access solid state memory devices; and optionally includes non-volatile memory, such as one or more magnetic disk storage devices, optical disk storage devices, flash memory devices, or other non-volatile solid state storage devices. Memory 370 optionally includes one or more storage devices remotely located from CPU(s) 310. In some embodiments, memory 370 stores programs, modules, and data structures analogous to the programs, modules, and data structures stored in memory 102 of portable multifunction device 100 (FIG. 1A), or a subset thereof. Furthermore, memory 370 optionally stores additional programs, modules, and data structures not present in memory 102 of portable multifunction device 100. For example, memory 370 of device 300 optionally stores drawing module 380, presentation module 382, word processing module 384, website creation module

386, disk authoring module 388, and/or spreadsheet module 390, while memory 102 of portable multifunction device 100 (FIG. 1A) optionally does not store these modules.

[0123] Each of the above-identified elements in FIG. 3 is, optionally, stored in one or more of the previously mentioned memory devices. Each of the above-identified modules corresponds to a set of instructions for performing a function described above. The above-identified modules or computer programs (e.g., sets of instructions or including instructions) need not be implemented as separate software programs (such as computer programs (e.g., including instructions)), procedures, or modules, and thus various subsets of these modules are, optionally, combined or otherwise rearranged in various embodiments. In some embodiments, memory 370 optionally stores a subset of the modules and data structures identified above. Furthermore, memory 370 optionally stores additional modules and data structures not described above.

[0124] Attention is now directed towards embodiments of user interfaces that are, optionally, implemented on, for example, portable multifunction device 100.

[0125] FIG. 4A illustrates an exemplary user interface for a menu of applications on portable multifunction device 100 in accordance with some embodiments. Similar user interfaces are, optionally, implemented on device 300. In some embodiments, user interface 400 includes the following elements, or a subset or superset thereof:

- Signal strength indicator(s) 402 for wireless communication(s), such as cellular and Wi-Fi signals;
- Time 404;
- Bluetooth indicator 405;
- Battery status indicator 406;
- Tray 408 with icons for frequently used applications, such as:
    - Icon 416 for telephone module 138, labeled “Phone,” which optionally includes an indicator 414 of the number of missed calls or voicemail messages;

- Icon 418 for e-mail client module 140, labeled "Mail," which optionally includes an indicator 410 of the number of unread e-mails;
- Icon 420 for browser module 147, labeled "Browser;" and
- Icon 422 for video and music player module 152, also referred to as iPod (trademark of Apple Inc.) module 152, labeled "iPod;" and

- Icons for other applications, such as:
  - Icon 424 for IM module 141, labeled "Messages;"
  - Icon 426 for calendar module 148, labeled "Calendar;"
  - Icon 428 for image management module 144, labeled "Photos;"
  - Icon 430 for camera module 143, labeled "Camera;"
  - Icon 432 for online video module 155, labeled "Online Video;"
  - Icon 434 for stocks widget 149-2, labeled "Stocks;"
  - Icon 436 for map module 154, labeled "Maps;"
  - Icon 438 for weather widget 149-1, labeled "Weather;"
  - Icon 440 for alarm clock widget 149-4, labeled "Clock;"
  - Icon 442 for workout support module 142, labeled "Workout Support;"
  - Icon 444 for notes module 153, labeled "Notes;" and
  - Icon 446 for a settings application or module, labeled "Settings," which provides access to settings for device 100 and its various applications 136.

[0126] It should be noted that the icon labels illustrated in FIG. 4A are merely exemplary. For example, icon 422 for video and music player module 152 is labeled "Music" or "Music Player." Other labels are, optionally, used for various application icons. In some embodiments, a label for a respective application icon includes a name of an application corresponding to the respective application icon. In some embodiments, a label for a particular application icon is distinct from a name of an application corresponding to the particular application icon.

[0127] FIG. 4B illustrates an exemplary user interface on a device (e.g., device 300, FIG. 3) with a touch-sensitive surface 451 (e.g., a tablet or touchpad 355, FIG. 3) that is separate

from the display 450 (e.g., touch screen display 112). Device 300 also, optionally, includes one or more contact intensity sensors (e.g., one or more of sensors 359) for detecting intensity of contacts on touch-sensitive surface 451 and/or one or more tactile output generators 357 for generating tactile outputs for a user of device 300.

[0128] Although some of the examples that follow will be given with reference to inputs on touch screen display 112 (where the touch-sensitive surface and the display are combined), in some embodiments, the device detects inputs on a touch-sensitive surface that is separate from the display, as shown in FIG. 4B. In some embodiments, the touch-sensitive surface (e.g., 451 in FIG. 4B) has a primary axis (e.g., 452 in FIG. 4B) that corresponds to a primary axis (e.g., 453 in FIG. 4B) on the display (e.g., 450). In accordance with these embodiments, the device detects contacts (e.g., 460 and 462 in FIG. 4B) with the touch-sensitive surface 451 at locations that correspond to respective locations on the display (e.g., in FIG. 4B, 460 corresponds to 468 and 462 corresponds to 470). In this way, user inputs (e.g., contacts 460 and 462, and movements thereof) detected by the device on the touch-sensitive surface (e.g., 451 in FIG. 4B) are used by the device to manipulate the user interface on the display (e.g., 450 in FIG. 4B) of the multifunction device when the touch-sensitive surface is separate from the display. It should be understood that similar methods are, optionally, used for other user interfaces described herein.

[0129] Additionally, while the following examples are given primarily with reference to finger inputs (e.g., finger contacts, finger tap gestures, finger swipe gestures), it should be understood that, in some embodiments, one or more of the finger inputs are replaced with input from another input device (e.g., a mouse-based input or stylus input). For example, a swipe gesture is, optionally, replaced with a mouse click (e.g., instead of a contact) followed by movement of the cursor along the path of the swipe (e.g., instead of movement of the contact). As another example, a tap gesture is, optionally, replaced with a mouse click while the cursor is located over the location of the tap gesture (e.g., instead of detection of the contact followed by ceasing to detect the contact). Similarly, when multiple user inputs are simultaneously detected, it should be understood that multiple computer mice are, optionally, used simultaneously, or a mouse and finger contacts are, optionally, used simultaneously.

[0130] FIG. 5A illustrates exemplary personal electronic device 500. Device 500 includes body 502. In some embodiments, device 500 can include some or all of the features described with respect to devices 100 and 300 (e.g., FIGS. 1A-4B). In some embodiments,

device 500 has touch-sensitive display screen 504, hereafter touch screen 504. Alternatively, or in addition to touch screen 504, device 500 has a display and a touch-sensitive surface. As with devices 100 and 300, in some embodiments, touch screen 504 (or the touch-sensitive surface) optionally includes one or more intensity sensors for detecting intensity of contacts (e.g., touches) being applied. The one or more intensity sensors of touch screen 504 (or the touch-sensitive surface) can provide output data that represents the intensity of touches. The user interface of device 500 can respond to touches based on their intensity, meaning that touches of different intensities can invoke different user interface operations on device 500.

[0131] Exemplary techniques for detecting and processing touch intensity are found, for example, in related applications: International Patent Application Serial No. PCT/US2013/040061, titled "Device, Method, and Graphical User Interface for Displaying User Interface Objects Corresponding to an Application," filed May 8, 2013, published as WIPO Publication No. WO/2013/169849, and International Patent Application Serial No. PCT/US2013/069483, titled "Device, Method, and Graphical User Interface for Transitioning Between Touch Input to Display Output Relationships," filed November 11, 2013, published as WIPO Publication No. WO/2014/105276, each of which is hereby incorporated by reference in their entirety.

[0132] In some embodiments, device 500 has one or more input mechanisms 506 and 508. Input mechanisms 506 and 508, if included, can be physical. Examples of physical input mechanisms include push buttons and rotatable mechanisms. In some embodiments, device 500 has one or more attachment mechanisms. Such attachment mechanisms, if included, can permit attachment of device 500 with, for example, hats, eyewear, earrings, necklaces, shirts, jackets, bracelets, watch straps, chains, trousers, belts, shoes, purses, backpacks, and so forth. These attachment mechanisms permit device 500 to be worn by a user.

[0133] FIG. 5B depicts exemplary personal electronic device 500. In some embodiments, device 500 can include some or all of the components described with respect to FIGS. 1A, 1B, and 3. Device 500 has bus 512 that operatively couples I/O section 514 with one or more computer processors 516 and memory 518. I/O section 514 can be connected to display screen 504, which can have touch-sensitive component 522 and, optionally, intensity sensor 524 (e.g., contact intensity sensor). In addition, I/O section 514 can be connected with communication unit 530 for receiving application and operating system data, using Wi-Fi,

Bluetooth, near field communication (NFC), cellular, and/or other wireless communication techniques. Device 500 can include input mechanisms 506 and/or 508. Input mechanism 506 is, optionally, a rotatable input device or a depressible and rotatable input device, for example. Input mechanism 508 is, optionally, a button, in some examples.

[0134] Input mechanism 508 is, optionally, a microphone, in some examples. Personal electronic device 500 optionally includes various sensors, such as GPS sensor 532, accelerometer 534, directional sensor 540 (e.g., compass), gyroscope 536, motion sensor 538, and/or a combination thereof, all of which can be operatively connected to I/O section 514.

[0135] Memory 518 of personal electronic device 500 can include one or more non-transitory computer-readable storage mediums, for storing computer-executable instructions, which, when executed by one or more computer processors 516, for example, can cause the computer processors to perform the techniques described below, including process 700 (FIG. 7). A computer-readable storage medium can be any medium that can tangibly contain or store computer-executable instructions for use by or in connection with the instruction execution system, apparatus, or device. In some examples, the storage medium is a transitory computer-readable storage medium. In some examples, the storage medium is a non-transitory computer-readable storage medium. The non-transitory computer-readable storage medium can include, but is not limited to, magnetic, optical, and/or semiconductor storages. Examples of such storage include magnetic disks, optical discs based on CD, DVD, or Blu-ray technologies, as well as persistent solid-state memory such as flash, solid-state drives, and the like. Personal electronic device 500 is not limited to the components and configuration of FIG. 5B, but can include other or additional components in multiple configurations.

[0136] As used here, the term "affordance" refers to a user-interactive graphical user interface object that is, optionally, displayed on the display screen of devices 100, 300, and/or 500 (FIGS. 1A, 3, and 5A-5B). For example, an image (e.g., icon), a button, and text (e.g., hyperlink) each optionally constitute an affordance.

[0137] As used herein, the term "focus selector" refers to an input element that indicates a current part of a user interface with which a user is interacting. In some implementations that include a cursor or other location marker, the cursor acts as a "focus selector" so that when an input (e.g., a press input) is detected on a touch-sensitive surface (e.g., touchpad 355 in FIG. 3 or touch-sensitive surface 451 in FIG. 4B) while the cursor is over a particular user

interface element (e.g., a button, window, slider, or other user interface element), the particular user interface element is adjusted in accordance with the detected input. In some implementations that include a touch screen display (e.g., touch-sensitive display system 112 in FIG. 1A or touch screen 112 in FIG. 4A) that enables direct interaction with user interface elements on the touch screen display, a detected contact on the touch screen acts as a "focus selector" so that when an input (e.g., a press input by the contact) is detected on the touch screen display at a location of a particular user interface element (e.g., a button, window, slider, or other user interface element), the particular user interface element is adjusted in accordance with the detected input. In some implementations, focus is moved from one region of a user interface to another region of the user interface without corresponding movement of a cursor or movement of a contact on a touch screen display (e.g., by using a tab key or arrow keys to move focus from one button to another button); in these implementations, the focus selector moves in accordance with movement of focus between different regions of the user interface. Without regard to the specific form taken by the focus selector, the focus selector is generally the user interface element (or contact on a touch screen display) that is controlled by the user so as to communicate the user's intended interaction with the user interface (e.g., by indicating, to the device, the element of the user interface with which the user is intending to interact). For example, the location of a focus selector (e.g., a cursor, a contact, or a selection box) over a respective button while a press input is detected on the touch-sensitive surface (e.g., a touchpad or touch screen) will indicate that the user is intending to activate the respective button (as opposed to other user interface elements shown on a display of the device).

[0138] As used in the specification and claims, the term "characteristic intensity" of a contact refers to a characteristic of the contact based on one or more intensities of the contact. In some embodiments, the characteristic intensity is based on multiple intensity samples. The characteristic intensity is, optionally, based on a predefined number of intensity samples, or a set of intensity samples collected during a predetermined time period (e.g., 0.05, 0.1, 0.2, 0.5, 1, 2, 5, 10 seconds) relative to a predefined event (e.g., after detecting the contact, prior to detecting liftoff of the contact, before or after detecting a start of movement of the contact, prior to detecting an end of the contact, before or after detecting an increase in intensity of the contact, and/or before or after detecting a decrease in intensity of the contact). A characteristic intensity of a contact is, optionally, based on one or more of: a maximum value of the intensities of the contact, a mean value of the intensities of the contact, an average

value of the intensities of the contact, a top 10 percentile value of the intensities of the contact, a value at the half maximum of the intensities of the contact, a value at the 90 percent maximum of the intensities of the contact, or the like. In some embodiments, the duration of the contact is used in determining the characteristic intensity (e.g., when the characteristic intensity is an average of the intensity of the contact over time). In some embodiments, the characteristic intensity is compared to a set of one or more intensity thresholds to determine whether an operation has been performed by a user. For example, the set of one or more intensity thresholds optionally includes a first intensity threshold and a second intensity threshold. In this example, a contact with a characteristic intensity that does not exceed the first threshold results in a first operation, a contact with a characteristic intensity that exceeds the first intensity threshold and does not exceed the second intensity threshold results in a second operation, and a contact with a characteristic intensity that exceeds the second threshold results in a third operation. In some embodiments, a comparison between the characteristic intensity and one or more thresholds is used to determine whether or not to perform one or more operations (e.g., whether to perform a respective operation or forgo performing the respective operation), rather than being used to determine whether to perform a first operation or a second operation.

[0139] Attention is now directed towards embodiments of user interfaces ("UI") and associated processes that are implemented on an electronic device, such as portable multifunction device 100, device 300, or device 500.

[0140] FIGS. 6A-6AB illustrate exemplary user interfaces for enabling a security mode at one or more computer systems, in accordance with some embodiments. The user interfaces in these figures are used to illustrate the processes described below, including the processes in FIG. 7.

[0141] FIG. 6A depicts computer system 600 (e.g., a smartphone), which includes display 600a (e.g., a touch-sensitive display). In some embodiments, computer system 600 includes one or more elements from device 100, device 300, and/or device 500. As shown in FIG. 6A, computer system 600 displays, via display 600a, email interface 602, which shows an email that includes image 604. In the embodiment depicted in FIG. 6A, computer system 600 is logged into John's user account, as indicated by "John's email" in email interface 602. In the embodiments depicted in FIGS. 6A-6K, computer system 600 is the only computer system or

device that is logged into John's account. In the embodiments depicted in FIGS. 6L-6AB, other devices are logged into John's account, in addition to computer system 600.

[0142] It should be appreciated that the exemplary user interfaces and techniques provided herein are illustrated in the figures and described below as being performed on respective computer systems. For example, in some embodiments the security mode is depicted and described as being enabled by computer system 600 (for computer system 600 and, optionally, other devices such as device 610). However, it should be appreciated that the embodiments are provided as an example and, unless specified otherwise, the user interfaces can be displayed on different devices and the corresponding techniques performed by the different devices. For example, the security mode can be enabled using device 610 in a manner that is analogous to that described with respect to computer system 600. For the sake of brevity, these details are not repeated.

[0143] In FIG. 6A, computer system 600 detects input 605-1, which is an upward swipe gesture located at a bottom region of display 600a (also referred to herein as a home gesture) that causes computer system 600 to display home screen 606, as shown in FIG. 6B. In FIG. 6B, computer system 600 detects input 605-2 (e.g., a tap input) on settings application icon 608. In response to detecting input 605-2, computer system 600 displays settings interface 612, as shown in FIG. 6C.

[0144] In FIG. 6C, computer system 600 detects input 605-3 on privacy/security option 614 and, in response, displays privacy and security interface 616, as shown in FIG. 6D. In FIG. 6D, computer system 600 detects input 605-4 selecting lockdown mode option 618 (currently shown as "off") and, in response, displays lockdown mode interface 622, as shown in FIG. 6E. Lockdown mode interface 622 includes notification 624 describing the lockdown mode and including option 624-1 that is selectable to begin enabling the lockdown mode.

[0145] In the embodiments described herein, lockdown mode is a security mode that can be enabled for computer systems that are associated with a same user account. For example, computer system 600 is logged into John's user account. Therefore, computer system 600 can enable lockdown mode to enable the security mode at computer system 600. In some embodiments, computer system 600 can also enable the security mode at other computer systems or devices that are also logged into John's user account. The security mode is intended to protect the computer system from harmful or malicious attackers by altering the

functionality or operation of the computer system to restrict access to data that can be potentially used to target the computer system in a cyberattack. For example, when the lockdown mode is enabled for a computer system, the computer system does not display images in certain communications such as emails, SMS messages, or text messages, the computer system is restricted from accessing non-encrypted websites, some applications are unavailable at the computer system or are limited in functionality, and/or other features or experiences provided by the computer system are unavailable or limited. Other example restrictions that can be enabled for the lockdown mode include: blocking message attachments, blocking incoming video calls from users that have not previously been called, blocking some web technologies and browsing features, removing shared content such as shared photos or shared collections of photos, blocking wired connections with other devices or accessories while the computer system is locked, blocking invitations for particular services from users that do not have proper permissions, and restricting or uninstalling various configuration profiles.

[0146] In FIG. 6E, computer system 600 detects input 605-5 selecting option 624-1, which is an option to enable lockdown mode for computer system 600. In some embodiments, input 605-5 is a request to enable lockdown mode for computer system 600. Because computer system 600 is the only computer system or device that is logged into John's account, computer system 600 begins to enable the lockdown mode for computer system 600, as depicted in FIGS. 6F-6H. If other computer systems or devices are logged into John's account (in addition to computer system 600), then computer system 600 does not immediately begin enabling lockdown mode, but instead displays prompt 640 in response to detecting input 605-5 selecting option 624-1, as described in greater detail below with reference to FIG. 6L. In some embodiments, as a part of enabling the lockdown mode for the computer system, computer system 600 displays prompt 626 in response to detecting input 605-5 on option 624-1, as shown in FIG. 6F. In some embodiments, in response to input 605-5, computer system 600 displays an interstitial interface that provides additional details about the lockdown mode, and prompt 626 or prompt 640 is displayed in response to an input on the interstitial interface to enable lockdown mode. In some embodiments, computer system 600 begins enabling the lockdown mode (as described below) in response to input 605-5 (or the input on the interstitial interface) without displaying prompt 626 (or prompt 640), when computer system 600 is the only computer system or device logged into the user account.

[0147] As depicted in FIG. 6F, computer system 600 displays prompt 626 which is a confirmation interface to confirm whether the user intends to enable the lockdown mode. Prompt 626 includes option 626-1, which can be selected to confirm the request to enable lockdown mode, and option 626-2, which can be selected to cancel the request to enable lockdown mode. In response to detecting input 605-6 selecting option 626-1, computer system 600 continues to enable the lockdown mode, which includes restarting computer system 600 and, optionally, authenticating the user, as depicted in FIGS. 6G and 6H. In FIG. 6G, computer system 600 displays authentication interface 628 to authenticate the user by requiring the user to enter a passcode to continue enabling the lockdown mode. In some embodiments, the lockdown mode is enabled without displaying authentication interface 628. FIG. 6H depicts computer system 600 restarting, which is performed as part of the process for enabling lockdown mode. In some embodiments, computer system 600 enables lockdown mode by shutting down and then restarting with the lockdown mode enabled.

[0148] FIG. 6I depicts computer system 600 after restarting with lockdown mode enabled. Computer system 600 displays lock screen interface 630 while lockdown mode is enabled. Because lockdown mode is enabled, various applications operating at computer system 600 are disabled or restricted, and some of the information that is otherwise displayed on lock screen interface 630 (when lockdown mode is not enabled) is depicted in a disabled or deemphasized appearance. For example, weather data 631, calendar data 632, and camera icon 633 are each shown in an unavailable, disabled, or otherwise deemphasized state to indicate that these features are unavailable while the lockdown mode is enabled.

[0149] In FIG. 6I, computer system 600 detects input 605-7 to initiate a process for unlocking computer system 600. In some embodiments, the computer system 600 performs an authentication process, such as a biometric authentication and/or a passcode authentication, as a part of unlocking computer system 600.

[0150] In FIG. 6J, computer system displays lockdown mode interface 622. In some embodiments, computer system 600 displays lockdown mode interface 622 in response to input 605-7. In some embodiments, computer system 600 displays lockdown mode interface 622 in response to one or more inputs similar to those described above with respect to FIGS. 6B-6D. Because the lockdown mode is enabled in FIG. 6J, computer system 600 displays lockdown mode interface 622 with notification 636 describing lockdown mode and including option 636-1 that is selectable to begin disabling the lockdown mode.

[0151] In the embodiments described herein, the process for disabling lockdown mode is distributed across each device logged into the user account for which lockdown mode is enabled. The distribution of the lockdown disablement process enhances security at the respective devices by preventing a malicious actor from being able to disable the security mode for all devices, in the event the actor is able to gain access to one of the devices logged into the user account. The distributed disablement process is described in greater detail below with respect to FIGS. 6T-6W.

[0152] In FIG. 6J, computer system 600 detects input 605-8 selecting option 636-1, which is an option to disable lockdown mode for computer system 600. In some embodiments, input 605-8 is a request to disable lockdown mode for computer system 600. In response to detecting input 605-8, computer system 600 begins the process for exiting lockdown mode. Because computer system 600 is the only computer system or device that is logged into John's account, computer system 600 displays prompt 638, as shown in FIG. 6K. If other computer systems or devices are logged into John's account, then computer system 600 displays prompt 660 in response to detecting input 605-8 selecting option 636-1, as described in greater detail below with reference to FIG. 6T. Prompt 638 is a confirmation interface to confirm whether the user intends to disable the lockdown mode at computer system 600. Prompt 638 includes option 638-1, which is selectable to disable the lockdown mode and restart computer system 600. Prompt 638 also includes and a cancel option that can be selected to cancel the request to turn off lockdown mode. In response to detecting input 605-9 selecting option 638-1, computer system 600 exits the lockdown mode by turning off computer system 600 (similar to as shown in FIG. 6H) and restarting with the lockdown mode disabled (similar to as shown in FIG. 6V). In some embodiments, computer system 600 displays authentication interface 628 in response to input 605-9 (similar to as shown in FIG. 6G), so that the user is authenticated prior to restarting the device and exiting lockdown mode.

[0153] FIGS. 6L-6W depict example user interfaces for enabling the lockdown mode for various embodiments in which multiple computer systems are logged into John's user account. For example, in FIG. 6L, device 610 (e.g., a tablet computer) is also logged into John's user account with computer system 600. Device 610 includes display 610a (e.g., a touch-sensitive display). In some embodiments, device 610 includes one or more elements from device 100, device 300, and/or device 500. In FIG. 6L, device 610 displays, via display

610a, lock screen interface 642, which is displayed while lockdown mode is not enabled for device 610.

[0154] As depicted in FIG. 6L, when multiple devices are logged into John's user account, computer system 600 displays prompt 640 in response to detecting input 605-5 on option 624-1 (shown in FIG. 6E). Prompt 640 provides options for selecting whether the lockdown mode should be enabled for all devices logged into John's user account, or just for computer system 600. For example, option 640-1 can be selected to enable the lockdown mode at all devices logged into John's user account (computer system 600 and device 610), and option 640-2 can be selected to enable the lockdown mode at only computer system 600. Option 640-3 can be selected to cancel the request to enable the lockdown mode.

[0155] As previously discussed, the process for enabling lockdown mode includes restarting the respective device for which lockdown mode is being enabled. In FIG. 6M, computer system 600 is restarting in response to detecting input 605-11 selecting option 640-2 for enabling lockdown mode for only computer system 600. Because option 640-2 was selected, device 610 does not enter lockdown mode, as shown in FIG. 6M.

[0156] In some embodiments, if option 640-2 is selected (enabling lockdown mode for only computer system 600 and not the other devices), other devices logged into the user account display a notification after a predetermined amount of time (e.g., 12 hours, 24 hours, or 48 hours) after the lockdown mode is enabled for the computer system. For example, in FIG. 6N, device 610 displays notification 644 informing the user that the lockdown mode was enabled for other devices logged into the user account. Notification 644 includes option 644-1 that is selectable to enable the lockdown mode for device 610. In some embodiments, option 644-1 is displayed in response to an input selecting notification 644.

[0157] FIG. 6N depicts computer system 600 displaying privacy and security interface 616 with lockdown mode option 618 indicating that the lockdown mode is enabled for computer system 600.

[0158] In FIG. 6O, both computer system 600 and device 610 are restarting in response to computer system 600 detecting input 605-10 selecting option 640-1 for enabling lockdown mode for all devices logged into the user account. Because computer system 600 and device 610 are both logged into the same user account (John's account), both computer system 600 and device 610 restart, as shown in FIG. 6O, and enter lockdown mode.

[0159] FIG. 6P depicts computer system 600 and device 610 displaying respective home screens 606 and 648 after restarting with lockdown mode enabled. Computer system 600 detects input 605-12 selecting email application icon 646, and device 610 detects input 605-13 selecting email application icon 650. In response to detecting input 605-12, computer system 600 displays email interface 602 as shown in FIG. 6Q. In response to detecting input 605-13, device 610 displays email interface 654 (similar to email interface 602) in FIG. 6Q.

[0160] In FIG. 6Q, both computer system 600 and device 610 are displaying the same email from "John's email" as originally depicted in FIG. 6A. However, because the lockdown mode is enabled for the devices, computer system 600 and device 610 display the email without image 604. This is because images are blocked from being displayed in emails when the lockdown mode is enabled. Instead of displaying the image, both computer system 600 and device 610 display respective links 652 and 656 to a website associated with the email displayed in email interfaces 602 and 654, respectively.

[0161] In FIG. 6Q, device 610 detects input 605-15 selecting link 656 and, in response, displays warning interface 657 and notification 658 in FIG. 6R. The website associated with link 656 is a non-encrypted website. Therefore, because device 610 is in lockdown mode, access to the website is restricted (due to the lack of security protocol for the website) and device 610 instead displays warning interface 657 warning the user that the website is not secure and notification 658, which includes option 658-1 and option 658-2. Option 658-1 is selectable to access the website and option 658-2 is selectable to dismiss notification 658. In response to detecting input 605-17 selecting option 658-2, device 610 dismisses notification 658 as shown in FIG. 6S. In response to detecting input 605-19 (a home gesture) in FIG. 6S, device 610 displays home screen 648 as shown in FIG. 6T.

[0162] FIGS. 6Q-6S depict computer system 600 navigating to lockdown mode interface 622 via input 605-14 (a home gesture) and input 605-16. In FIG. 6S, computer system 600 displays lockdown mode interface 622, which includes prompt 636 displayed because lockdown mode is currently enabled at computer system 600. Computer system 600 detects input 605-18 selecting option 636-1 to turn off lockdown mode at computer system 600.

[0163] As previously mentioned, when lockdown mode is enabled for multiple devices logged into the user account, computer system 600 displays prompt 660 in response to detecting input 605-18 selecting option 636-1. Prompt 660 includes options 660-1, 660-2,

and 660-3. Option 660-1 is selectable to begin the process of turning off lockdown mode for all devices (e.g., computer system 600 and device 610). Option 660-2 is selectable to turn off lockdown mode just for computer system 600 (similar to option 638-1 described with respect to FIG. 6K). Option 660-3 is selectable to cancel the request for exiting lockdown mode. When option 660-2 is selected, computer system 600 turns off and restarts with lockdown mode disabled, as shown in FIGS. 6T and 6V (optionally displaying authentication interface 628 prior to turning off), without causing device 610 to also restart and exit lockdown mode.

[0164] In response to detecting input 605-20 selecting option 660-1, computer system 600 initiates a process for exiting lockdown mode at computer system 600 and device 610. As mentioned above, this includes turning off computer system 600 and restarting with lockdown mode disabled as shown in FIGS. 6T and 6V (optionally displaying authentication interface 628 prior to turning off). However, because the process for disabling lockdown mode is distributed across the devices logged into the user account, selecting option 660-1 does not cause device 610 to exit lockdown mode. Instead, steps for exiting the lockdown mode have to be performed at device 610 (as discussed below with respect to FIG. 6U) in order for device 610 to exit lockdown mode. If other devices were logged into John's account with lockdown mode enabled, these additional steps would also have to be performed at each of these other devices in order for them to exit lockdown mode.

[0165] Referring now to FIG. 6U, device 610 displays prompt 662 prompting the user to disable lockdown mode at device 610. The display of prompt 662 is triggered by the selection of option 660-1 in FIG. 6T. For example, in some embodiments, in response to detecting selection of option 660-1, computer system 600 sends data to a server indicating the request to exit lockdown mode at all devices logged into the user account. The server then sends data to the devices of the user account indicating the request to exit the lockdown mode and, in response, the devices display prompt 662, as shown in FIG. 6U. Prompt 662 includes option 662-1, which is selectable to disable lockdown mode at device 610, and option 662-2, which is selectable to dismiss prompt 662 and remain in lockdown mode.

[0166] In response to detecting input 605-21 selecting option 662-1, device 610 turns off as shown in FIG. 6W and restarts with lockdown mode disabled (e.g., displaying lock screen interface 642 as shown in FIG. 6L). In some embodiments, device 610 optionally displays authentication interface 664, as shown in FIG. 6V, to authenticate the user in a manner similar to authentication interface 628, prior to restarting and exiting lockdown mode.

[0167] In FIG. 6V, computer system 600 is depicted after restarting with lockdown mode disabled. Accordingly, computer system 600 displays lock screen interface 630 with weather data 631, calendar data 632, and camera icon 633 displayed in an enabled state. For example, weather data 631 shows current weather information, calendar data 632 shows current calendar data, and camera icon 633 is selectable to access a camera user interface of computer system 600.

[0168] FIGS. 6X-6AB depict example user interfaces for an embodiment in which the lockdown mode is initiated using a smartwatch when multiple devices are logged into John's user account. FIGS. 6X-6AB depict smartwatch 620, which includes display 620a (e.g., a touch-sensitive display). Smartwatch 620 is a computer system or device that is logged into John's user account. In some embodiments, smartwatch 620 includes one or more elements from device 100, device 300, and/or device 500. Computer system 600 and device 610 are also logged into John's user account in FIGS. 6X-6AB.

[0169] In FIG. 6X, smartwatch 620 displays privacy and security interface 668, which includes lockdown mode option 670. Computer system 600 displays lock screen interface 630, and device 610 displays lock screen interface 642. Lockdown mode is not enabled for smartwatch 620, computer system 600, and device 610.

[0170] In response to detecting input 605-22 selecting lockdown mode option 670, smartwatch 620 displays lockdown mode interface 676, as shown in FIG. 6Y. Lockdown mode interface 676 includes option 678, which is selectable to initiate a process for enabling lockdown mode at smartwatch 620. In response to detecting input 605-24 selecting option 678, smartwatch 620 displays prompt 680 with options 680-1 and 680-2. Option 680-1 is selectable to turn on lockdown mode for all devices logged into John's account (similar to option 640-1). Option 680-2 is selectable to turn on lockdown mode for only smartwatch 620 and computer system 600 (and not for device 610). In the embodiments depicted in FIGS. 6X-6AB, smartwatch 620 is linked with computer system 600 such that data is transmitted (e.g., directly) between smartwatch 620 and computer system 600. Thus, to effectively secure smartwatch 620, lockdown mode should also be enabled for computer system 600 so that compromised data is not shared between smartwatch 620 and computer system 600. Therefore, smartwatch 620 displays option 680-2 for enabling lockdown mode at both smartwatch 620 and computer system 600, instead of an option for enabling lockdown mode only at smartwatch 620.

[0171] In response to detecting input 605-25 selecting option 680-1, smartwatch 620 initiates a process for enabling lockdown mode at all devices logged into John's user account, namely, smartwatch 620, computer system 600, and device 610. Accordingly, all devices restart, as shown in FIG. 6AA, and turn on with lockdown mode enabled. In response to detecting input 605-26 selecting option 680-2, smartwatch 620 initiates a process for enabling lockdown mode at only smartwatch 620 and computer system 600. Accordingly, smartwatch 620 and computer system 600 restart, as shown in FIG. 6AB, and turn on with lockdown mode enabled. Device 610 does not enter lockdown mode and therefore does not restart, as shown in FIG. 6AB.

[0172] FIG. 7 is a flow diagram illustrating a method for enabling a security mode at one or more computer systems, using a computer system in accordance with some embodiments. Method 700 is performed at a computer system (e.g., 100, 300, 500, 600, 610, and/or 620) (e.g., a smartphone, a wearable device (e.g., a smartwatch), a tablet computer, a desktop computer, a laptop computer, and/or a head-mounted device (e.g., a head-mounted augmented reality and/or extended reality device)) that is in communication with (e.g., includes and/or is connected to) a display generation component (e.g., 600a, 610a, and/or 620a) (e.g., a display controller, a touch-sensitive display system, a display screen, a monitor, a projector, a holographic display, and/or a head-mounted display system) and one or more input devices (e.g., 600a, 610a, and/or 620a) (e.g., a touch-sensitive surface, a keyboard, mouse, trackpad, one or more optical sensors for detecting gestures, one or more capacitive sensors for detecting hover inputs, and/or accelerometer/gyroscope/inertial measurement units). Some operations in method 700 are, optionally, combined, the orders of some operations are, optionally, changed, and some operations are, optionally, omitted.

[0173] As described below, method 700 provides an intuitive way for enabling a security mode at one or more computer systems. The method reduces the cognitive burden on a user for enabling a security mode at one or more computer systems, thereby creating a more efficient human-machine interface. For battery-operated computing devices, enabling a user to enable a security mode at one or more computer systems faster and more efficiently conserves power and increases the time between battery charges.

[0174] In method 700, the computer system (e.g., 600) receives (702), via the one or more input devices (e.g., 600a), a request (e.g., 605-5 and/or 605-6) (e.g., a set of one or more inputs) to enable a security mode at the computer system (e.g., a lockdown mode, a mode of

limited operability, and/or a mode in which one or more features and/or operations are restricted to increase security of the computer system), wherein the computer system is associated with (e.g., logged into) a user account.

[0175] In response (704) to receiving the request (e.g., 605-5 and/or 605-6) to enable the security mode at the computer system (e.g., 600), the computer system performs the following steps. In accordance with a determination that a set of one or more electronic devices (e.g., 610 and/or 620) other than the computer system are associated with (e.g., logged into) the user account (e.g., electronic devices other than the computer system are also logged into the user account), the computer system displays (706) a respective user interface (e.g., 640) (e.g., a prompt, a message, and/or a notification) that includes one or more options (e.g., 640-1 and/or 640-2) for enabling the security mode at the set of one or more electronic devices and the computer system. In some embodiments, if electronic devices other than the computer system are also logged into the user account (in addition to the computer system), then the computer system displays a prompt to enable the security mode at all electronic devices logged into the account (including the computer system). In some embodiments, the prompt includes an option to enable the security mode at the computer system and the other electronic devices. In some embodiments, the prompt includes an option to enable the security mode at only the computer system, and not at the other electronic devices. In accordance with a determination that a set of one or more electronic devices other than the computer system are not associated with (e.g., not logged into) the user account (e.g., electronic devices other than the computer system are not logged into the user account) (e.g., the computer system is the only electronic device logged into the user account), the computer system (e.g., 600) enables (708) (or initiates a process for enabling) the security mode at the computer system without displaying the respective user interface (e.g., 640) that includes one or more options (e.g., 640-1 and/or 640-2) for enabling the security mode at the set of one or more electronic devices and the computer system. Displaying the respective interface that includes one or more options for enabling the security mode at the set of one or more electronic devices and the computer system when the set of one or more electronic devices other than the computer system are associated with the user account, and enabling the security mode at the computer system without displaying the respective user interface when the set of one or more electronic devices other than the computer system are not associated with the user account, reduces the number of inputs at the computer system by automatically enabling the security mode at the computer system without displaying additional options

when no other devices are associated with the user account. In some embodiments, if the computer system (e.g., 600) is the only electronic device logged into the user account, then the security mode is enabled at the computer system without prompting to enable the security mode at other devices (e.g., as shown in FIGS. 6E-6I). In some embodiments, as a part of the process of enabling the security mode at the computer system without prompting to enable the security mode at other devices, the computer system displays a prompt (e.g., 626, 626-1) to confirm the security mode should be enabled for the computer system. In some embodiments, the computer system enables the security mode without displaying the prompt (e.g., 626, 626-1) to confirm the security mode should be enabled for the computer system.

[0176] In some embodiments, the security mode is disabled (e.g., exited) at the computer system (e.g., 600) (e.g., without exiting or disabling the security mode at other electronic devices) in response to a request (e.g., 605-8, 605-9, 605-18, and/or 605-20) to disable the security mode received at the computer system. In some embodiments, the security mode is disabled at a first electronic device (e.g., 610 or 620) (e.g., without exiting or disabling the security mode at the computer system or at other electronic devices) in the set of one or more electronic devices in response to a request (e.g., 605-21) to disable the security mode received at the first electronic device. Disabling the security mode at the computer system in response to a request received at the computer system and disabling the security mode at the first electronic device in response to a request received at the first electronic device enhances security of the computer system and the set of one or more electronic devices by requiring input at the respective devices in order to exit the security mode. In some embodiments, the security mode is disabled at respective devices in response to a request to exit or disable the security mode that is received at each respective device. In other words, the security mode is disabled for a respective device in response to a request to exit the security mode that is only received at the respective device (e.g., the security mode is not exited or disabled in response to a request that is received at a different electronic device).

[0177] In some embodiments, while the security mode is enabled at the computer system (e.g., 600) (and, in some embodiments, while the security mode is also enabled at one or more of the electronic devices in the set of one or more electronic devices), the computer system receives a set of one or more inputs (e.g., 605-8 and/or 605-18) corresponding to a request to initiate a process for disabling the security mode (e.g., a process for disabling the security mode at the computer system and, in some embodiments, one or more of the

electronic devices in the set of one or more electronic devices). In response to receiving the set of one or more inputs corresponding to a request to initiate the process for disabling the security mode, the computer system performs the following steps. In accordance with a determination that the set of one or more electronic devices (e.g., 610 and/or 620) other than the computer system are associated with the user account (and, in some embodiments, in accordance with a determination that the security mode is enabled at one or more of the electronic devices other than the security system), the computer system (e.g., 600) displays a user interface (e.g., 660) that includes one or more options (e.g., 660-1) (e.g., restart and/or disable options) for initiating a process to disable the security mode (e.g., including restarting (e.g., turning off and then turning back on) the computer system and the set of one or more electronic devices) at the computer system and the set of one or more electronic devices (e.g., 610 and/or 620). In some embodiments, the user interface includes a first disable option (e.g., 660-2) that is selectable to disable the security mode at (and restart) only the computer system and a second disable option (e.g., 660-1) that is selectable to initiate a process for disabling the security mode at (and restarting) the computer system and the set of one or more electronic devices. In some embodiments, the computer system disables the security mode (and restarts) automatically (e.g., without further user input) in response to selecting the first or second disable option. In some embodiments, the electronic devices other than the computer system do not automatically restart and disable the security mode in response to selecting the second disable option and, instead, display a prompt (e.g., 662) for confirming the restart/disable operation. In some embodiments, each of the electronic devices restart and disable the security mode after the restart/disable operation is confirmed at the respective electronic device. In accordance with a determination that the set of one or more electronic devices other than the computer system are not associated with the user account (or, in some embodiments, in accordance with a determination that the security mode is not enabled at the set of one or more electronic devices other than the security system), the computer system disables the security mode at the computer system (e.g., and restarting the computer system) without displaying the user interface (e.g., 660) that includes one or more options for initiating a process to disable the security mode at the computer system and the one or more electronic devices. Displaying the user interface that includes one or more options for initiating a process to disable the security mode at the computer system and the set of one or more electronic devices when the set of one or more electronic devices other than the computer system are associated with the user account, and disabling the security mode at the computer system without displaying the user interface when the set of one or more electronic

devices other than the computer system are not associated with the user account, reduces the number of inputs at the computer system by automatically disabling the security mode at the computer system without displaying additional options when no other devices are associated with the user account.

[0178] In some embodiments, in response to receiving the request (e.g., 605-5) to enable the security mode at the computer system (e.g., 600) and in accordance with the determination that the set of one or more electronic devices (e.g., 610 and/or 620) other than the computer system are associated with (e.g., logged into) the user account (e.g., electronic devices other than the computer system are also logged into the user account), the computer system forgoes enabling the security mode at the computer system (e.g., the security mode is not enabled in response to receiving the request (e.g., 605-5) to enable the security mode at the computer system when the set of one or more electronic devices other than the computer system are associated with the user account). Displaying the respective user interface that includes one or more options for enabling the security mode at the set of one or more electronic devices and the computer system without enabling the security mode at the computer system, reduces the number of inputs at the computer system by permitting the user to specify which devices should have the security mode enabled, thereby avoiding redundant or excessive inputs caused by having to navigate to a subsequent menu to select the respective devices after the security mode has been enabled for the computer system. In some embodiments, the security mode is enabled for the computer system and, optionally, the set of one or more electronic devices in response to input (e.g., 605-10 and/or 605-11) received at the respective user interface (e.g., 640) (which is displayed while the security mode is not enabled).

[0179] In some embodiments, displaying the respective user interface (e.g., 640) that includes one or more options for enabling the security mode at the set of one or more electronic devices (e.g., 610 and/or 620) and the computer system (e.g., 600) includes: displaying a first enable option (e.g., 640-2) (e.g., a restart or enable option for "just this device") that is selectable to enable the security mode at the computer system (e.g., 600) without enabling the security mode at the set of one or more electronic devices (e.g., 610 and/or 620) other than the computer system; and displaying a second enable option (e.g., 640-1) (e.g., a restart or enable option for "all devices") that is selectable to enable the security mode at the computer system and the set of one or more electronic devices. Displaying the

first enable option that is selectable to enable the security mode at the computer system without enabling the security mode at the set of one or more electronic devices other than the computer system, and displaying the second enable option that is selectable to enable the security mode at the computer system and the set of one or more electronic devices, provides additional control options for selecting which devices should have the security mode enabled without cluttering the UI with the additional displayed controls until they are needed.

[0180] In some embodiments, enabling the security mode at the computer system (e.g., 600) without enabling the security mode at the set of one or more electronic devices (e.g., 610 and/or 620) other than the computer system (e.g., in response to selecting the first enable option) includes: initiating a process for displaying (e.g., causing display of) within a predetermined period of time (e.g., 12 hours, 24 hours, or 36 hours), at the set of one or more electronic devices other than the computer system (e.g., at each respective device other than the computer system), a notification (e.g., 644 and/or 644-1) that is selectable to enable (e.g., for the respective device) the security mode at the set of one or more electronic devices other than the computer system. Initiating a process for displaying the notification that is selectable to enable the security mode at the set of one or more electronic devices other than the computer system improves security of the set of one or more electronic devices by prompting the user of the devices to enable the security mode. In some embodiments, if the option to enable the security mode at only the computer system is selected, a notification is displayed at each of the other electronic devices within a predetermined period of time, wherein the notification provides an option for enabling the lockdown mode at the respective device.

[0181] In some embodiments, enabling the security mode at the computer system (e.g., 600) and the set of one or more electronic devices (e.g., 610 and/or 620) (e.g., in response to selecting the second enable option) includes: enabling the security mode at the computer system and the set of one or more electronic devices without receiving additional input (e.g., without requiring further input and/or a confirmation input) at the set of one or more electronic devices (e.g., 610 and/or 620). Enabling the security mode at the computer system and the set of one or more electronic devices without receiving additional input at the set of one or more electronic devices reduces the number of inputs at the computer system and the set of one or more electronic devices by not requiring confirmation to enter the security mode and increases the security of the computer system and set of one or more electronic devices

by automatically enabling the security mode at the computer system and set of one or more electronic devices.

[0182] In some embodiments, enabling the security mode at the computer system (e.g., 600) (and/or the set of one or more electronic devices (e.g., 610 and/or 620)) includes restarting the computer system (and/or the set of one or more electronic devices). In some embodiments, disabling (e.g., exiting) the security mode at the computer system (and/or the set of one or more electronic devices) includes restarting the computer system (and/or the set of one or more electronic devices).

[0183] In some embodiments, enabling the security mode at the computer system includes: in accordance with a determination that the computer system is a first type of electronic device (e.g., 620) (e.g., a smartwatch or head-mounted device) that is associated with (e.g., linked and/or connected to (e.g., via direct wireless communication)) a second computer system (e.g., 600) (e.g., a smartphone, tablet, or laptop computer), enabling the security mode at the computer system (e.g., 620) and the second computer system (e.g., 600). Enabling the security mode at the computer system and the second computer system when the computer system is a first type of electronic device that is associated with the second computer system reduces the number of inputs at the computer system and the second computer system and increases the security of the computer system and the second computer system by automatically enabling the security mode at the computer system and the second computer system. In some embodiments, if the computer system is a smartwatch that is associated with another device such as a phone, tablet, or computer, the security mode is enabled for both the smartwatch and the associated device. In some embodiments, the respective user interface (e.g., 680) includes a first option (e.g., 680-2) (e.g., a "turn on for this watch and phone" option) that is selectable for enabling the security mode at only the computer system and the second computer system, and a second option (e.g., 680-1) (e.g., a "turn on for all devices" option) that is selectable for enabling the security mode at the computer system (e.g., 620), the second computer system (e.g., 600), and the set of one or more electronic devices (e.g., 610).

[0184] In some embodiments, the computer system (e.g., 600 and/or 610) receives a request (e.g., 605-12 and/or 605-13) to display a message (e.g., email, text message, and/or SMS message) that includes image data (e.g., 604 as shown in FIG. 6A) (e.g., a photo, video, and/or GIF). In response to receiving the request to display the message that includes image

data, the computer system displays the message, including: in accordance with a determination that the security mode is not enabled for the computer system, the computer system displays the message with the image data (e.g., as shown in FIG. 6A); and in accordance with a determination that the security mode is enabled for the computer system, the computer system displays the message without the image data (e.g., as shown in FIG. 6Q). Displaying the message without the image data when the security mode is enabled for the computer system improves security of the computer system by eliminating the processing of data that could jeopardize the security of the computer system. In some embodiments, the security mode limits the display of images in messages.

[0185] In some embodiments, the computer system (e.g., 600 and/or 610) receives a request (e.g., 605-15) to access a website (e.g., a webpage and/or a URL address) that does not meet security criteria (e.g., the website does not meet encryption, authentication, and/or other security criteria (e.g., a non-https website)). In response to receiving the request to access the website that does not meet security criteria: in accordance with a determination that the security mode is not enabled for the computer system, the computer system displays the website; and in accordance with a determination that the security mode is enabled for the computer system, the computer system displays a notification (e.g., 657 and/or 658) without displaying the website (e.g., a notification indicating that the website does not meet security criteria). Displaying the notification without displaying the website when the security mode is enabled for the computer system improves security of the computer system by eliminating the processing of data that could jeopardize the security of the computer system. In some embodiments, the notification includes an option (e.g., 658-1) to continue to the website. In some embodiments, the notification includes an option (e.g., 658-2) to cancel the request to access the website. In some embodiments, the security mode limits access to websites that do not meet security criteria.

[0186] The foregoing description, for purpose of explanation, has been described with reference to specific embodiments. However, the illustrative discussions above are not intended to be exhaustive or to limit the invention to the precise forms disclosed. Many modifications and variations are possible in view of the above teachings. The embodiments were chosen and described in order to best explain the principles of the techniques and their practical applications. Others skilled in the art are thereby enabled to best utilize the

techniques and various embodiments with various modifications as are suited to the particular use contemplated.

[0187] Although the disclosure and examples have been fully described with reference to the accompanying drawings, it is to be noted that various changes and modifications will become apparent to those skilled in the art. Such changes and modifications are to be understood as being included within the scope of the disclosure and examples as defined by the claims.

[0188] As described above, one aspect of the present technology is the gathering and use of data available from various sources to enable a security mode at one or more computer systems. The present disclosure contemplates that in some instances, this gathered data may include personal information data that uniquely identifies or can be used to contact or locate a specific person. Such personal information data can include demographic data, location-based data, telephone numbers, email addresses, social network IDs, home addresses, data or records relating to a user's health or level of fitness (e.g., vital signs measurements, medication information, exercise information), date of birth, or any other identifying or personal information.

[0189] The present disclosure recognizes that the use of such personal information data, in the present technology, can be used to the benefit of users. Further, other uses for personal information data that benefit the user are also contemplated by the present disclosure. For instance, health and fitness data may be used to provide insights into a user's general wellness, or may be used as positive feedback to individuals using technology to pursue wellness goals.

[0190] The present disclosure contemplates that the entities responsible for the collection, analysis, disclosure, transfer, storage, or other use of such personal information data will comply with well-established privacy policies and/or privacy practices. In particular, such entities should implement and consistently use privacy policies and practices that are generally recognized as meeting or exceeding industry or governmental requirements for maintaining personal information data private and secure. Such policies should be easily accessible by users, and should be updated as the collection and/or use of data changes. Personal information from users should be collected for legitimate and reasonable uses of the entity and not shared or sold outside of those legitimate uses. Further, such collection/sharing

should occur after receiving the informed consent of the users. Additionally, such entities should consider taking any needed steps for safeguarding and securing access to such personal information data and ensuring that others with access to the personal information data adhere to their privacy policies and procedures. Further, such entities can subject themselves to evaluation by third parties to certify their adherence to widely accepted privacy policies and practices. In addition, policies and practices should be adapted for the particular types of personal information data being collected and/or accessed and adapted to applicable laws and standards, including jurisdiction-specific considerations. For instance, in the US, collection of or access to certain health data may be governed by federal and/or state laws, such as the Health Insurance Portability and Accountability Act (HIPAA); whereas health data in other countries may be subject to other regulations and policies and should be handled accordingly. Hence different privacy practices should be maintained for different personal data types in each country.

[0191] Despite the foregoing, the present disclosure also contemplates embodiments in which users selectively block the use of, or access to, personal information data. That is, the present disclosure contemplates that hardware and/or software elements can be provided to prevent or block access to such personal information data. For example, the present technology can be configured to allow users to select to "opt in" or "opt out" of participation in the collection of personal information data. In addition to providing "opt in" and "opt out" options, the present disclosure contemplates providing notifications relating to the access or use of personal information. For instance, a user may be notified upon downloading an app that their personal information data will be accessed and then reminded again just before personal information data is accessed by the app.

[0192] Moreover, it is the intent of the present disclosure that personal information data should be managed and handled in a way to minimize risks of unintentional or unauthorized access or use. Risk can be minimized by limiting the collection of data and deleting data once it is no longer needed. In addition, and when applicable, including in certain health related applications, data de-identification can be used to protect a user's privacy. De-identification may be facilitated, when appropriate, by removing specific identifiers (e.g., date of birth, etc.), controlling the amount or specificity of data stored (e.g., collecting location data a city level rather than at an address level), controlling how data is stored (e.g., aggregating data across users), and/or other methods.

[0193] Therefore, although the present disclosure broadly covers use of personal information data to implement one or more various disclosed embodiments, the present disclosure also contemplates that the various embodiments can also be implemented without the need for accessing such personal information data. That is, the various embodiments of the present technology are not rendered inoperable due to the lack of all or a portion of such personal information data. For example, a security mode can be enabled at one or more computer systems using non-personal information data or a bare minimum amount of personal information, such as the content being requested by the device associated with a user, other non-personal information, or publicly available information.

CLAIMS

What is claimed is:

1. A method, comprising:

at a computer system that is in communication with a display generation component and one or more input devices:

receiving, via the one or more input devices, a request to enable a security mode at the computer system, wherein the computer system is associated with a user account; and

in response to receiving the request to enable the security mode at the computer system:

in accordance with a determination that a set of one or more electronic devices other than the computer system are associated with the user account, displaying a respective user interface that includes one or more options for enabling the security mode at the set of one or more electronic devices and the computer system; and

in accordance with a determination that a set of one or more electronic devices other than the computer system are not associated with the user account, enabling the security mode at the computer system without displaying the respective user interface that includes one or more options for enabling the security mode at the set of one or more electronic devices and the computer system.

2. The method of claim 1, wherein:

the security mode is disabled at the computer system in response to a request to disable the security mode received at the computer system; and

the security mode is disabled at a first electronic device in the set of one or more electronic devices in response to a request to disable the security mode received at the first electronic device.

3. The method of any of claims 1-2, further comprising:

while the security mode is enabled at the computer system, receiving a set of one or more inputs corresponding to a request to initiate a process for disabling the security mode; and

in response to receiving the set of one or more inputs corresponding to a request to initiate the process for disabling the security mode:

in accordance with a determination that the set of one or more electronic devices other than the computer system are associated with the user account, displaying a user interface that includes one or more options for initiating a process to disable the security mode at the computer system and the set of one or more electronic devices; and

in accordance with a determination that the set of one or more electronic devices other than the computer system are not associated with the user account, disabling the security mode at the computer system without displaying the user interface that includes one or more options for initiating a process to disable the security mode at the computer system and the one or more electronic devices.

4. The method of any of claims 1-3, in response to receiving the request to enable the security mode at the computer system and in accordance with the determination that the set of one or more electronic devices other than the computer system are associated with the user account, forgoing enabling the security mode at the computer system.

5. The method of any of claims 1-4, wherein displaying the respective user interface that includes one or more options for enabling the security mode at the set of one or more electronic devices and the computer system includes:

displaying a first enable option that is selectable to enable the security mode at the computer system without enabling the security mode at the set of one or more electronic devices other than the computer system; and

displaying a second enable option that is selectable to enable the security mode at the computer system and the set of one or more electronic devices.

6. The method of claim 5, wherein enabling the security mode at the computer system without enabling the security mode at the set of one or more electronic devices other than the computer system includes:

initiating a process for displaying within a predetermined period of time, at the set of one or more electronic devices other than the computer system, a notification that is selectable to enable the security mode at the set of one or more electronic devices other than the computer system.

7. The method of any of claims 5-6, wherein enabling the security mode at the computer system and the set of one or more electronic devices includes:

enabling the security mode at the computer system and the set of one or more electronic devices without receiving additional input at the set of one or more electronic devices.

8. The method of any of claims 1-7, wherein enabling the security mode at the computer system includes restarting the computer system.

9. The method of any of claims 1-8, wherein disabling the security mode at the computer system includes restarting the computer system.

10. The method of any of claims 1-9, wherein enabling the security mode at the computer system includes:

in accordance with a determination that the computer system is a first type of electronic device that is associated with a second computer system, enabling the security mode at the computer system and the second computer system.

11. The method of any of claims 1-10, further comprising:

receiving a request to display a message that includes image data; and

in response to receiving the request to display the message that includes image data, displaying the message, including:

in accordance with a determination that the security mode is not enabled for the computer system, displaying the message with the image data; and

in accordance with a determination that the security mode is enabled for the computer system, displaying the message without the image data.

12. The method of any of claims 1-11, further comprising:

receiving a request to access a website that does not meet security criteria; and

in response to receiving the request to access the website that does not meet security criteria:

in accordance with a determination that the security mode is not enabled for the computer system, displaying the website; and

in accordance with a determination that the security mode is enabled for the computer system, displaying a notification without displaying the website.

13. A non-transitory computer-readable storage medium storing one or more programs configured to be executed by one or more processors of a computer system that is in

communication with a display generation component and one or more input devices, the one or more programs including instructions for performing the method of any of claims 1-12.

14. A computer system that is configured to communicate with a display generation component and one or more input devices, the computer system comprising:

one or more processors; and

memory storing one or more programs configured to be executed by the one or more processors, the one or more programs including instructions for performing the method of any of claims 1-12.

15. A computer system that is configured to communicate with a display generation component and one or more input devices, comprising:

means for performing the method of any of claims 1-12.

16. A computer program product, comprising one or more programs configured to be executed by one or more processors of a computer system that is in communication with a display generation component and one or more input devices, the one or more programs including instructions for performing the method of any of claims 1-12.

17. A non-transitory computer-readable storage medium storing one or more programs configured to be executed by one or more processors of a computer system that is in communication with a display generation component and one or more input devices, the one or more programs including instructions for:

receiving, via the one or more input devices, a request to enable a security mode at the computer system, wherein the computer system is associated with a user account; and

in response to receiving the request to enable the security mode at the computer system:

in accordance with a determination that a set of one or more electronic devices other than the computer system are associated with the user account, displaying a respective user interface that includes one or more options for enabling the security mode at the set of one or more electronic devices and the computer system; and

in accordance with a determination that a set of one or more electronic devices other than the computer system are not associated with the user account, enabling the security mode at the computer system without displaying the respective user interface that includes

one or more options for enabling the security mode at the set of one or more electronic devices and the computer system.

18. A computer system configured to communicate with a display generation component and one or more input devices, comprising:

one or more processors; and

memory storing one or more programs configured to be executed by the one or more processors, the one or more programs including instructions for:

receiving, via the one or more input devices, a request to enable a security mode at the computer system, wherein the computer system is associated with a user account; and

in response to receiving the request to enable the security mode at the computer system:

in accordance with a determination that a set of one or more electronic devices other than the computer system are associated with the user account, displaying a respective user interface that includes one or more options for enabling the security mode at the set of one or more electronic devices and the computer system; and

in accordance with a determination that a set of one or more electronic devices other than the computer system are not associated with the user account, enabling the security mode at the computer system without displaying the respective user interface that includes one or more options for enabling the security mode at the set of one or more electronic devices and the computer system.

19. A computer system configured to communicate with a display generation component and one or more input devices, comprising:

means for receiving, via the one or more input devices, a request to enable a security mode at the computer system, wherein the computer system is associated with a user account; and

means for, in response to receiving the request to enable the security mode at the computer system:

in accordance with a determination that a set of one or more electronic devices other than the computer system are associated with the user account, displaying a respective user interface that includes one or more options for enabling the security mode at the set of one or more electronic devices and the computer system; and

in accordance with a determination that a set of one or more electronic devices other than the computer system are not associated with the user account, enabling the security mode at the computer system without displaying the respective user interface that includes one or more options for enabling the security mode at the set of one or more electronic devices and the computer system.

20. A computer program product, comprising one or more programs configured to be executed by one or more processors of a computer system that is in communication with a display generation component and one or more input devices, the one or more programs including instructions for:

receiving, via the one or more input devices, a request to enable a security mode at the computer system, wherein the computer system is associated with a user account; and

in response to receiving the request to enable the security mode at the computer system:

in accordance with a determination that a set of one or more electronic devices other than the computer system are associated with the user account, displaying a respective user interface that includes one or more options for enabling the security mode at the set of one or more electronic devices and the computer system; and

in accordance with a determination that a set of one or more electronic devices other than the computer system are not associated with the user account, enabling the security mode at the computer system without displaying the respective user interface that includes one or more options for enabling the security mode at the set of one or more electronic devices and the computer system.

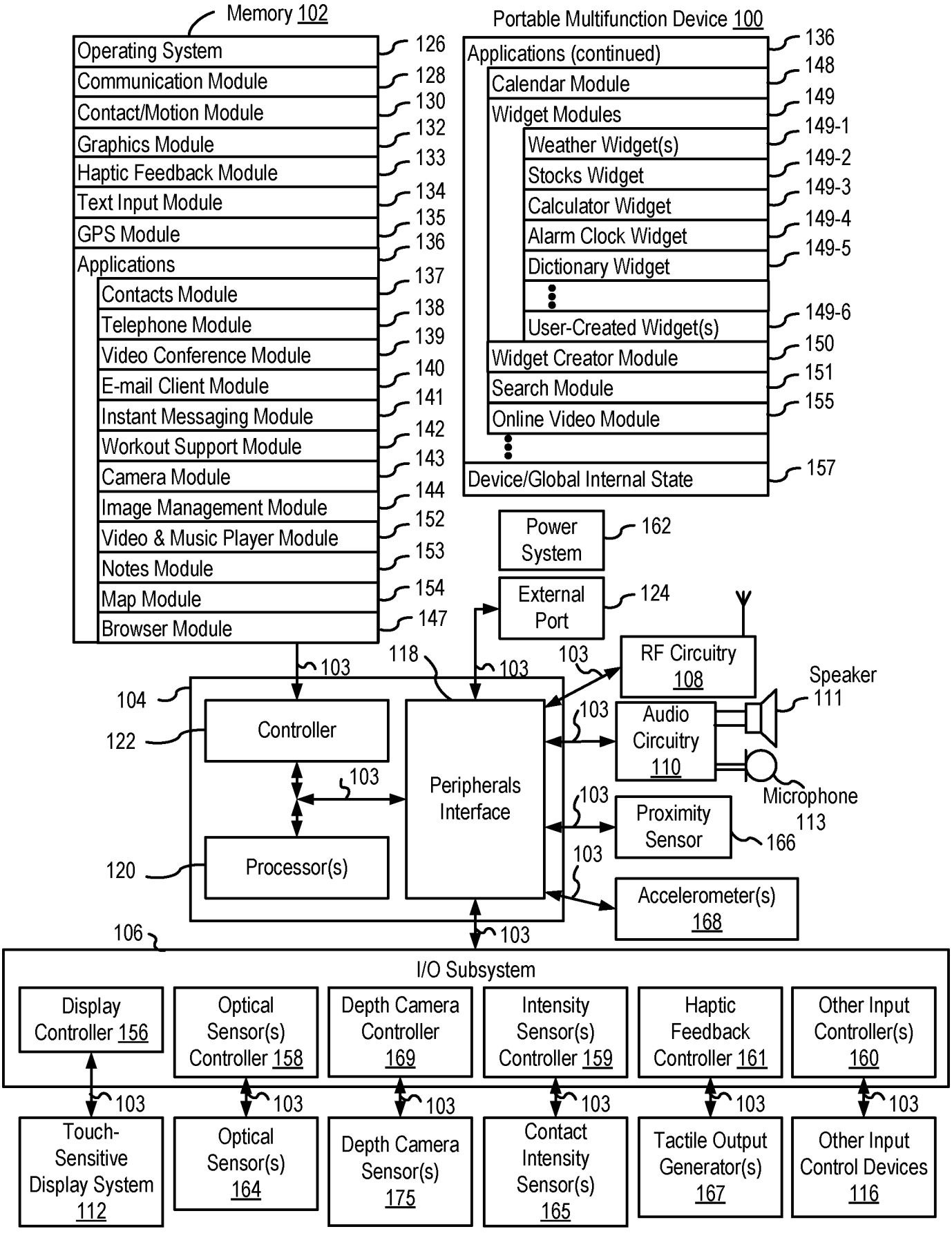

Memory 102
Operating System
126
Communication Module
128
Contact/Motion Module
130
Graphics Module
132
Haptic Feedback Module
133
Text Input Module
134
GPS Module
135
Applications
136
Contacts Module
137
Telephone Module
138
Video Conference Module
139
E-mail Client Module
140
Instant Messaging Module
141
Workout Support Module
142
Camera Module
143
Image Management Module
144
Video & Music Player Module
152
Notes Module
153
Map Module
154
Browser Module
147
Portable Multifunction Device 100
Applications (continued)
136
Calendar Module
148
Widget Modules
149
Weather Widget(s)
149-1
Stocks Widget
149-2
Calculator Widget
149-3
Alarm Clock Widget
149-4
Dictionary Widget
149-5
User-Created Widget(s)
149-6
Widget Creator Module
150
Search Module
151
Online Video Module
155
Device/Global Internal State
157
Power System
162
External Port
124
RF Circuitry 108
Speaker 111
Audio Circuitry 110
Microphone 113
Proximity Sensor
166
Accelerometer(s) 168
Controller
122
Processor(s)
120
Peripherals Interface
104
118
103
I/O Subsystem
106
Display Controller 156
Optical Sensor(s) Controller 158
Depth Camera Controller 169
Intensity Sensor(s) Controller 159
Haptic Feedback Controller 161
Other Input Controller(s) 160
Touch-Sensitive Display System 112
Optical Sensor(s) 164
Depth Camera Sensor(s) 175
Contact Intensity Sensor(s) 165
Tactile Output Generator(s) 167
Other Input Control Devices 116

FIG. 1A

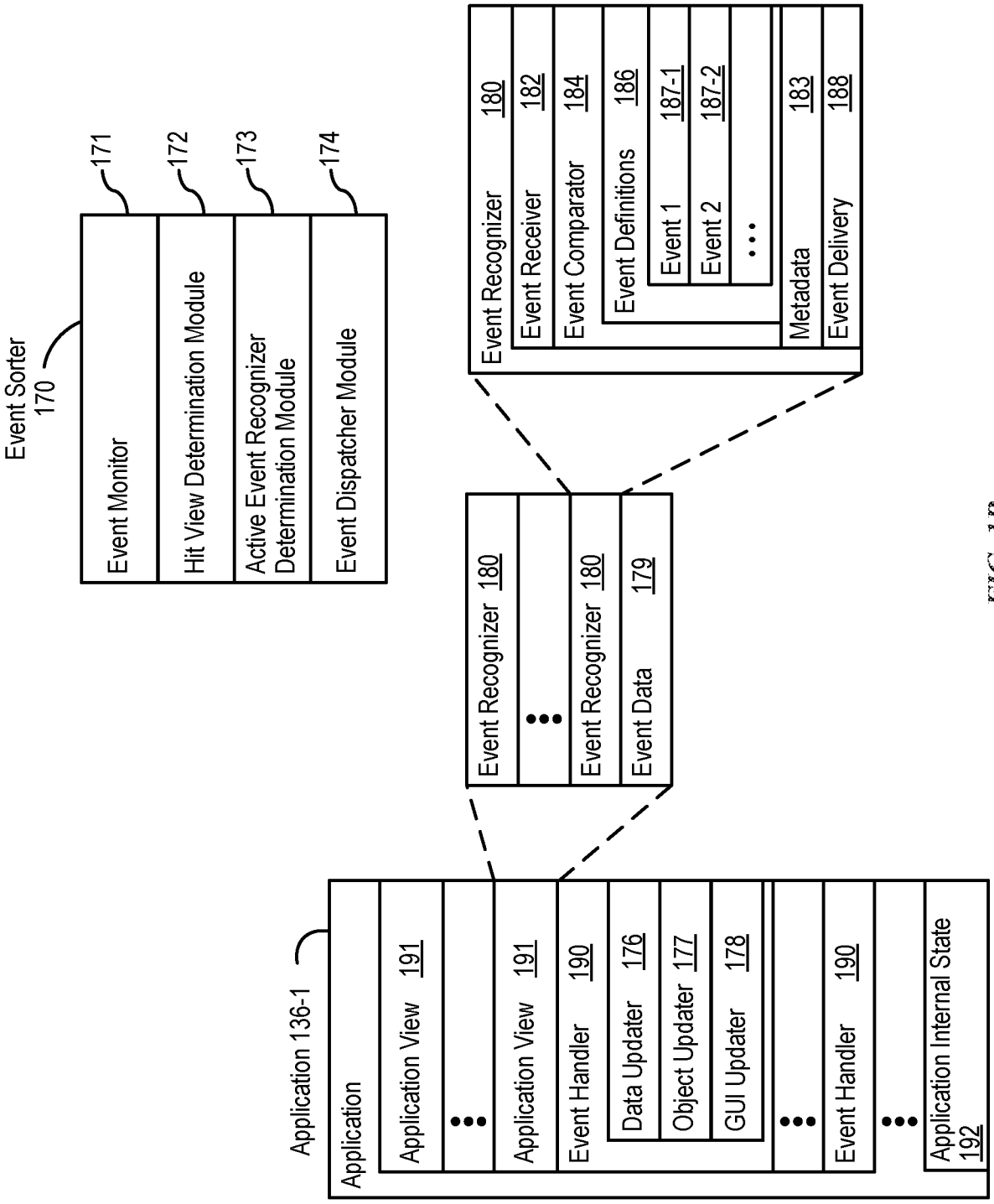

Event Sorter 170
Event Monitor
171
Hit View Determination Module
172
Active Event Recognizer Determination Module
173
Event Dispatcher Module
174
Application 136-1
Application
Application View 191
Application View 191
Event Handler 190
Data Updater 176
Object Updater 177
GUI Updater 178
Event Handler 190
Application Internal State 192
Event Recognizer 180
Event Recognizer 180
Event Data 179
Event Recognizer 180
Event Receiver 182
Event Comparator 184
Event Definitions 186
Event 1 187-1
Event 2 187-2
Metadata 183
Event Delivery 188

FIG. 1B

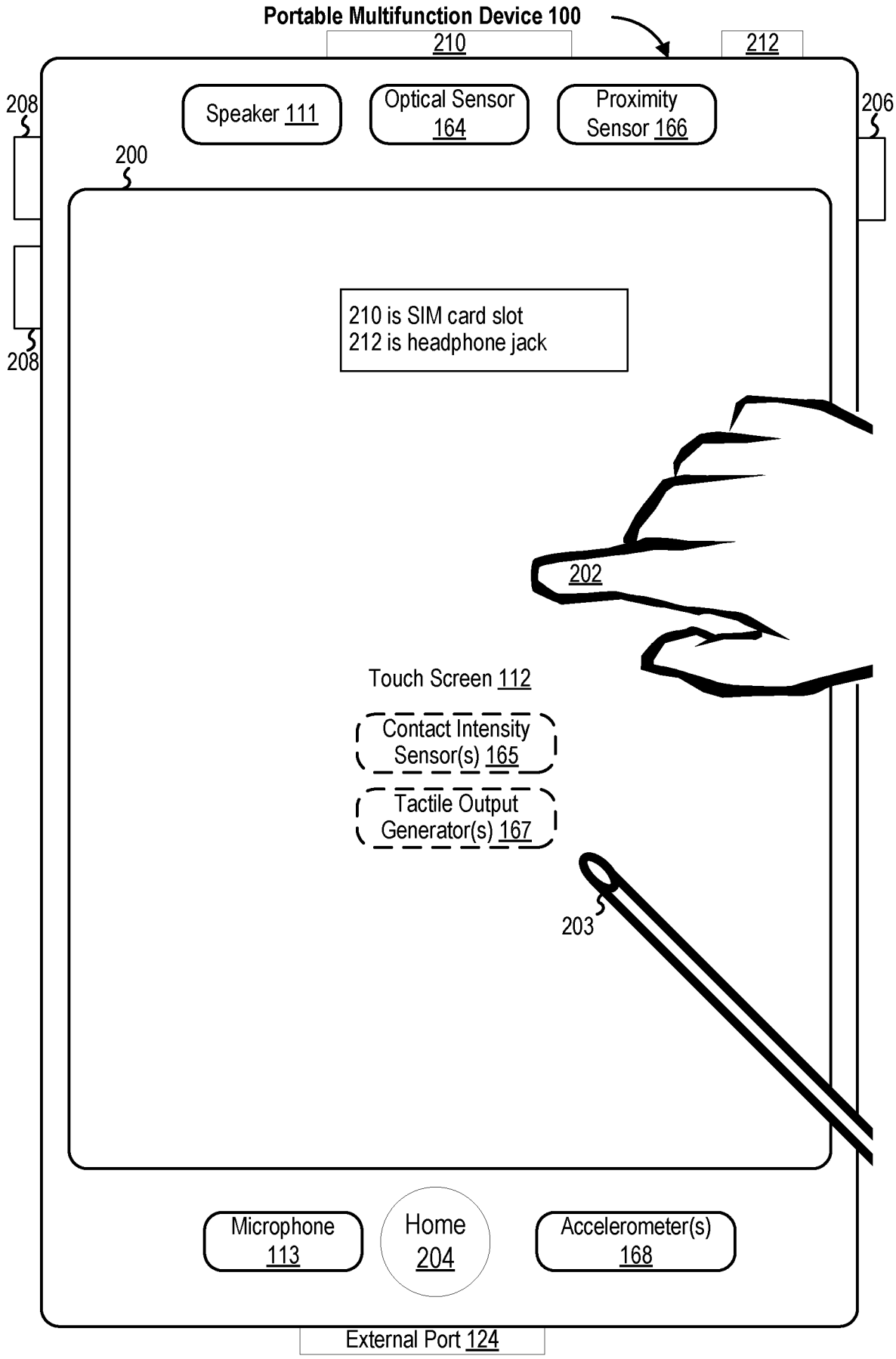

Portable Multifunction Device 100
210
212
208
Speaker 111
Optical Sensor 164
Proximity Sensor 166
206
200
210 is SIM card slot
212 is headphone jack
208
202
Touch Screen 112
Contact Intensity Sensor(s) 165
Tactile Output Generator(s) 167
203
Microphone 113
Home 204
Accelerometer(s) 168
External Port 124

FIG. 2

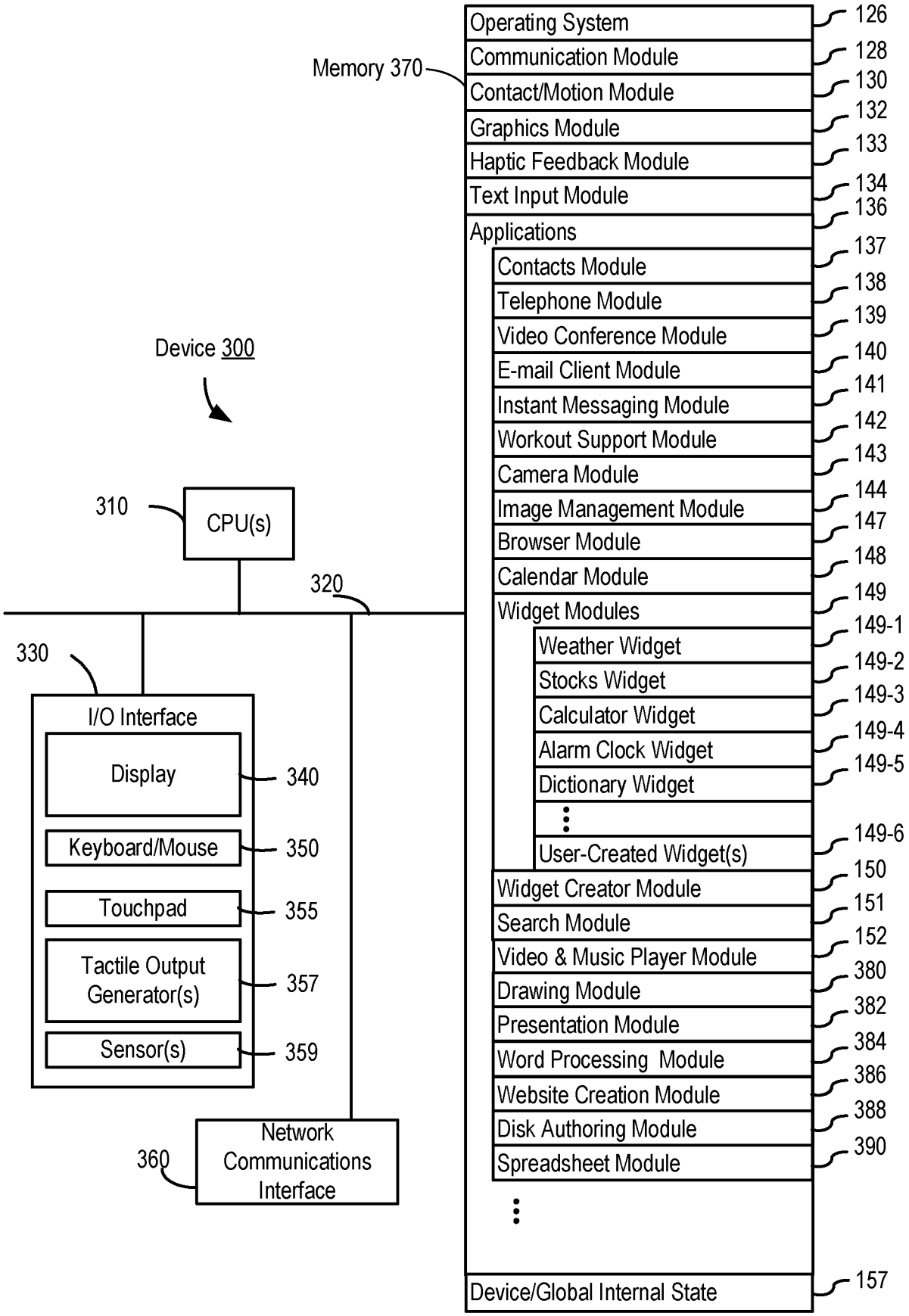

Memory 370
Operating System
126
Communication Module
128
Contact/Motion Module
130
Graphics Module
132
Haptic Feedback Module
133
Text Input Module
134
Applications
136
Contacts Module
137
Telephone Module
138
Video Conference Module
139
E-mail Client Module
140
Instant Messaging Module
141
Workout Support Module
142
Camera Module
143
Image Management Module
144
Browser Module
147
Calendar Module
148
Widget Modules
149
Weather Widget
149-1
Stocks Widget
149-2
Calculator Widget
149-3
Alarm Clock Widget
149-4
Dictionary Widget
149-5
User-Created Widget(s)
149-6
Widget Creator Module
150
Search Module
151
Video & Music Player Module
152
Drawing Module
380
Presentation Module
382
Word Processing Module
384
Website Creation Module
386
Disk Authoring Module
388
Spreadsheet Module
390
Device/Global Internal State
157
Device 300
310
CPU(s)
320
330
I/O Interface
Display
340
Keyboard/Mouse
350
Touchpad
355
Tactile Output Generator(s)
357
Sensor(s)
359
360
Network Communications Interface

FIG. 3

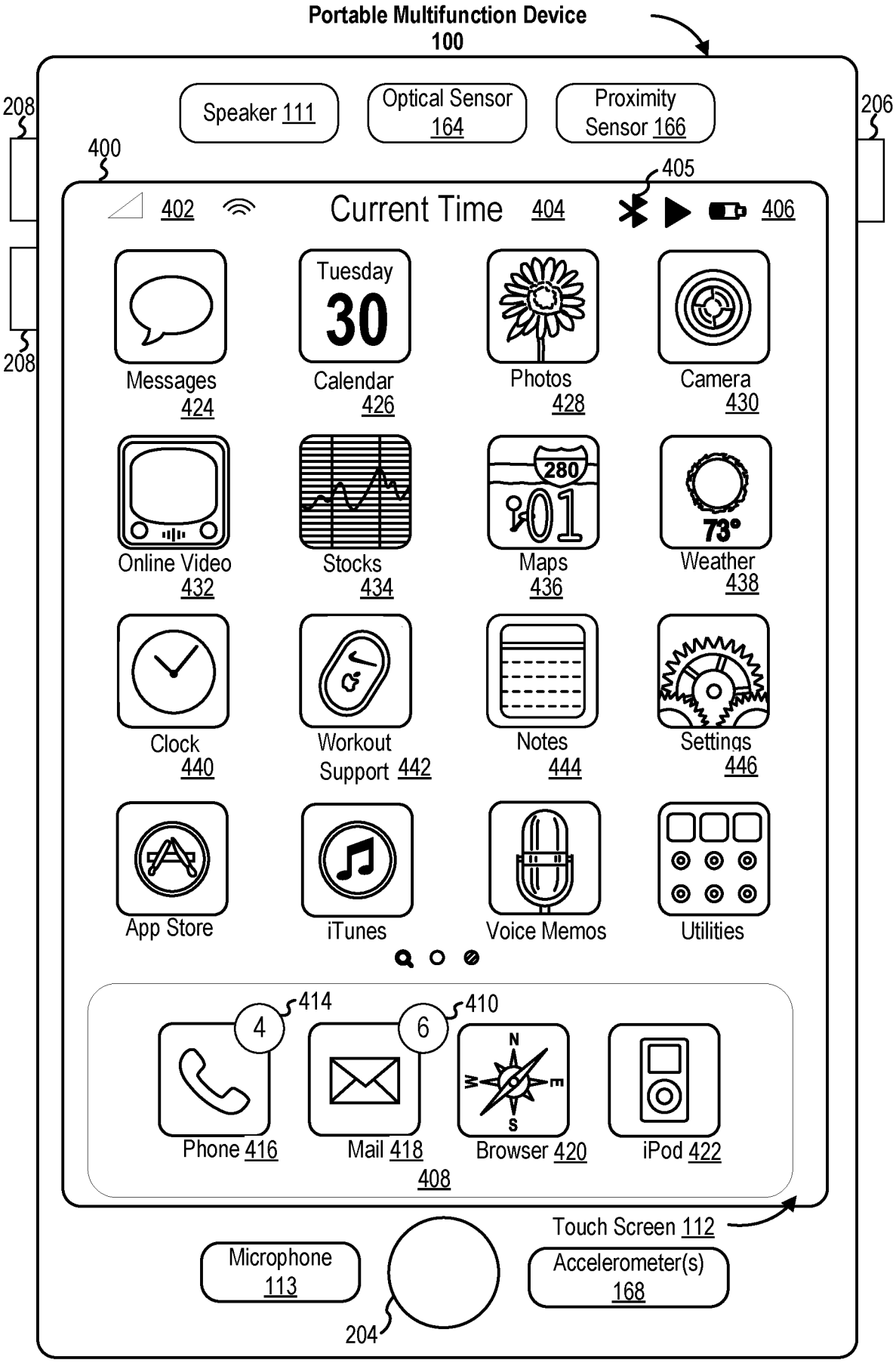
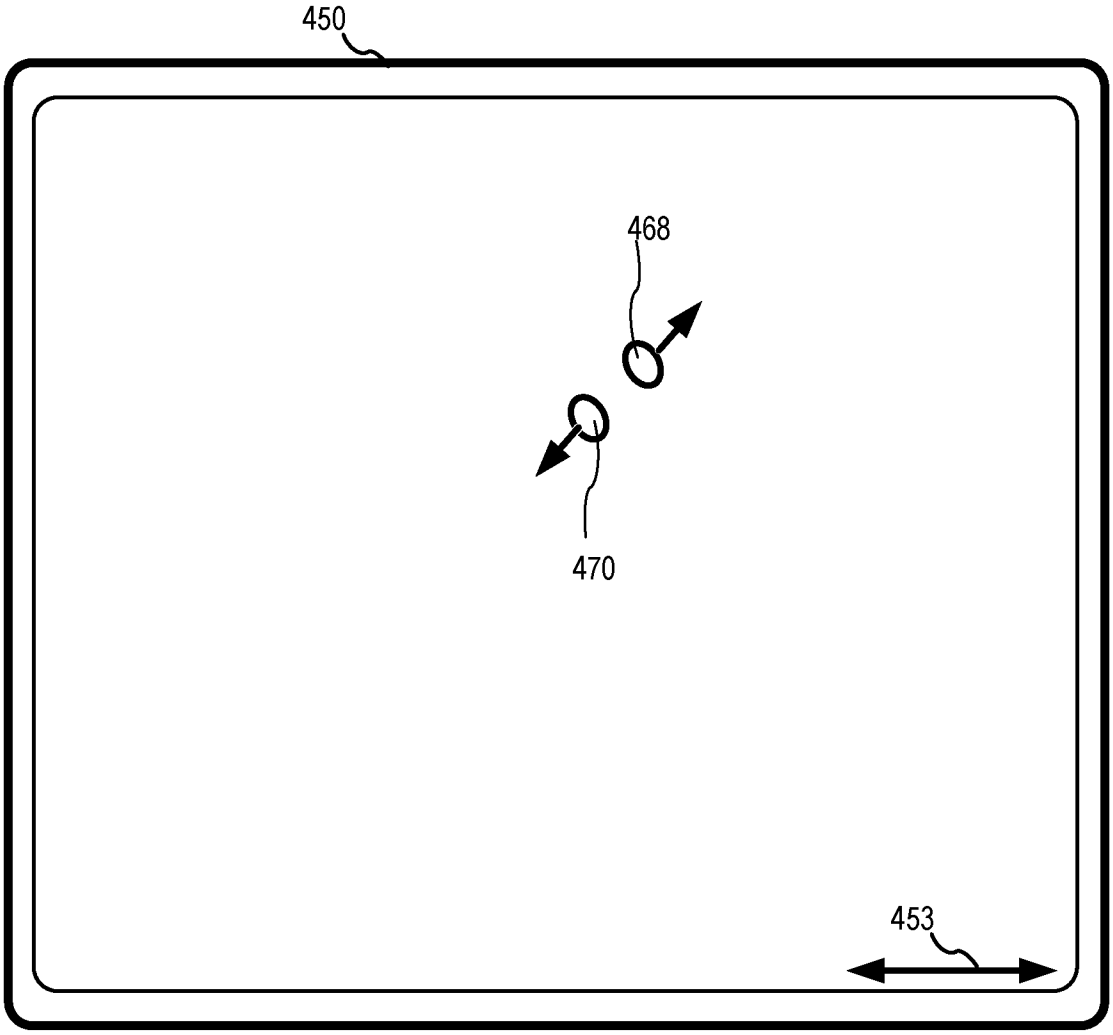

Portable Multifunction Device
100
Speaker 111
Optical Sensor 164
Proximity Sensor 166
208
206
400
405
402
Current Time 404
406
Messages 424
Tuesday 30
Calendar 426
Photos 428
Camera 430
Online Video 432
Stocks 434
280
Maps 436
73°
Weather 438
Clock 440
Workout Support 442
Notes 444
Settings 446
App Store
iTunes
Voice Memos
Utilities
414
410
4
6
Phone 416
Mail 418
Browser 420
iPod 422
408
Touch Screen 112
Microphone 113
Accelerometer(s) 168
204

FIG. 4A


450
468
470
453

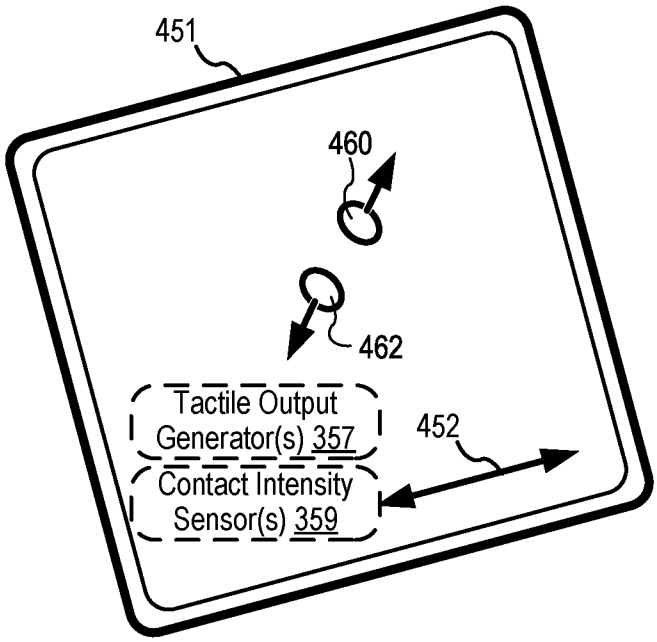

451
460
462
Tactile Output Generator(s) 357
Contact Intensity Sensor(s) 359
452

FIG. 4B

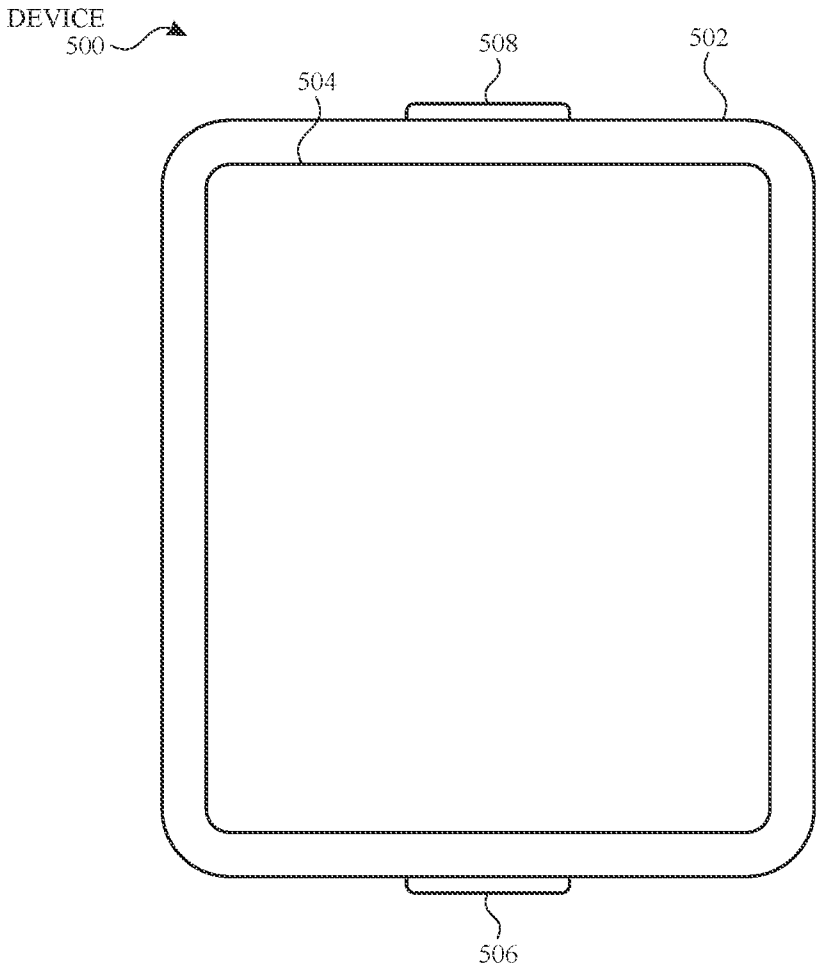


FIG. 5A

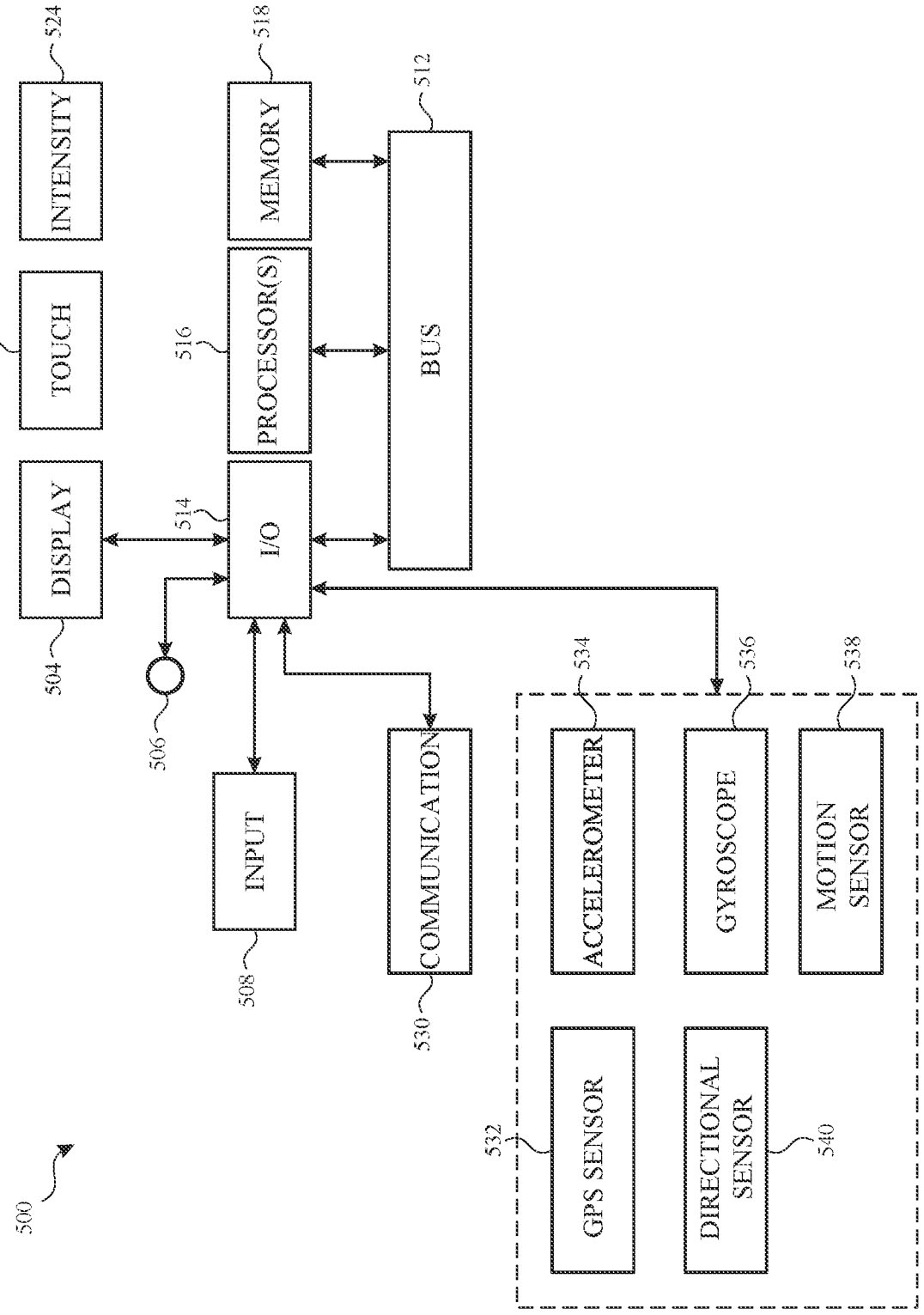

500
DISPLAY
504
TOUCH
522
INTENSITY
524
506
INPUT
508
I/O
514
PROCESSOR(S)
516
MEMORY
518
BUS
512
COMMUNICATION
530
ACCELEROMETER
534
GYROSCOPE
536
MOTION SENSOR
538
GPS SENSOR
532
DIRECTIONAL SENSOR
540

FIG. 5B

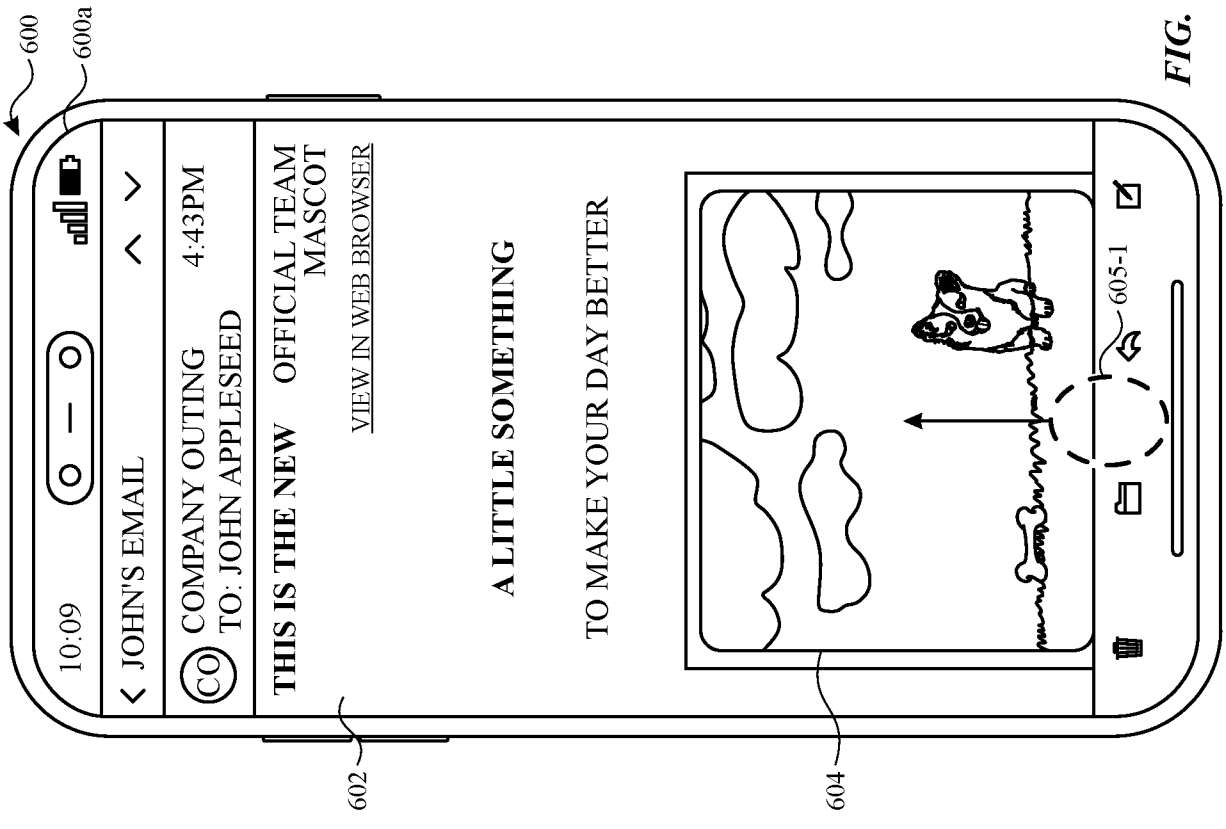

600
600a
10:09
JOHN'S EMAIL
COMPANY OUTING 4:43PM
TO: JOHN APPLESEED
THIS IS THE NEW OFFICIAL TEAM MASCOT
VIEW IN WEB BROWSER
A LITTLE SOMETHING
TO MAKE YOUR DAY BETTER
602
604
605-1

FIG. 6A

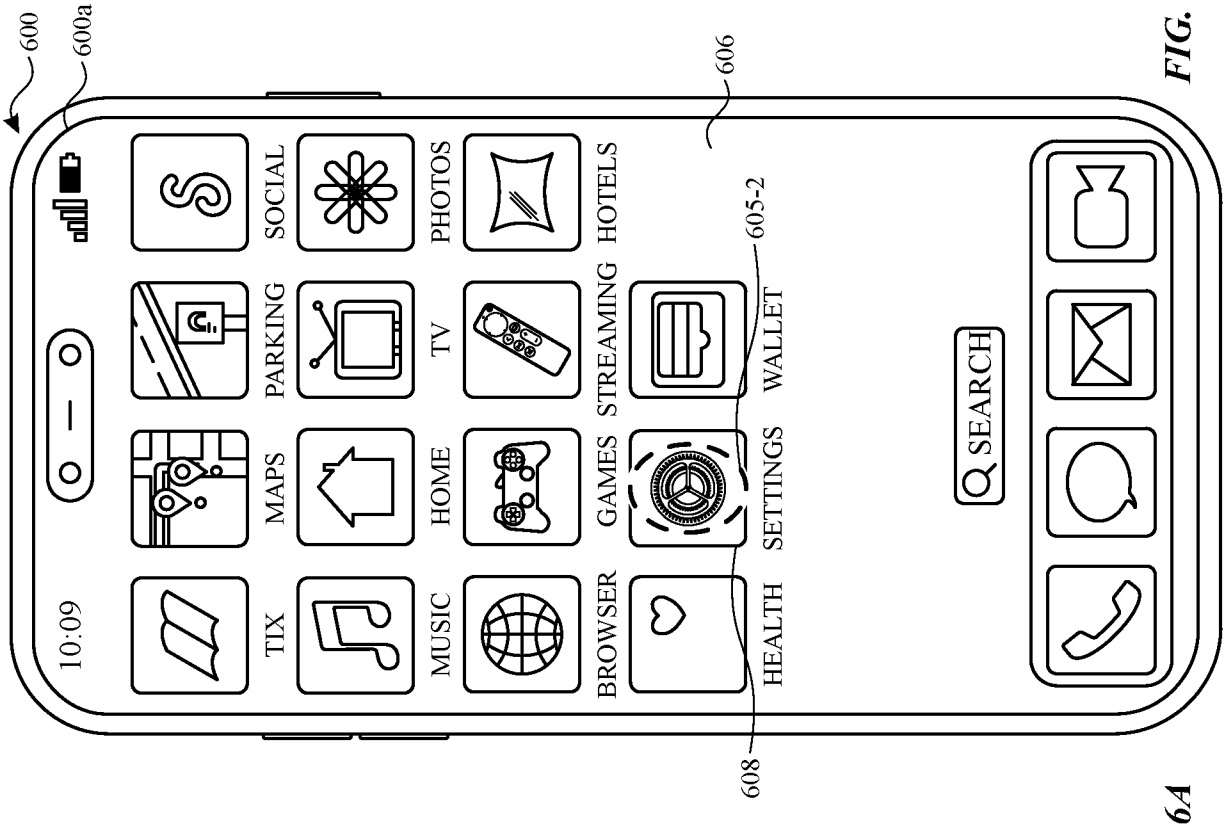

600
600a
10:09
TIX
MAPS
HOME
PARKING
TV
SOCIAL
MUSIC
GAMES
STREAMING
PHOTOS
BROWSER
SETTINGS
WALLET
HOTELS
HEALTH
SEARCH
606
608
605-2

FIG. 6B

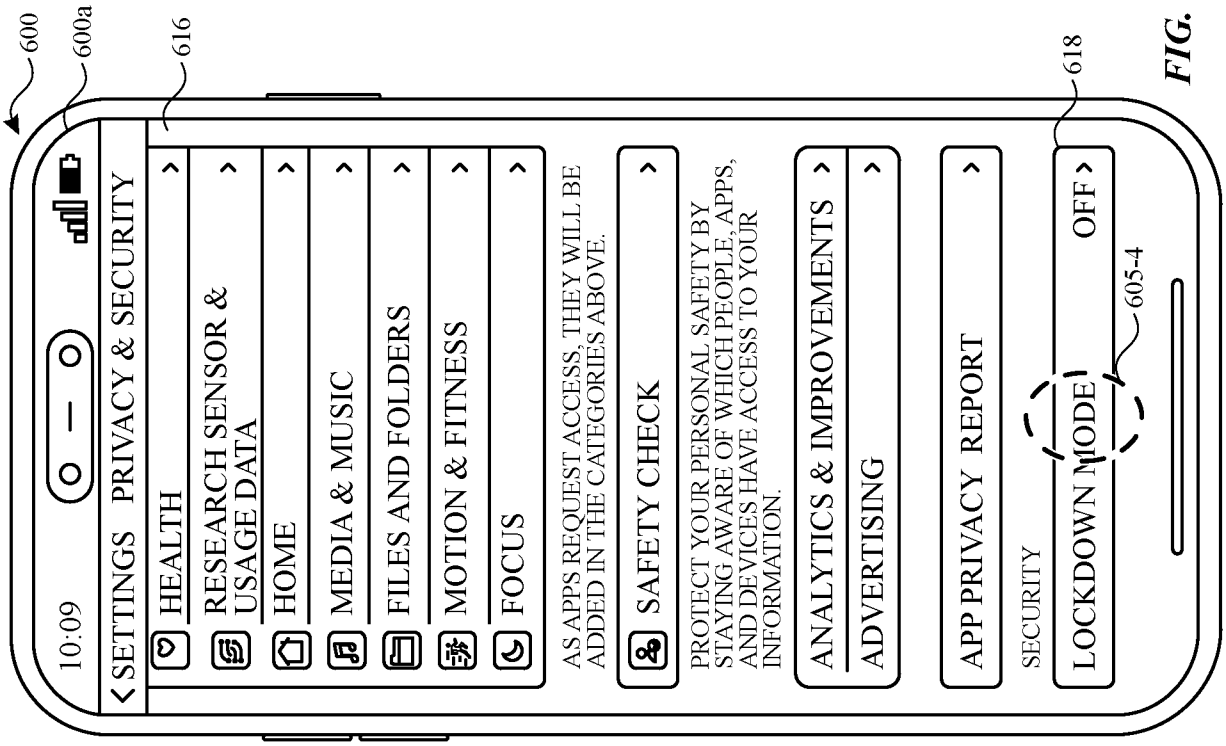

600
600a
616
10:09
SETTINGS PRIVACY & SECURITY
HEALTH
RESEARCH SENSOR & USAGE DATA
HOME
MEDIA & MUSIC
FILES AND FOLDERS
MOTION & FITNESS
FOCUS
AS APPS REQUEST ACCESS, THEY WILL BE ADDED IN THE CATEGORIES ABOVE.
SAFETY CHECK
PROTECT YOUR PERSONAL SAFETY BY STAYING AWARE OF WHICH PEOPLE, APPS, AND DEVICES HAVE ACCESS TO YOUR INFORMATION.
ANALYTICS & IMPROVEMENTS
ADVERTISING
APP PRIVACY REPORT
SECURITY
LOCKDOWN MODE
OFF
618
605-4

FIG. 6D

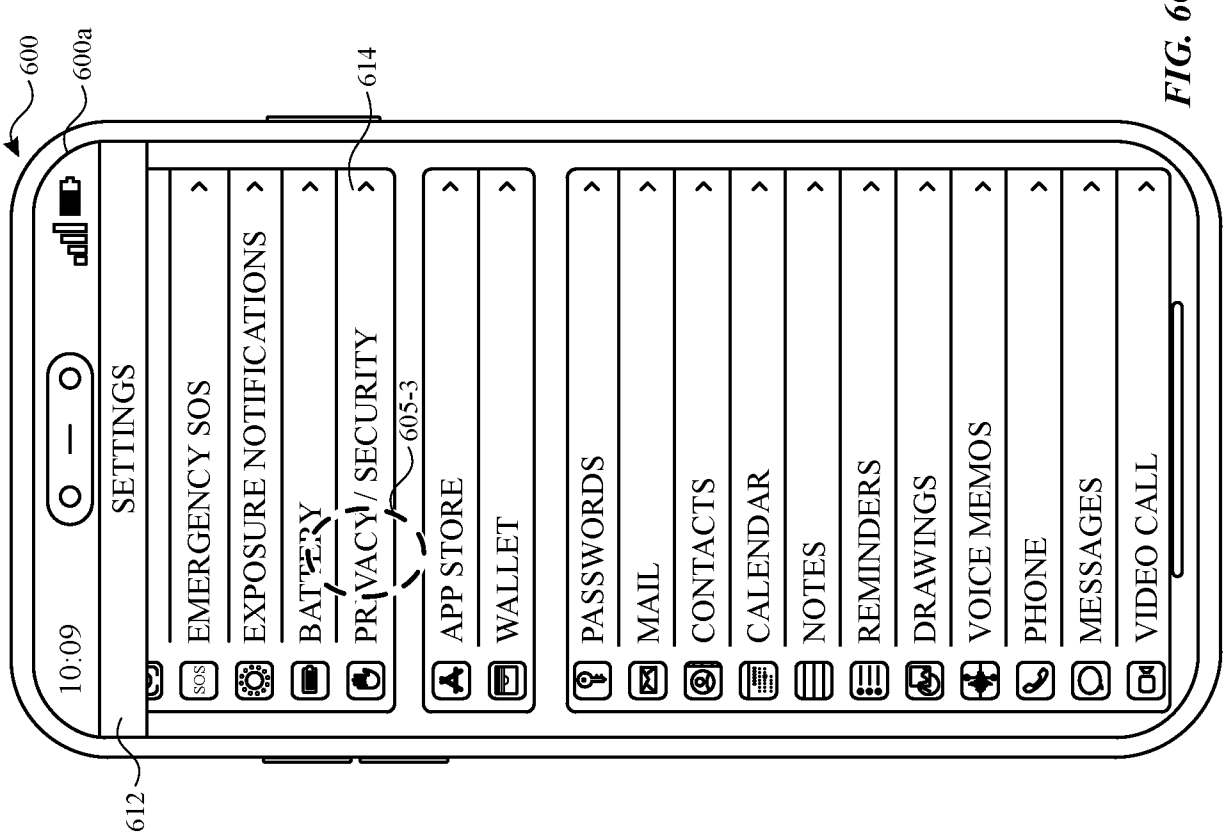

600
600a
614
612
10:09
SETTINGS
EMERGENCY SOS
EXPOSURE NOTIFICATIONS
BATTERY
PRIVACY / SECURITY
605-3
APP STORE
WALLET
PASSWORDS
MAIL
CONTACTS
CALENDAR
NOTES
REMINDERS
DRAWINGS
VOICE MEMOS
PHONE
MESSAGES
VIDEO CALL

FIG. 6C

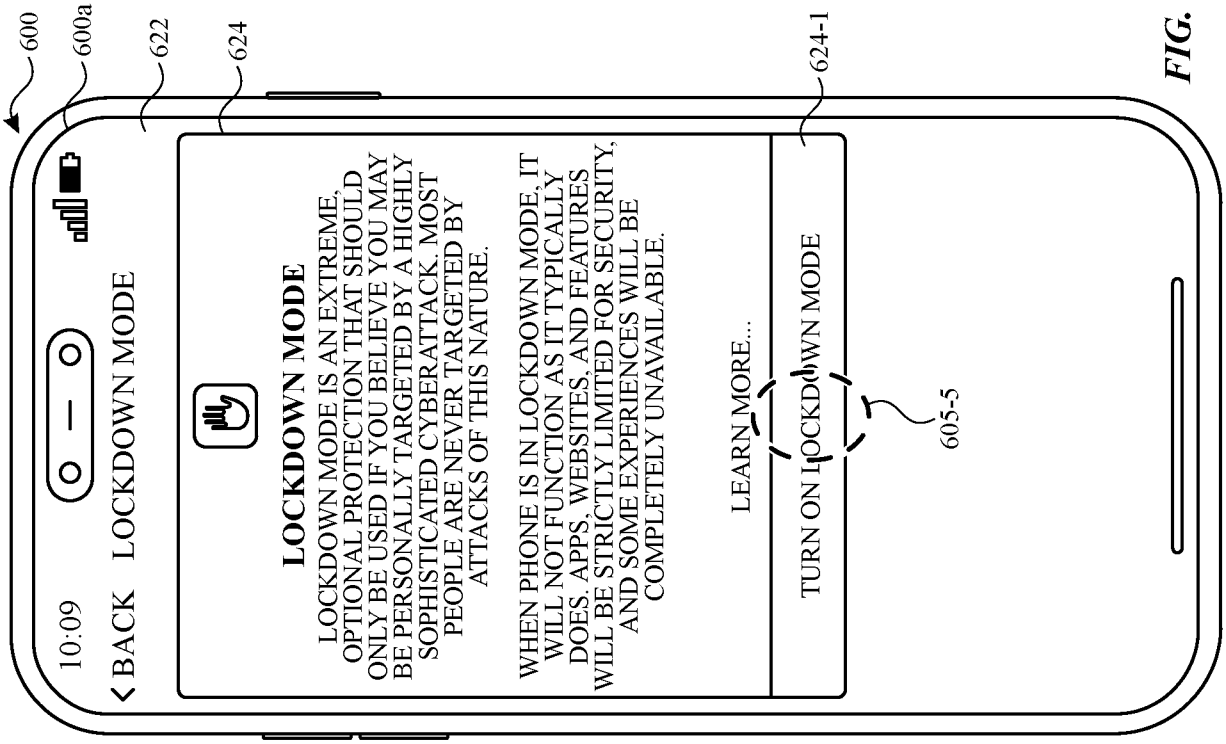

600
600a
10:09
BACK LOCKDOWN MODE
LOCKDOWN MODE
LOCKDOWN MODE IS AN EXTREME, OPTIONAL PROTECTION THAT SHOULD ONLY BE USED IF YOU BELIEVE YOU MAY BE PERSONALLY TARGETED BY A HIGHLY SOPHISTICATED CYBERATTACK. MOST PEOPLE ARE NEVER TARGETED BY ATTACKS OF THIS NATURE.
WHEN PHONE IS IN LOCKDOWN MODE, IT WILL NOT FUNCTION AS IT TYPICALLY DOES. APPS, WEBSITES, AND FEATURES WILL BE STRICTLY LIMITED FOR SECURITY, AND SOME EXPERIENCES WILL BE COMPLETELY UNAVAILABLE.
LEARN MORE...
TURN ON LOCKDOWN MODE
622
624
624-1
605-5

FIG. 6E

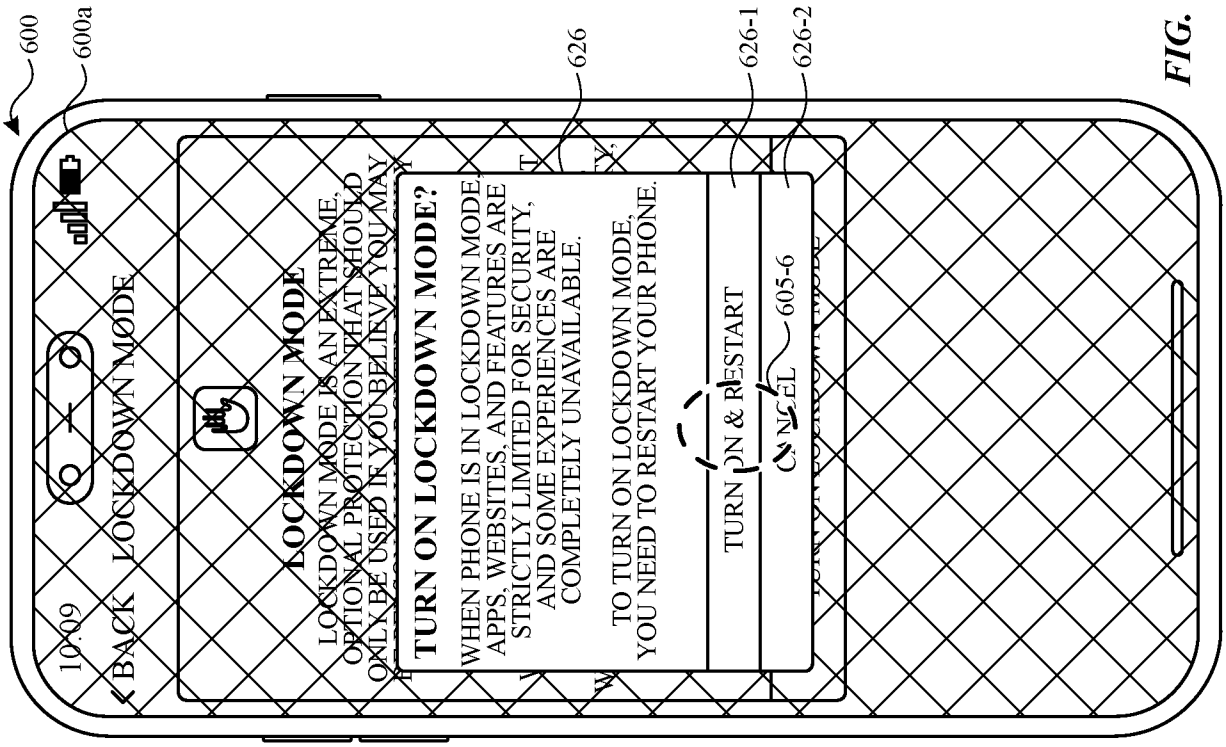

600
600a
10:09
BACK LOCKDOWN MODE
LOCKDOWN MODE
LOCKDOWN MODE IS AN EXTREME, OPTIONAL PROTECTION THAT SHOULD ONLY BE USED IF YOU BELIEVE YOU MAY
TURN ON LOCKDOWN MODE?
WHEN PHONE IS IN LOCKDOWN MODE, APPS, WEBSITES, AND FEATURES ARE STRICTLY LIMITED FOR SECURITY, AND SOME EXPERIENCES ARE COMPLETELY UNAVAILABLE.
TO TURN ON LOCKDOWN MODE, YOU NEED TO RESTART YOUR PHONE.
TURN ON & RESTART
CANCEL
626
626-1
626-2
605-6

FIG. 6F

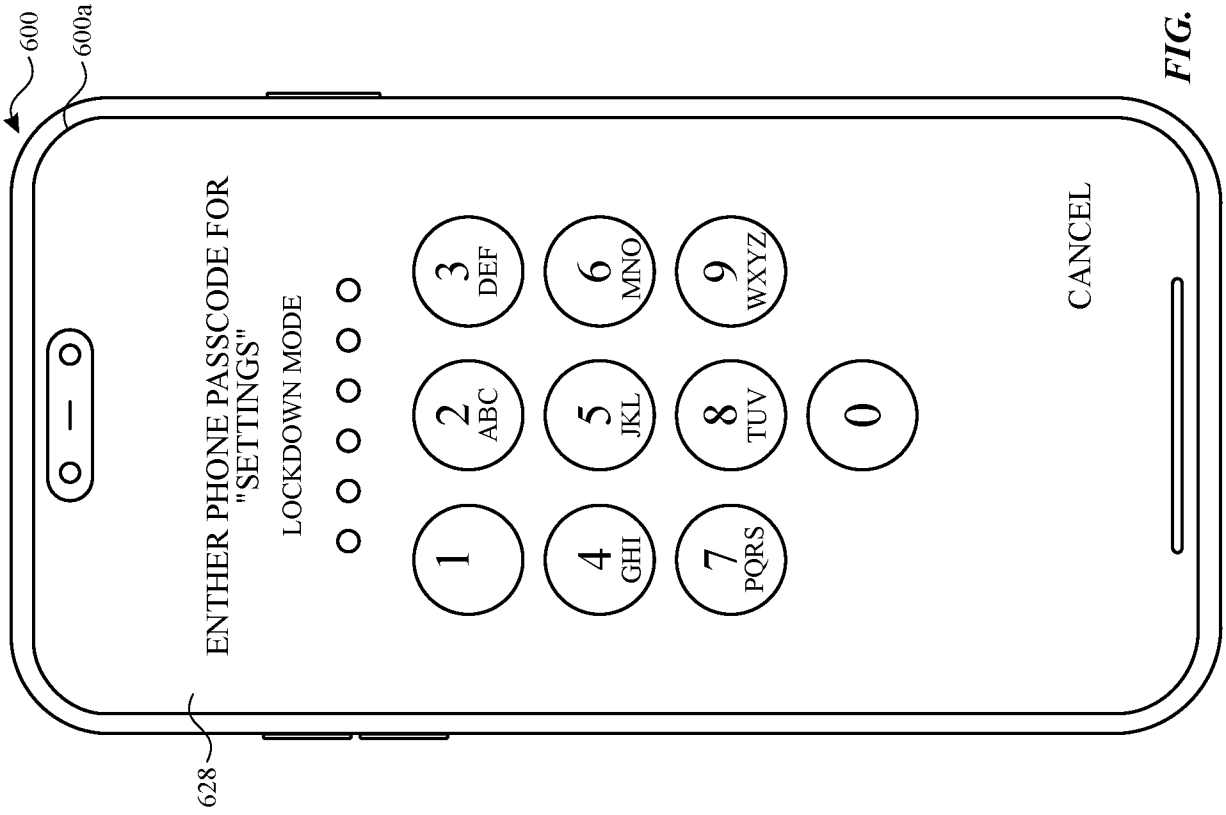

600
600a
628
ENTHER PHONE PASSCODE FOR
"SETTINGS"
LOCKDOWN MODE
1
2 ABC
3 DEF
4 GHI
5 JKL
6 MNO
7 PQRS
8 TUV
9 WXYZ
0
CANCEL

FIG. 6G

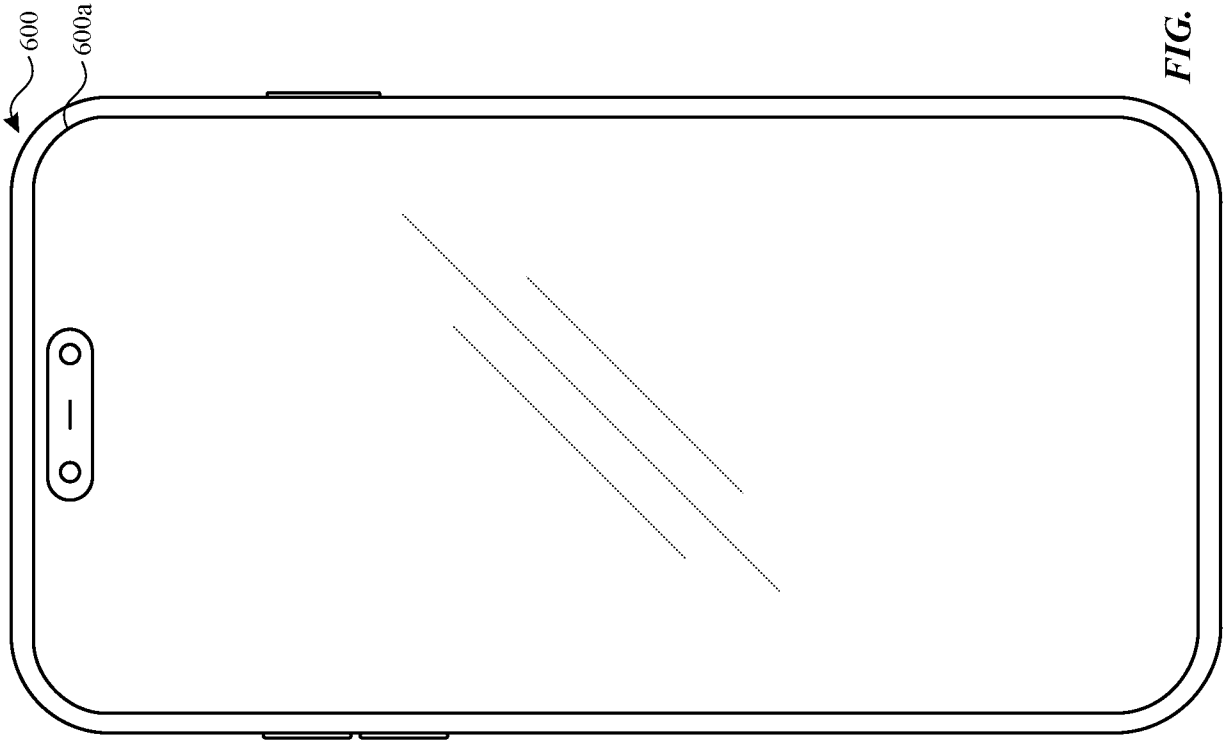

600
600a

FIG. 6H

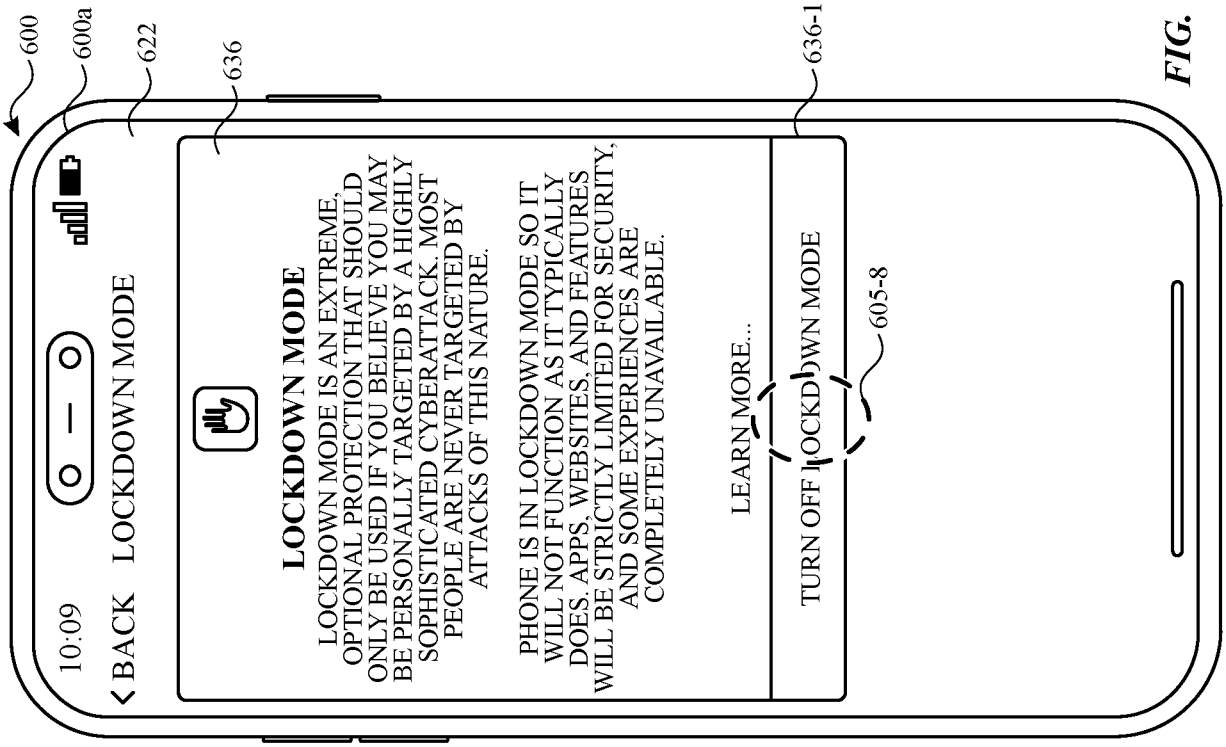

600
600a
622
636
636-1
10:09
BACK LOCKDOWN MODE
LOCKDOWN MODE
LOCKDOWN MODE IS AN EXTREME, OPTIONAL PROTECTION THAT SHOULD ONLY BE USED IF YOU BELIEVE YOU MAY BE PERSONALLY TARGETED BY A HIGHLY SOPHISTICATED CYBERATTACK. MOST PEOPLE ARE NEVER TARGETED BY ATTACKS OF THIS NATURE.
PHONE IS IN LOCKDOWN MODE SO IT WILL NOT FUNCTION AS IT TYPICALLY DOES. APPS, WEBSITES, AND FEATURES WILL BE STRICTLY LIMITED FOR SECURITY, AND SOME EXPERIENCES ARE COMPLETELY UNAVAILABLE.
LEARN MORE...
TURN OFF LOCKDOWN MODE
605-8

FIG. 6J

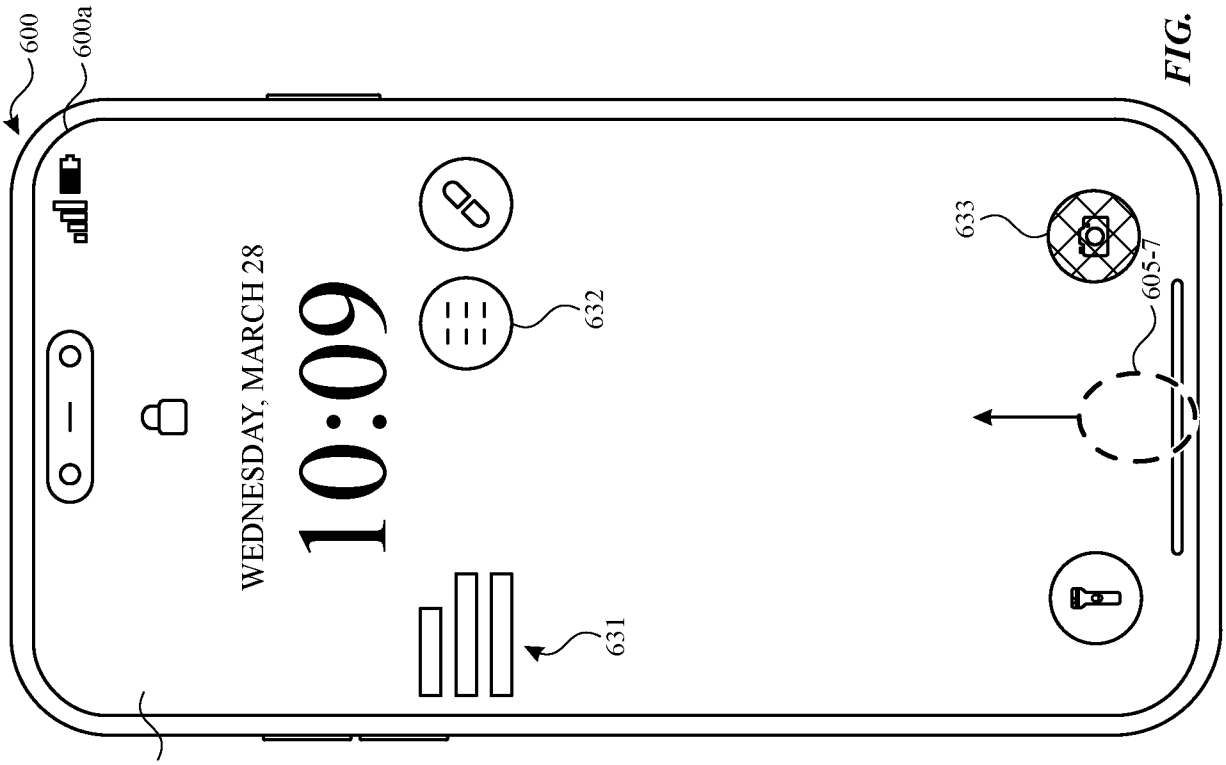

600
600a
630
631
WEDNESDAY, MARCH 28
10:09
632
633
605-7

FIG. 6I

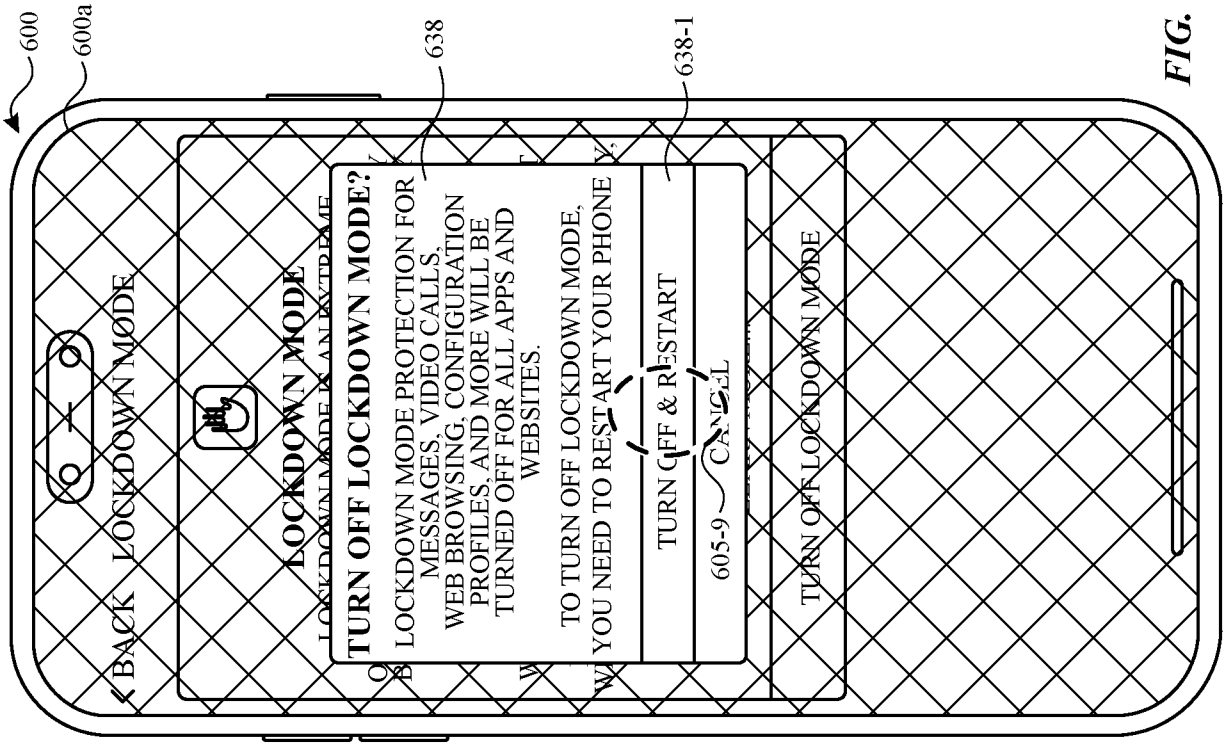

600
600a
BACK LOCKDOWN MODE
LOCKDOWN MODE
TURN OFF LOCKDOWN MODE?
LOCKDOWN MODE PROTECTION FOR MESSAGES, VIDEO CALLS, WEB BROWSING, CONFIGURATION PROFILES, AND MORE WILL BE TURNED OFF FOR ALL APPS AND WEBSITES.
TO TURN OFF LOCKDOWN MODE, YOU NEED TO RESTART YOUR PHONE
TURN OFF & RESTART
CANCEL
638
638-1
605-9
TURN OFF LOCKDOWN MODE

FIG. 6K

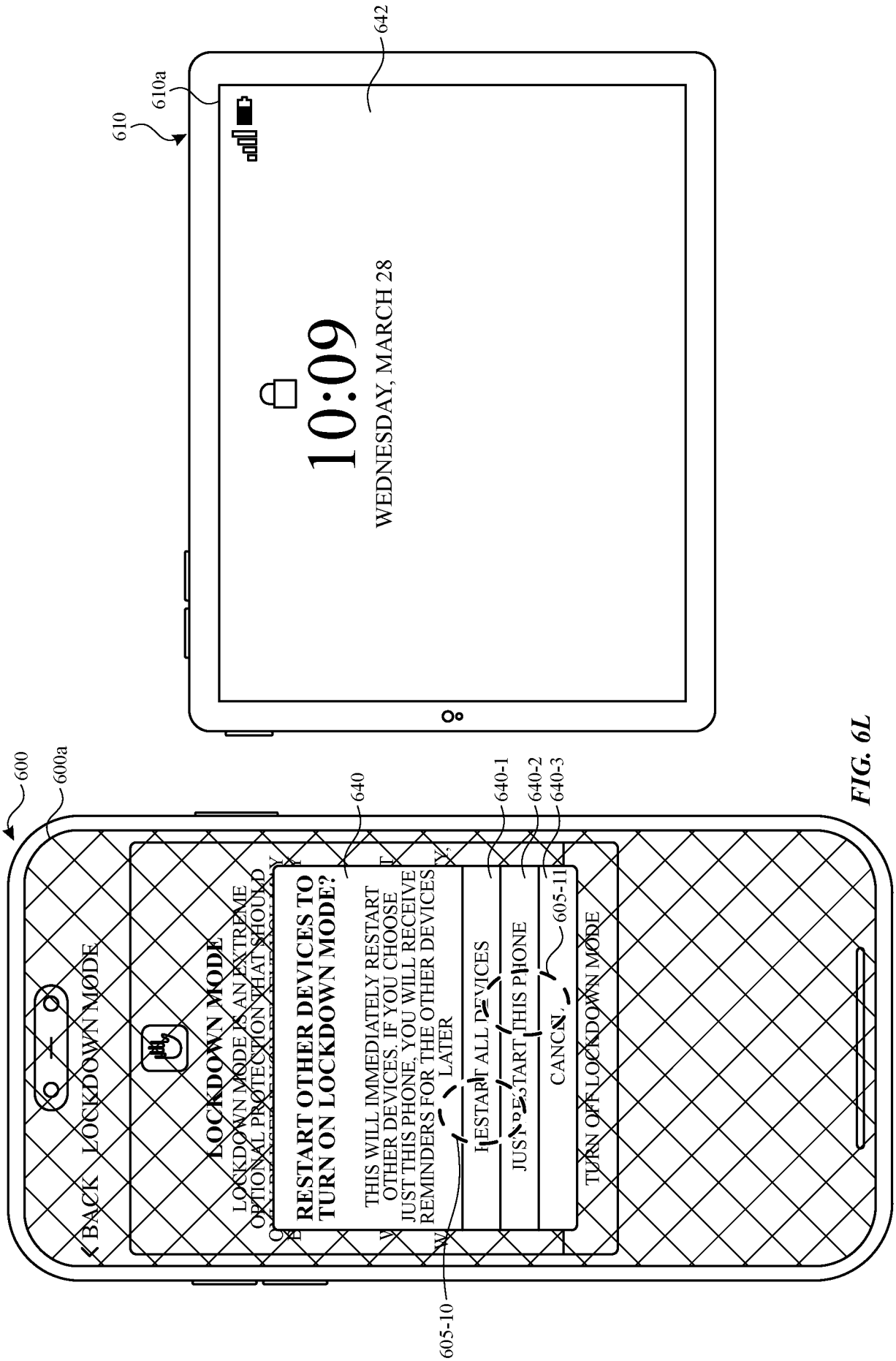

610
610a
642
10:09
WEDNESDAY, MARCH 28
600
600a
640
640-1
640-2
640-3
605-10
605-11
BACK LOCKDOWN MODE
LOCKDOWN MODE
LOCKDOWN MODE IS AN EXTREME
RESTART OTHER DEVICES TO
TURN ON LOCKDOWN MODE?
THIS WILL IMMEDIATELY RESTART
OTHER DEVICES. IF YOU CHOOSE
JUST THIS PHONE, YOU WILL RECEIVE
REMINDERS FOR THE OTHER DEVICES
LATER
RESTART ALL DEVICES
JUST RESTART THIS PHONE
CANCEL
TURN OFF LOCKDOWN MODE

FIG. 6L

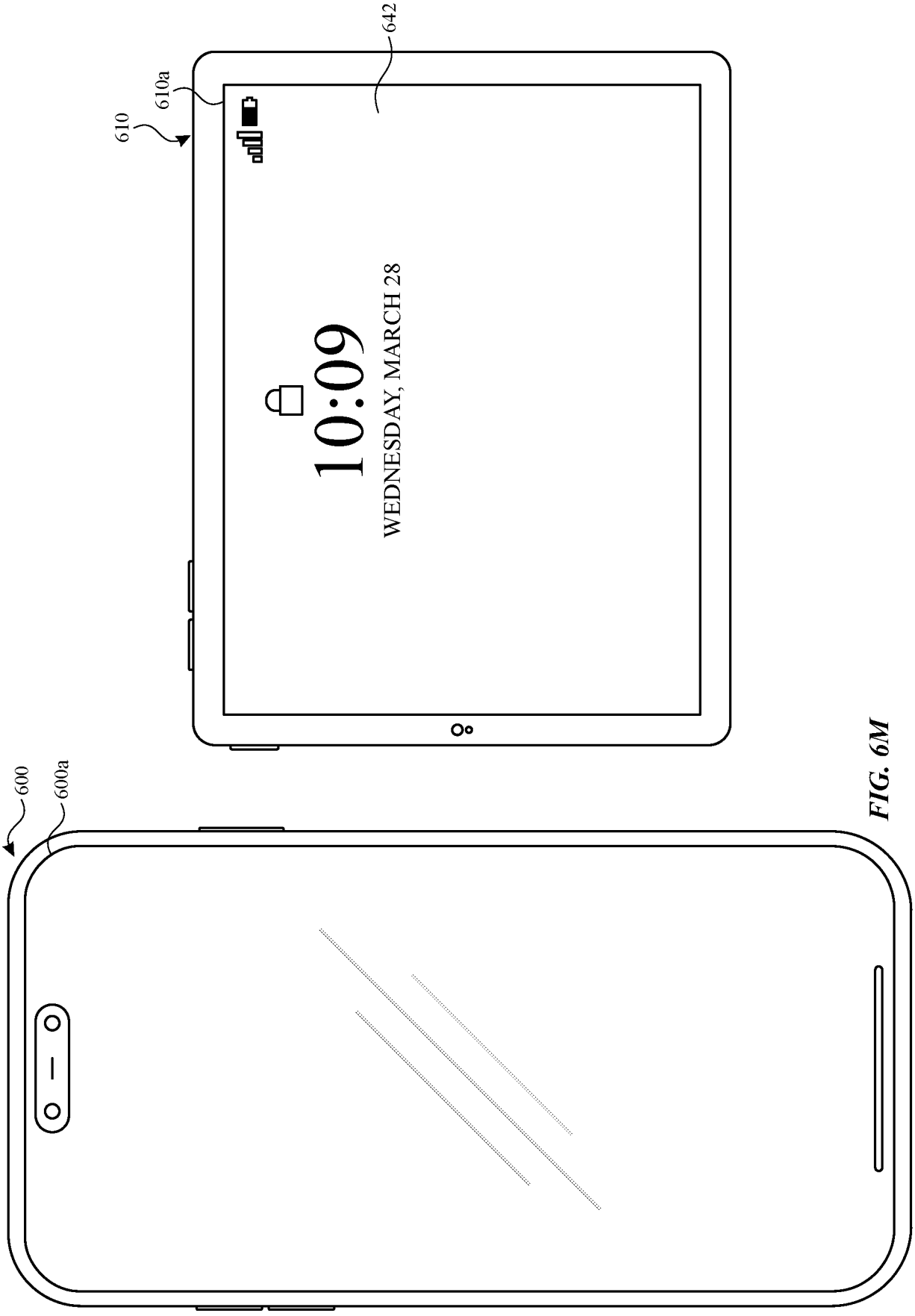


FIG. 6M

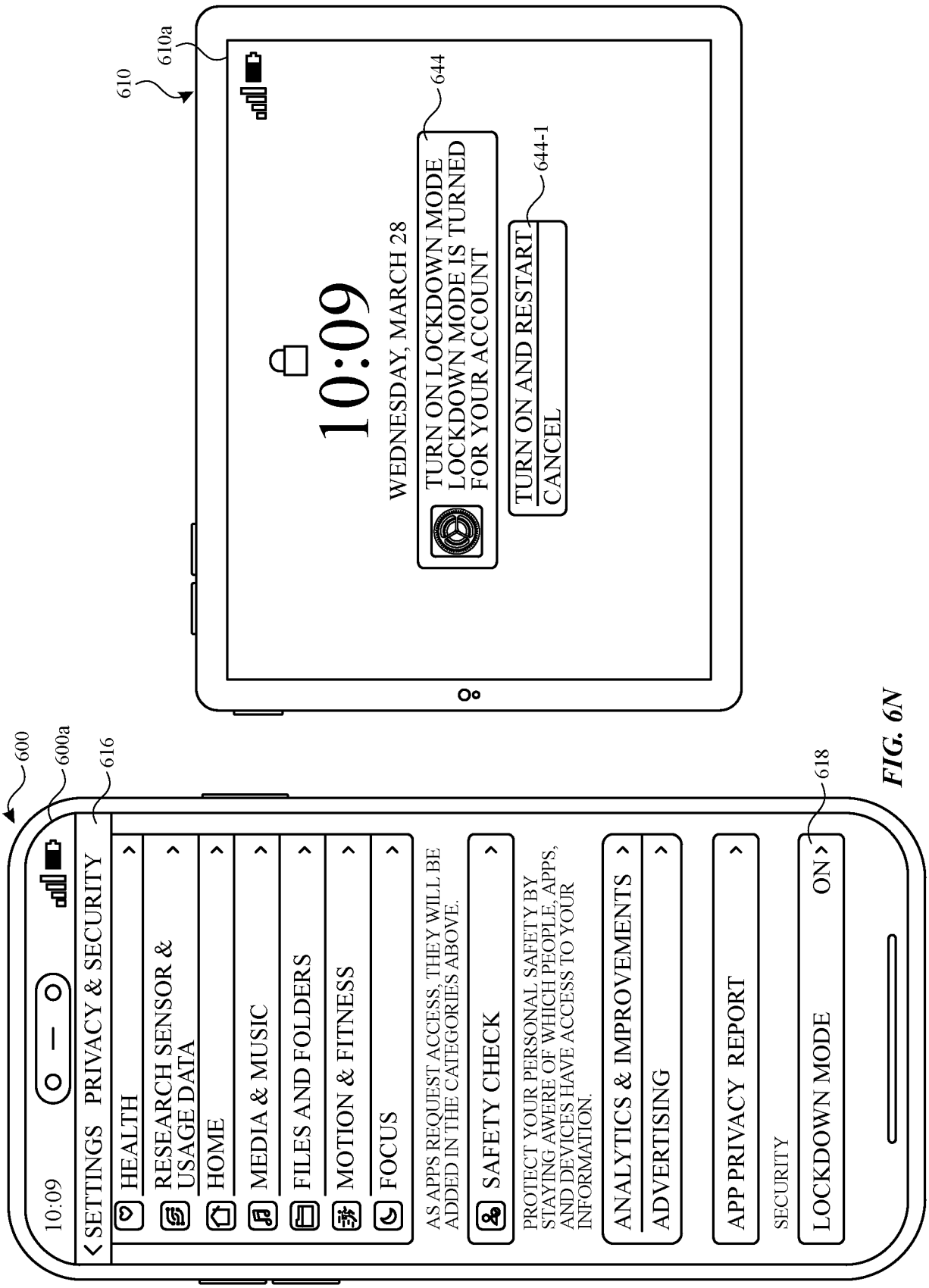

600
600a
616
10:09
SETTINGS PRIVACY & SECURITY
HEALTH
RESEARCH SENSOR & USAGE DATA
HOME
MEDIA & MUSIC
FILES AND FOLDERS
MOTION & FITNESS
FOCUS
AS APPS REQUEST ACCESS, THEY WILL BE ADDED IN THE CATEGORIES ABOVE.
SAFETY CHECK
PROTECT YOUR PERSONAL SAFETY BY STAYING AWERE OF WHICH PEOPLE, APPS, AND DEVICES HAVE ACCESS TO YOUR INFORMATION.
ANALYTICS & IMPROVEMENTS
ADVERTISING
APP PRIVACY REPORT
SECURITY
LOCKDOWN MODE ON
618
610
610a
10:09
WEDNESDAY, MARCH 28
644
TURN ON LOCKDOWN MODE
LOCKDOWN MODE IS TURNED FOR YOUR ACCOUNT
644-1
TURN ON AND RESTART
CANCEL

FIG. 6N

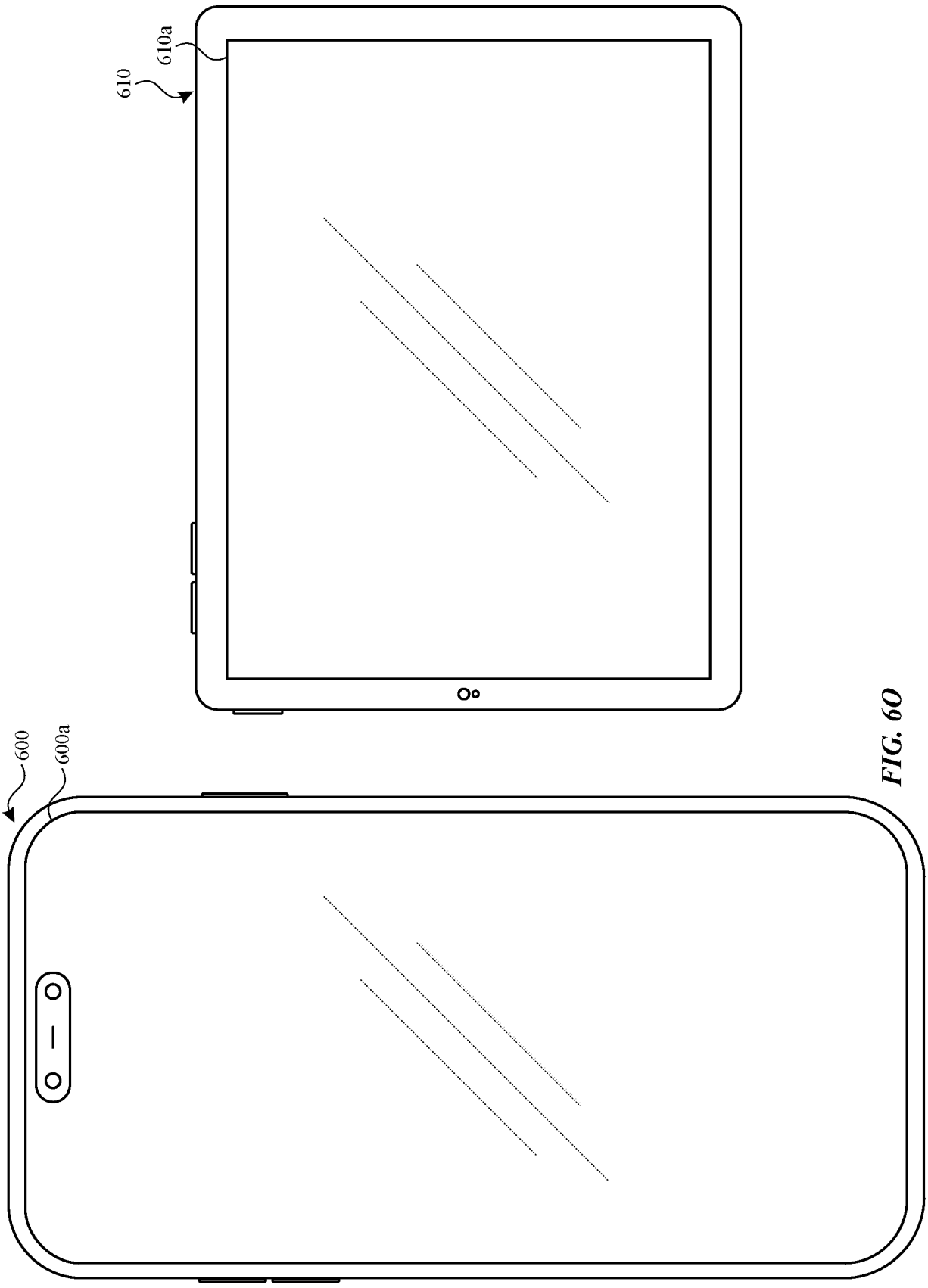


FIG. 6O

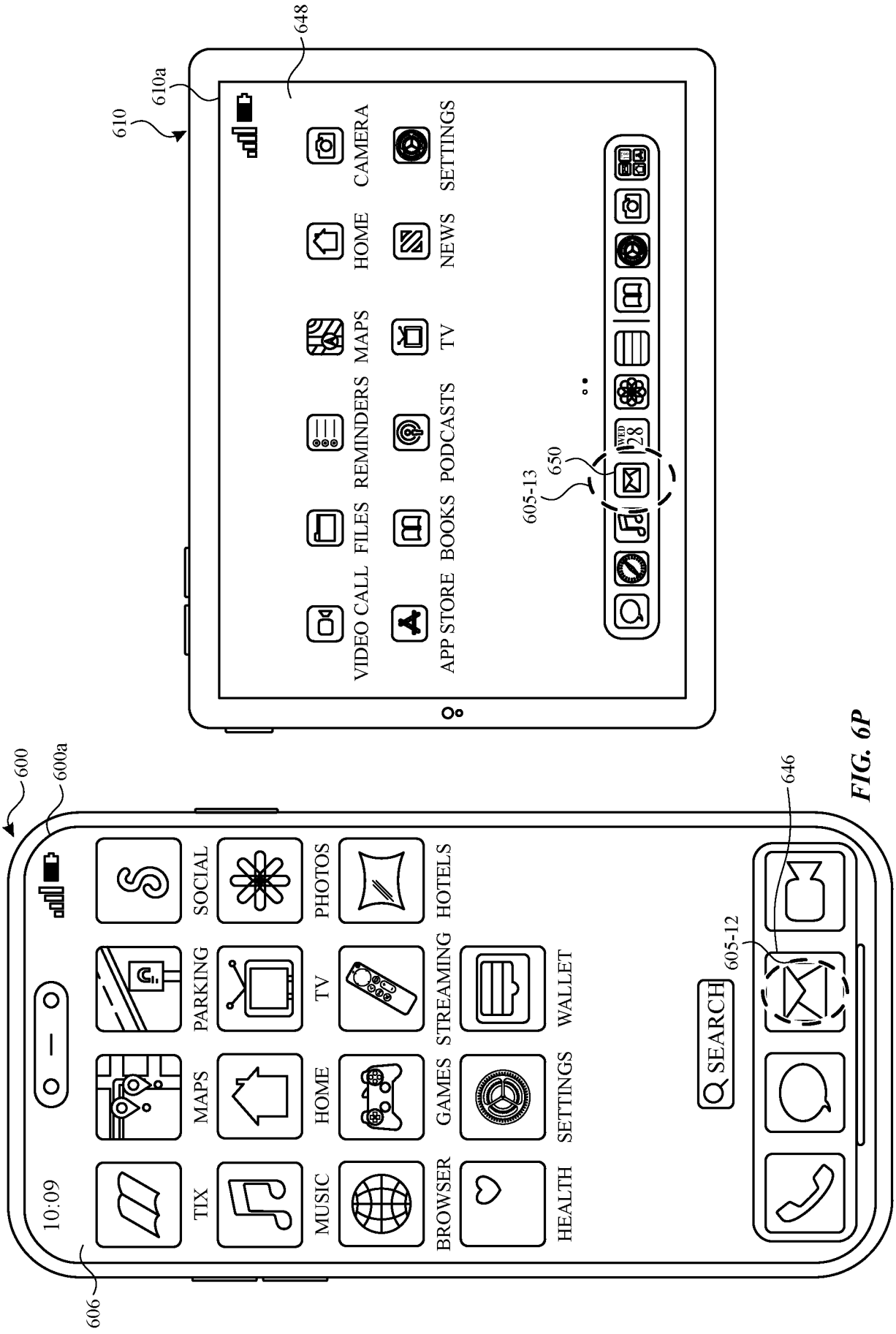

600
600a
606
10:09
TIX
MAPS
PARKING
SOCIAL
MUSIC
HOME
TV
PHOTOS
BROWSER
GAMES
STREAMING
HOTELS
HEALTH
SETTINGS
WALLET
Q SEARCH
605-12
646
610
610a
648
VIDEO CALL
FILES
REMINDERS
MAPS
HOME
CAMERA
APP STORE
BOOKS
PODCASTS
TV
NEWS
SETTINGS
605-13
650

FIG. 6P

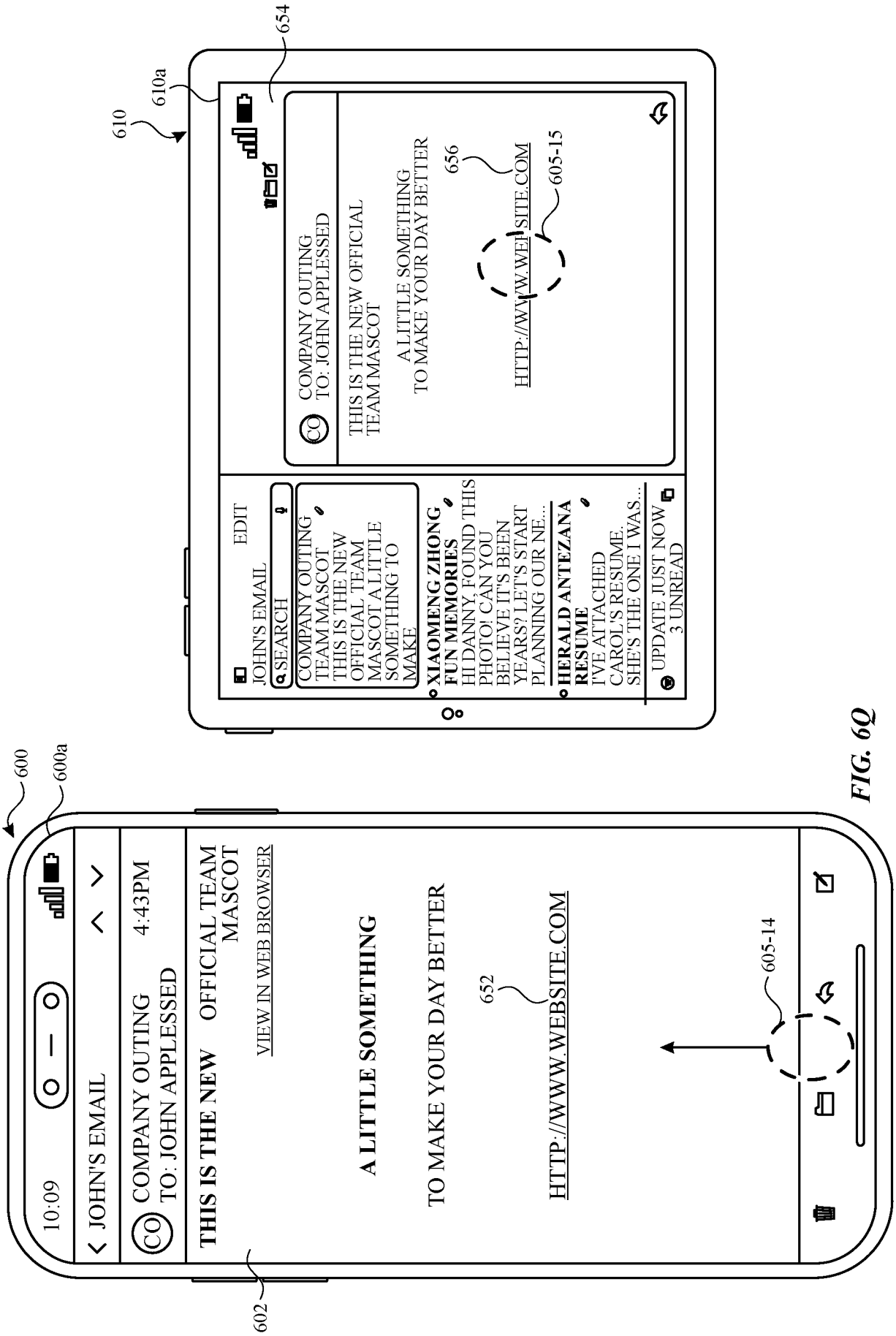

600
600a
10:09
JOHN'S EMAIL
COMPANY OUTING
TO: JOHN APPLESSED
4:43PM
THIS IS THE NEW OFFICIAL TEAM MASCOT
VIEW IN WEB BROWSER
A LITTLE SOMETHING
TO MAKE YOUR DAY BETTER
652
HTTP://WWW.WEBSITE.COM
605-14
602
610
610a
654
EDIT
JOHN'S EMAIL
SEARCH
COMPANY OUTING
TEAM MASCOT
THIS IS THE NEW
OFFICIAL TEAM
MASCOT A LITTLE
SOMETHING TO
MAKE
XIAOMENG ZHONG
FUN MEMORIES
HI DANNY, FOUND THIS
PHOTO! CAN YOU
BELIEVE IT'S BEEN
YEARS? LET'S START
PLANNING OUR NE...
HERALD ANTEZANA
RESUME
I'VE ATTACHED
CAROL'S RESUME.
SHE'S THE ONE I WAS...
UPDATE JUST NOW
3 UNREAD
COMPANY OUTING
TO: JOHN APPLESSED
THIS IS THE NEW OFFICIAL
TEAM MASCOT
A LITTLE SOMETHING
TO MAKE YOUR DAY BETTER
656
HTTP://WWW.WEBSITE.COM
605-15

FIG. 6Q

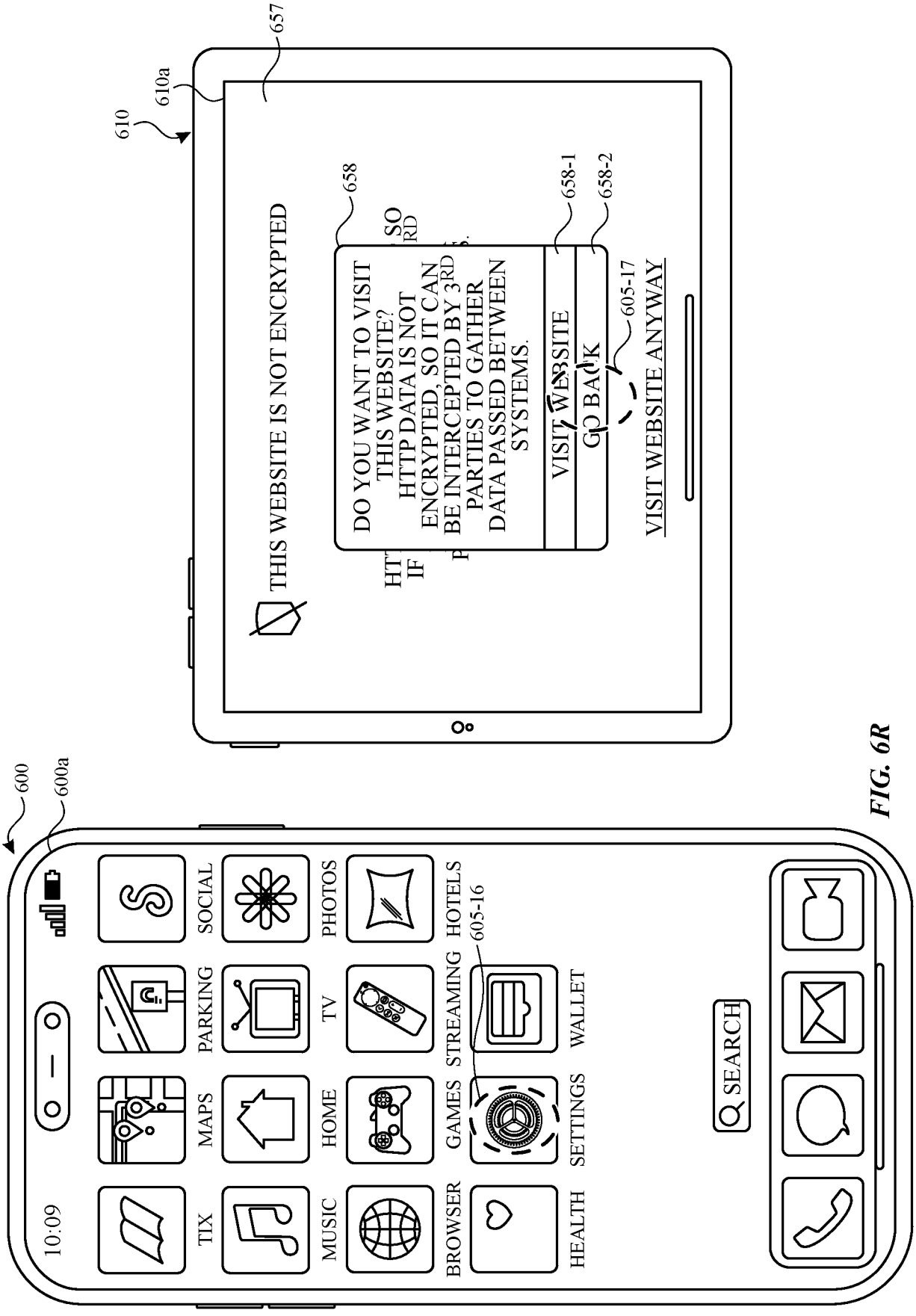

600
600a
10:09
TIX
MAPS
HOME
MUSIC
BROWSER
HEALTH
SETTINGS
GAMES
STREAMING
WALLET
TV
PARKING
SOCIAL
PHOTOS
HOTELS
605-16
Q SEARCH
610
610a
657
THIS WEBSITE IS NOT ENCRYPTED
658
DO YOU WANT TO VISIT THIS WEBSITE? HTTP DATA IS NOT ENCRYPTED, SO IT CAN BE INTERCEPTED BY 3RD PARTIES TO GATHER DATA PASSED BETWEEN SYSTEMS.
658-1
VISIT WEBSITE
658-2
GO BACK
605-17
VISIT WEBSITE ANYWAY

FIG. 6R

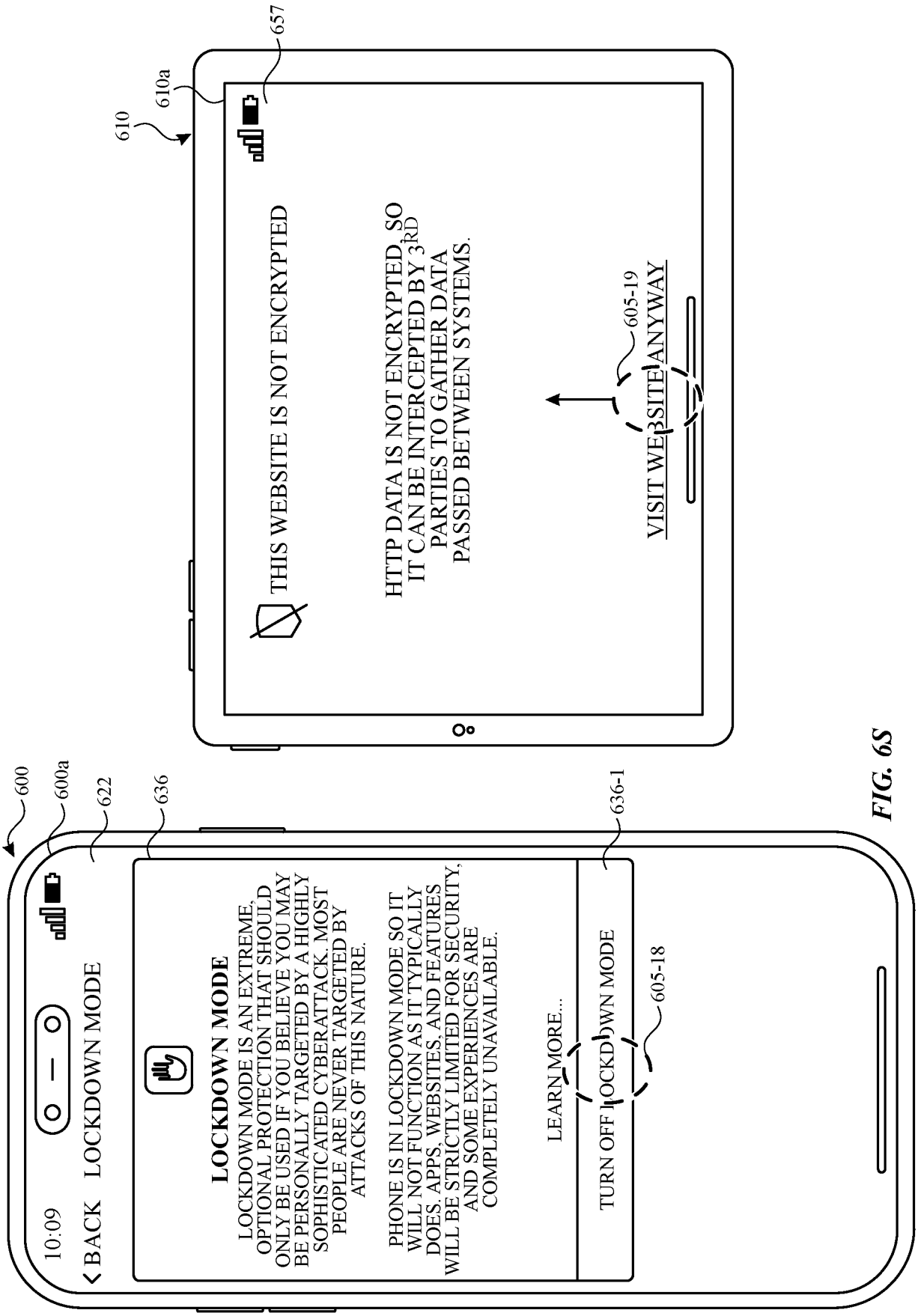

600
600a
622
636
636-1
10:09
BACK LOCKDOWN MODE
LOCKDOWN MODE
LOCKDOWN MODE IS AN EXTREME, OPTIONAL PROTECTION THAT SHOULD ONLY BE USED IF YOU BELIEVE YOU MAY BE PERSONALLY TARGETED BY A HIGHLY SOPHISTICATED CYBERATTACK. MOST PEOPLE ARE NEVER TARGETED BY ATTACKS OF THIS NATURE.
PHONE IS IN LOCKDOWN MODE SO IT WILL NOT FUNCTION AS IT TYPICALLY DOES. APPS, WEBSITES, AND FEATURES WILL BE STRICTLY LIMITED FOR SECURITY, AND SOME EXPERIENCES ARE COMPLETELY UNAVAILABLE.
LEARN MORE...
TURN OFF LOCKDOWN MODE
605-18
610
610a
657
THIS WEBSITE IS NOT ENCRYPTED
HTTP DATA IS NOT ENCRYPTED, SO IT CAN BE INTERCEPTED BY 3RD PARTIES TO GATHER DATA PASSED BETWEEN SYSTEMS.
605-19
VISIT WEBSITE ANYWAY

FIG. 6S

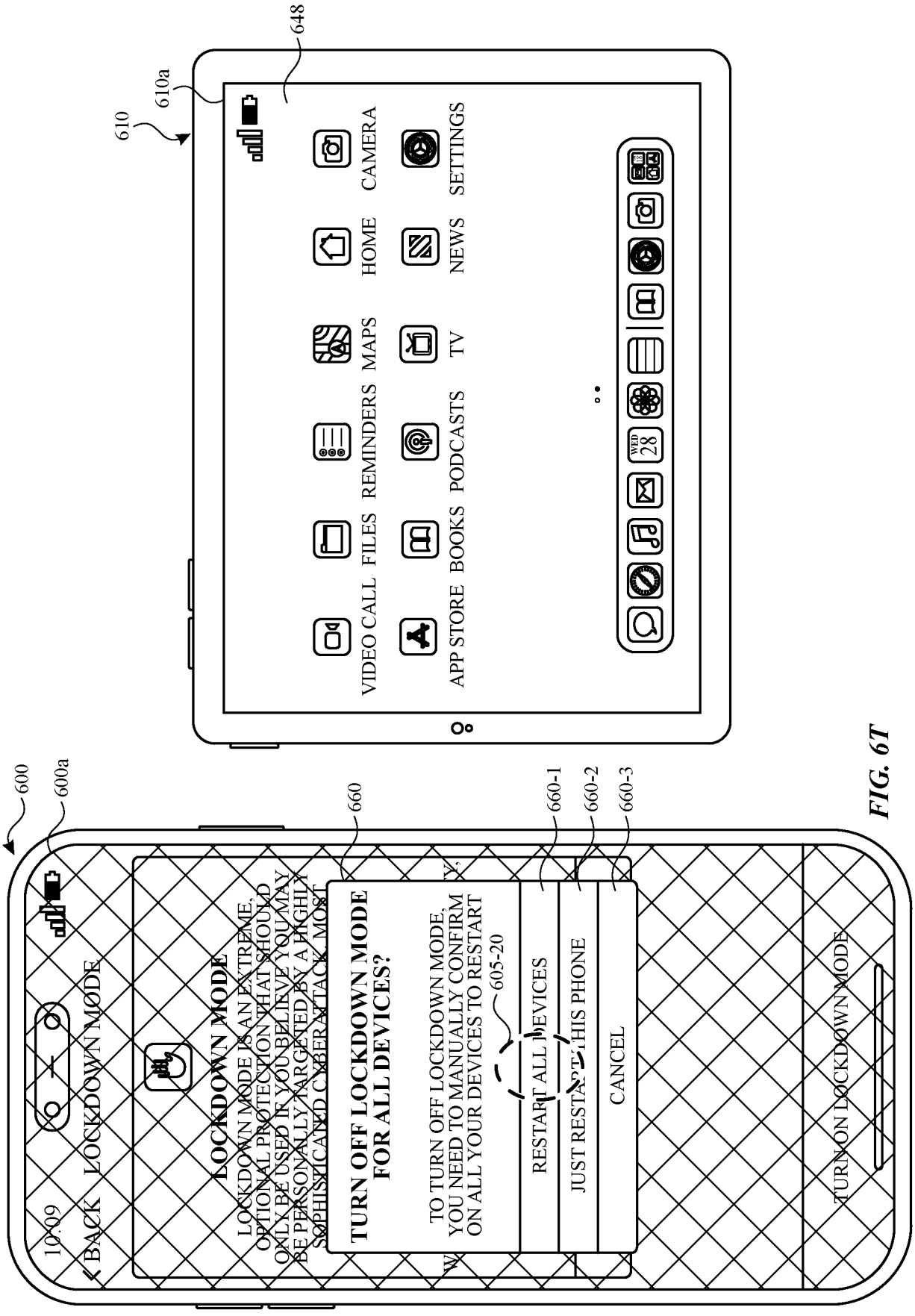

600
600a
610
610a
648
660
660-1
660-2
660-3
605-20
10:09
BACK
LOCKDOWN MODE
LOCKDOWN MODE
LOCKDOWN MODE IS AN EXTREME, OPTIONAL PROTECTION THAT SHOULD ONLY BE USED IF YOU BELIEVE YOU MAY BE PERSONALLY TARGETED BY A HIGHLY SOPHISTICATED CYBER ATTACK. MOST
TURN OFF LOCKDOWN MODE FOR ALL DEVICES?
TO TURN OFF LOCKDOWN MODE, YOU NEED TO MANUALLY CONFIRM ON ALL YOUR DEVICES TO RESTART
RESTART ALL DEVICES
JUST RESTART THIS PHONE
CANCEL
TURN ON LOCKDOWN MODE
VIDEO CALL
FILES
REMINDERS
MAPS
HOME
CAMERA
APP STORE
BOOKS
PODCASTS
TV
NEWS
SETTINGS
WED
28

FIG. 6T

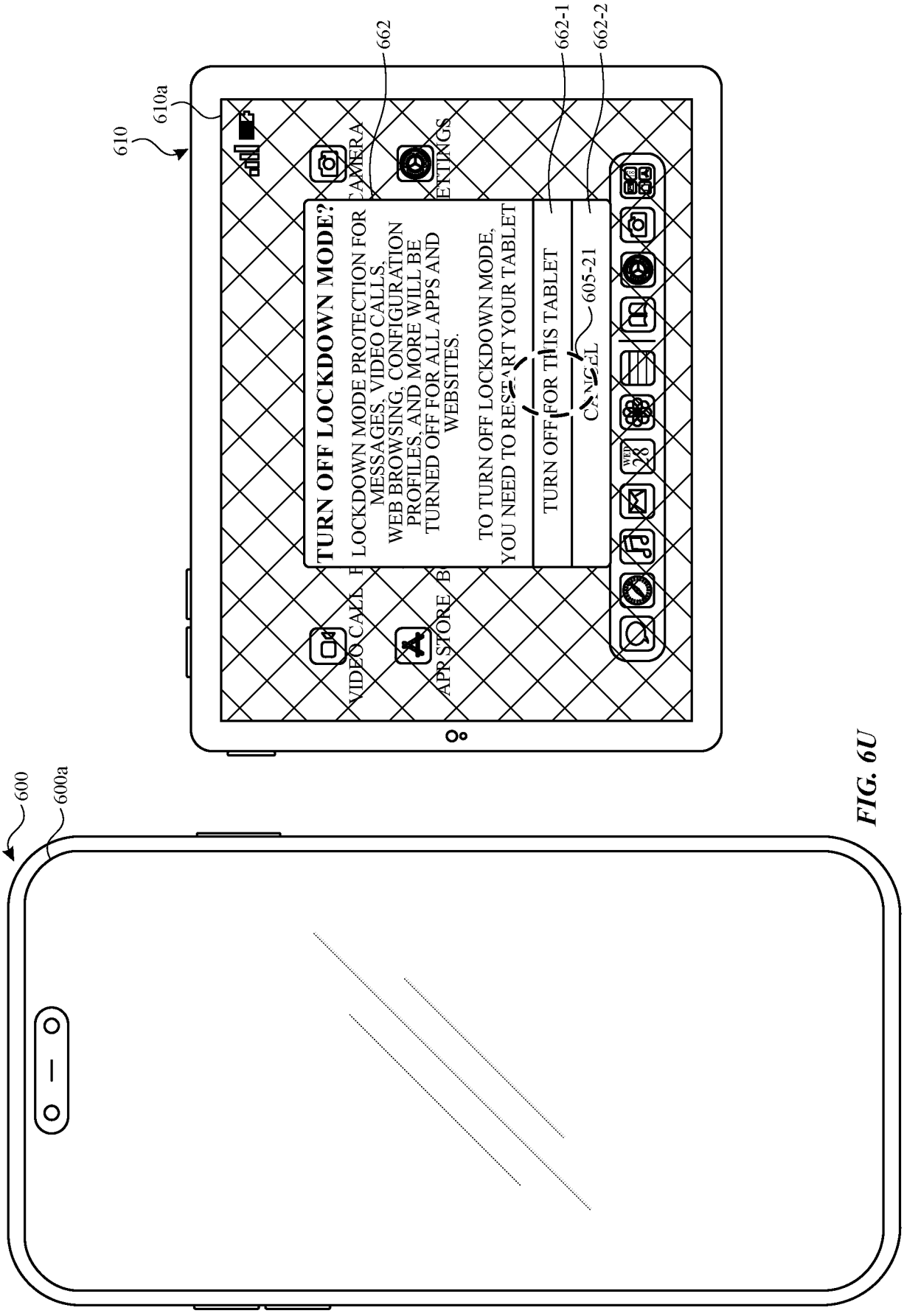

600
600a
610
610a
662
662-1
662-2
605-21
TURN OFF LOCKDOWN MODE?
LOCKDOWN MODE PROTECTION FOR MESSAGES, VIDEO CALLS, WEB BROWSING, CONFIGURATION PROFILES, AND MORE WILL BE TURNED OFF FOR ALL APPS AND WEBSITES.
TO TURN OFF LOCKDOWN MODE, YOU NEED TO RESTART YOUR TABLET
TURN OFF FOR THIS TABLET
CANCEL
CAMERA
SETTINGS
VIDEO CALL
APP STORE

FIG. 6U

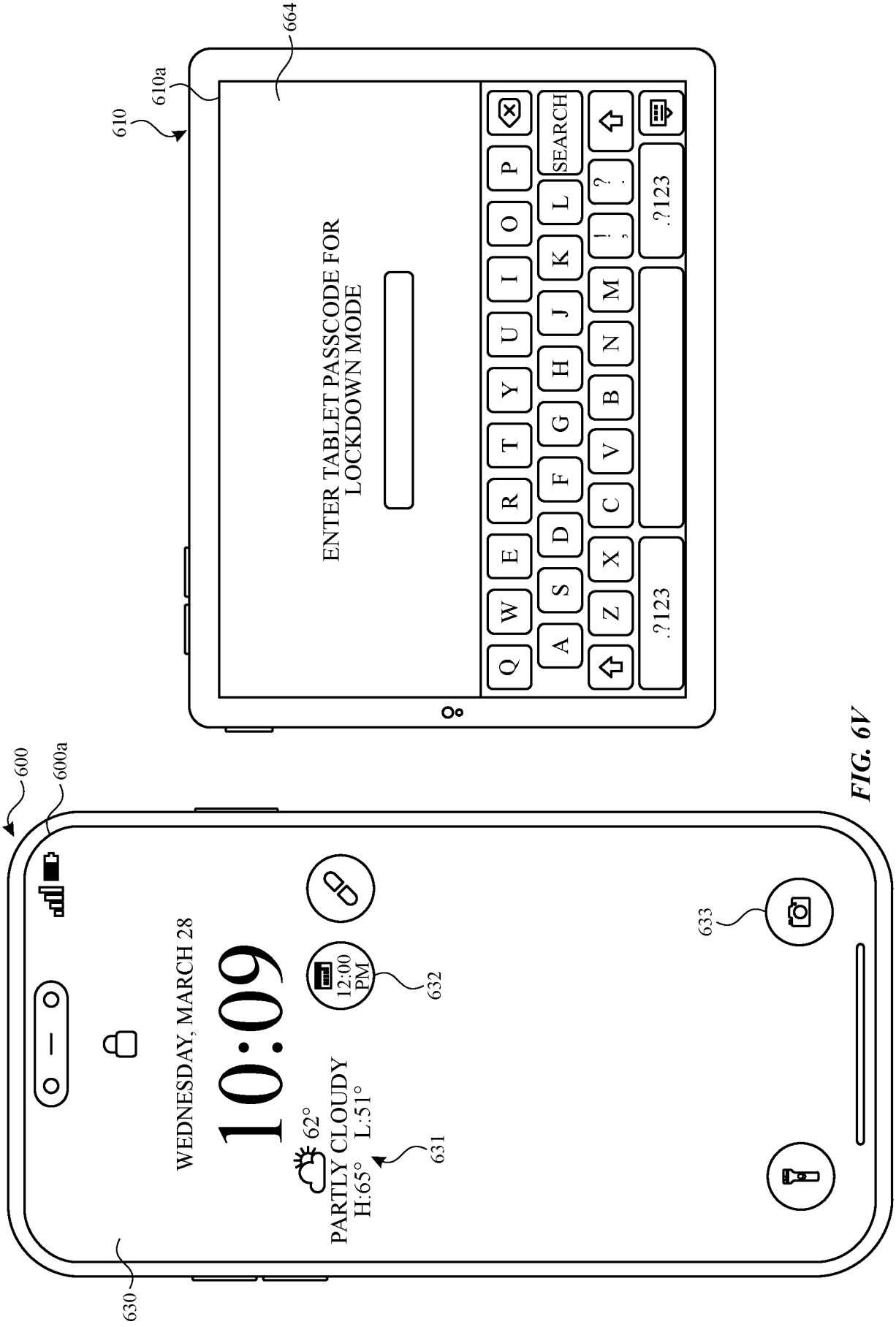

600
600a
630
631
632
633
610
610a
664
WEDNESDAY, MARCH 28
10:09
62°
PARTLY CLOUDY
H:65° L:51°
12:00 PM
ENTER TABLET PASSCODE FOR LOCKDOWN MODE
SEARCH
.?123

FIG. 6V

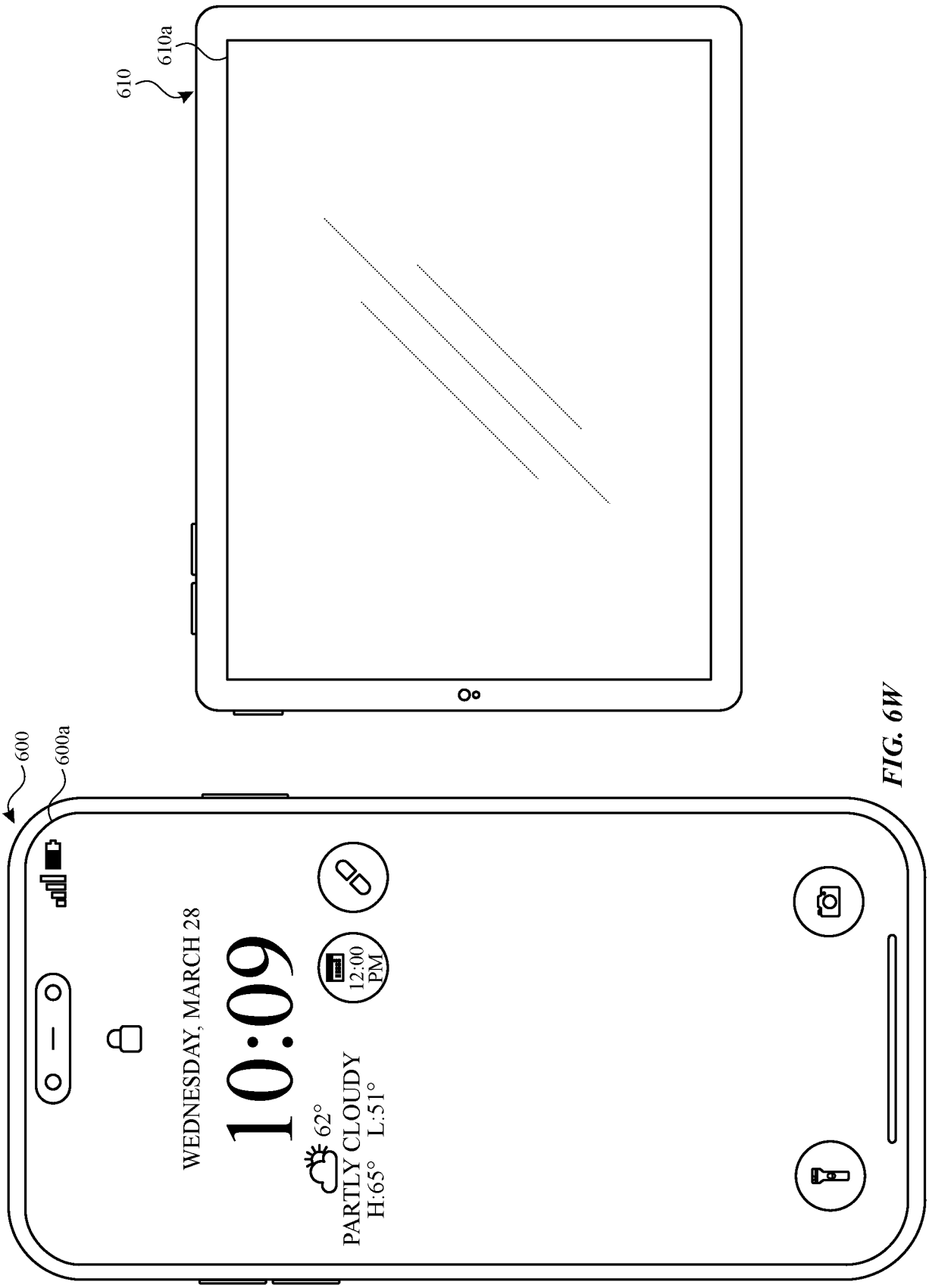

610
610a
600
600a
WEDNESDAY, MARCH 28
10:09
12:00 PM
62°
PARTLY CLOUDY
H:65° L:51°

FIG. 6W

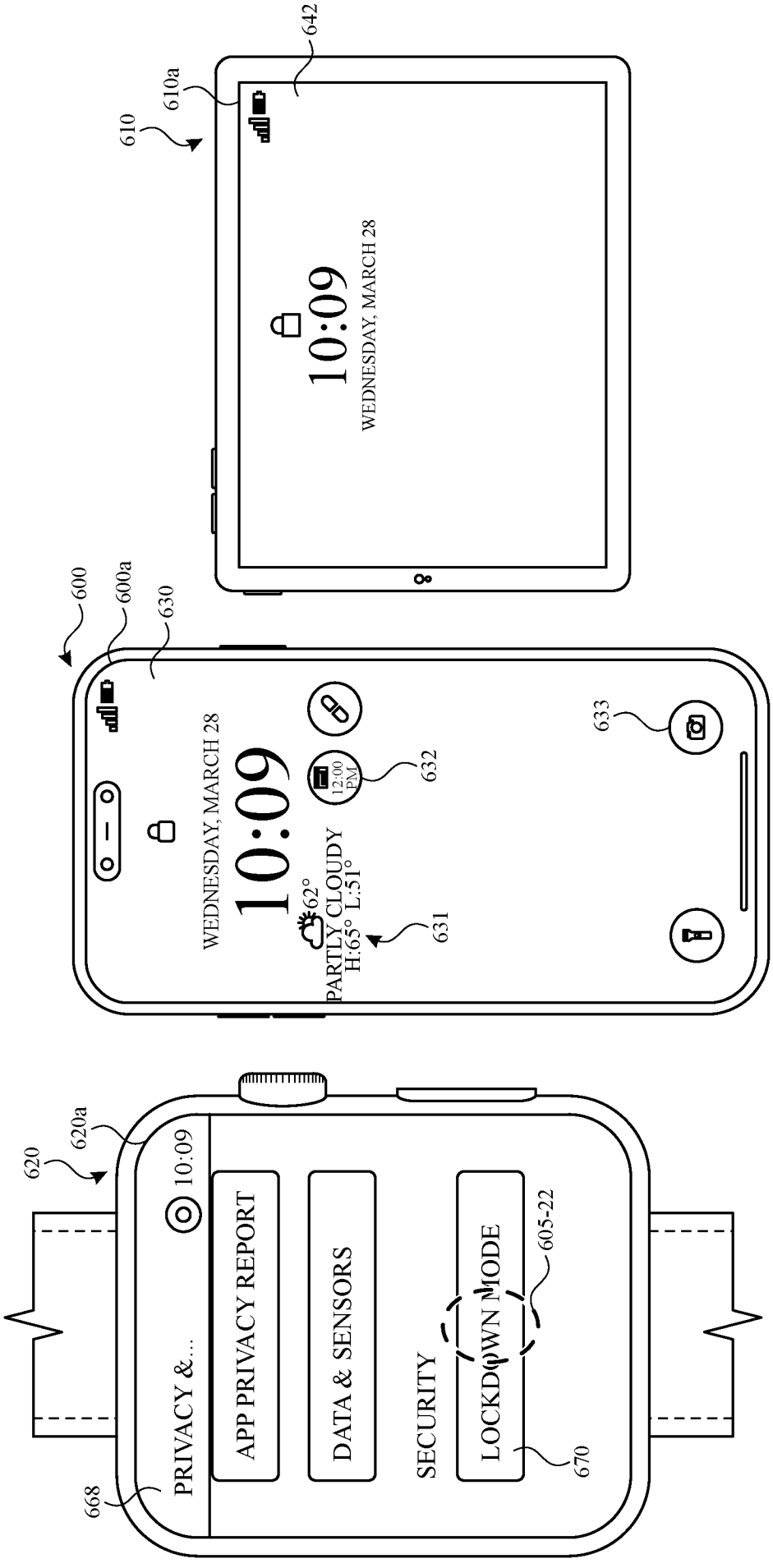

620
620a
10:09
PRIVACY &...
APP PRIVACY REPORT
DATA & SENSORS
SECURITY
LOCKDOWN MODE
605-22
670
668
600
600a
630
WEDNESDAY, MARCH 28
10:09
62°
PARTLY CLOUDY
H:65° L:51°
631
12:00 PM
632
633
610
610a
642
10:09
WEDNESDAY, MARCH 28

FIG. 6X

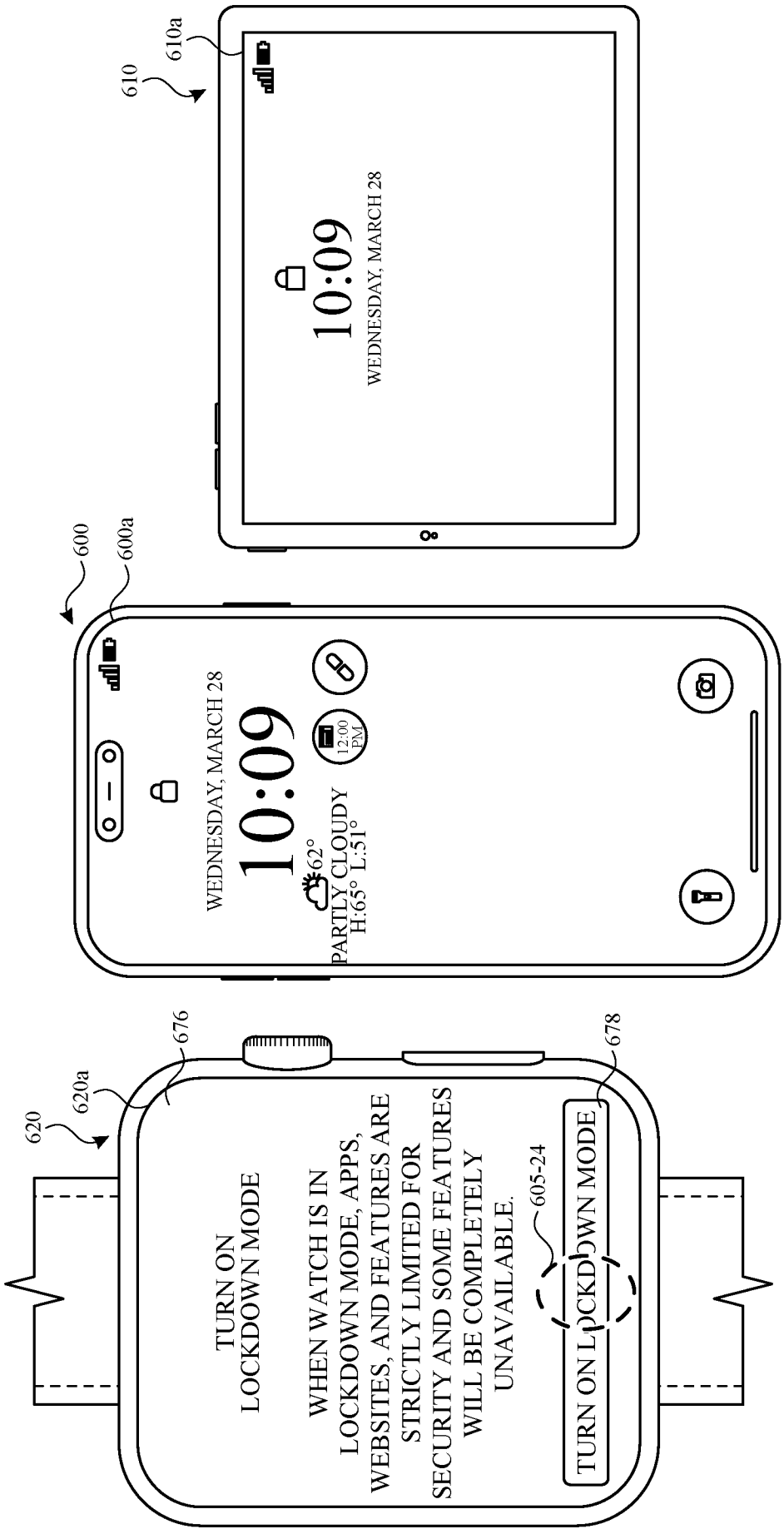

610
610a
10:09
WEDNESDAY, MARCH 28
600
600a
WEDNESDAY, MARCH 28
10:09
62°
PARTLY CLOUDY
H:65° L:51°
12:00
PM
620
620a
676
TURN ON
LOCKDOWN MODE
WHEN WATCH IS IN
LOCKDOWN MODE, APPS,
WEBSITES, AND FEATURES ARE
STRICTLY LIMITED FOR
SECURITY AND SOME FEATURES
WILL BE COMPLETELY
UNAVAILABLE.
605-24
678
TURN ON LOCKDOWN MODE

FIG. 6Y

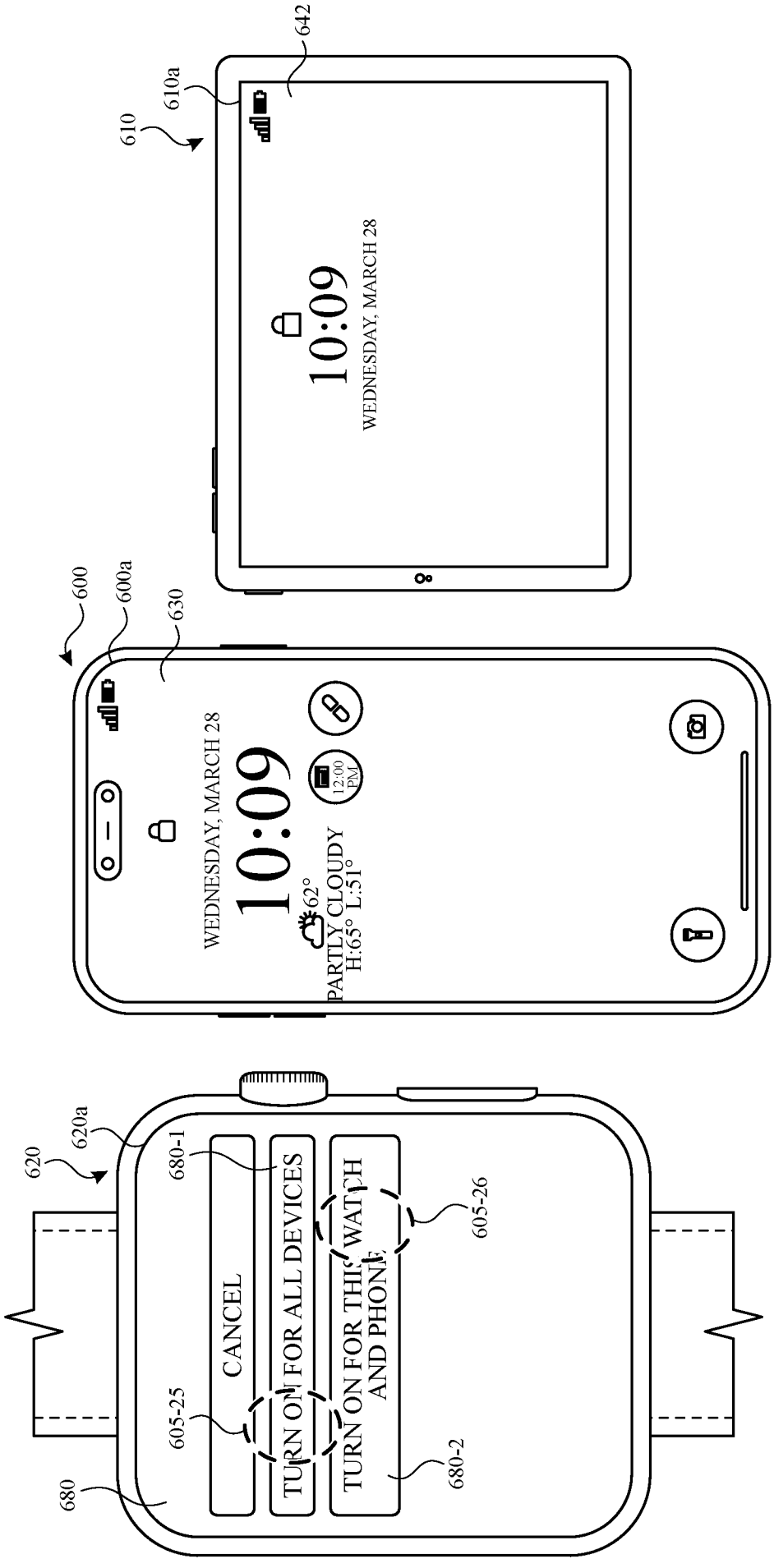

642
610a
610
10:09
WEDNESDAY, MARCH 28
600
600a
630
WEDNESDAY, MARCH 28
10:09
62°
PARTLY CLOUDY
H:65° L:51°
12:00 PM
620
620a
680-1
CANCEL
TURN ON FOR ALL DEVICES
TURN ON FOR THIS WATCH AND PHONE
605-25
605-26
680-2
680

FIG. 6Z

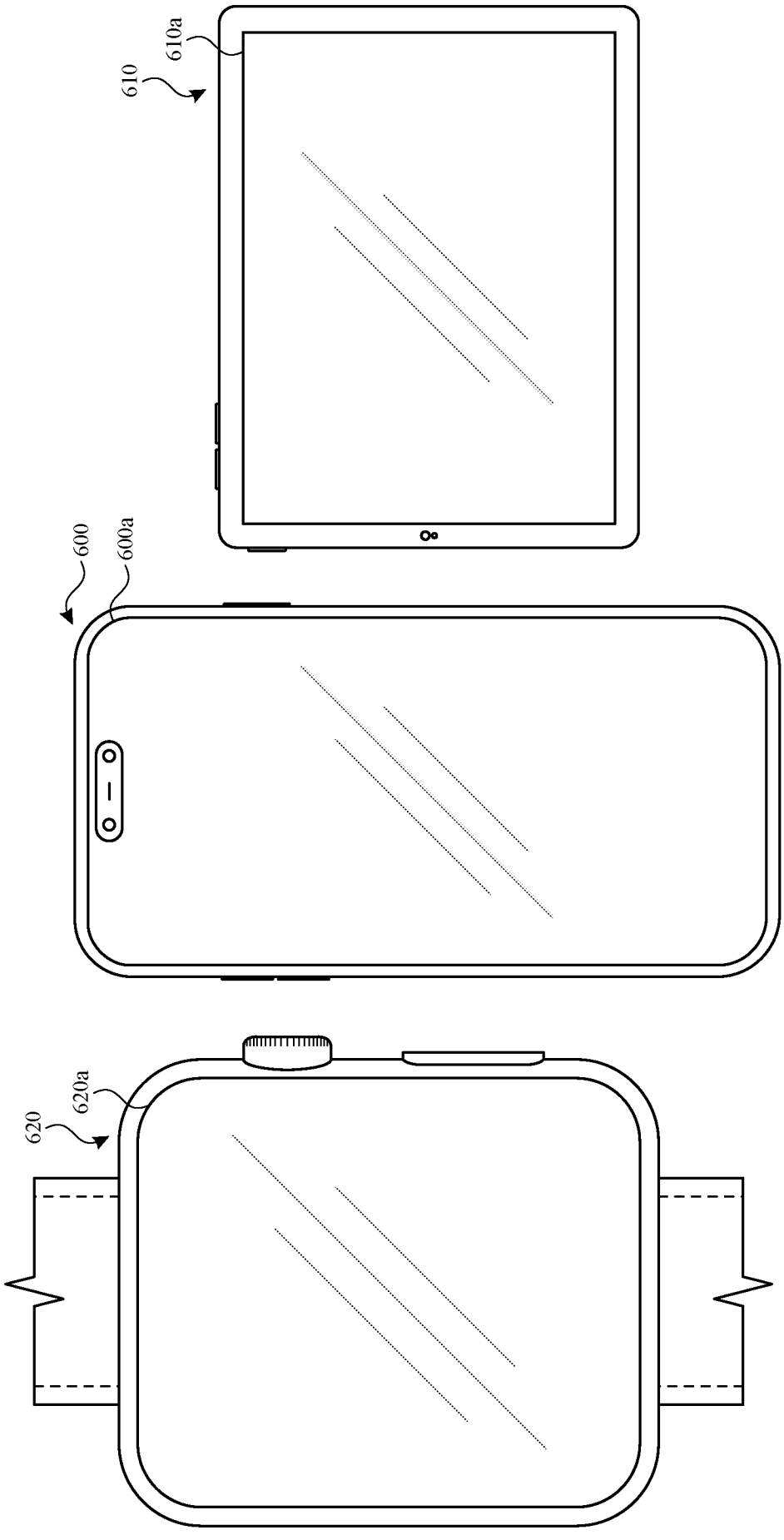


FIG. 6AA

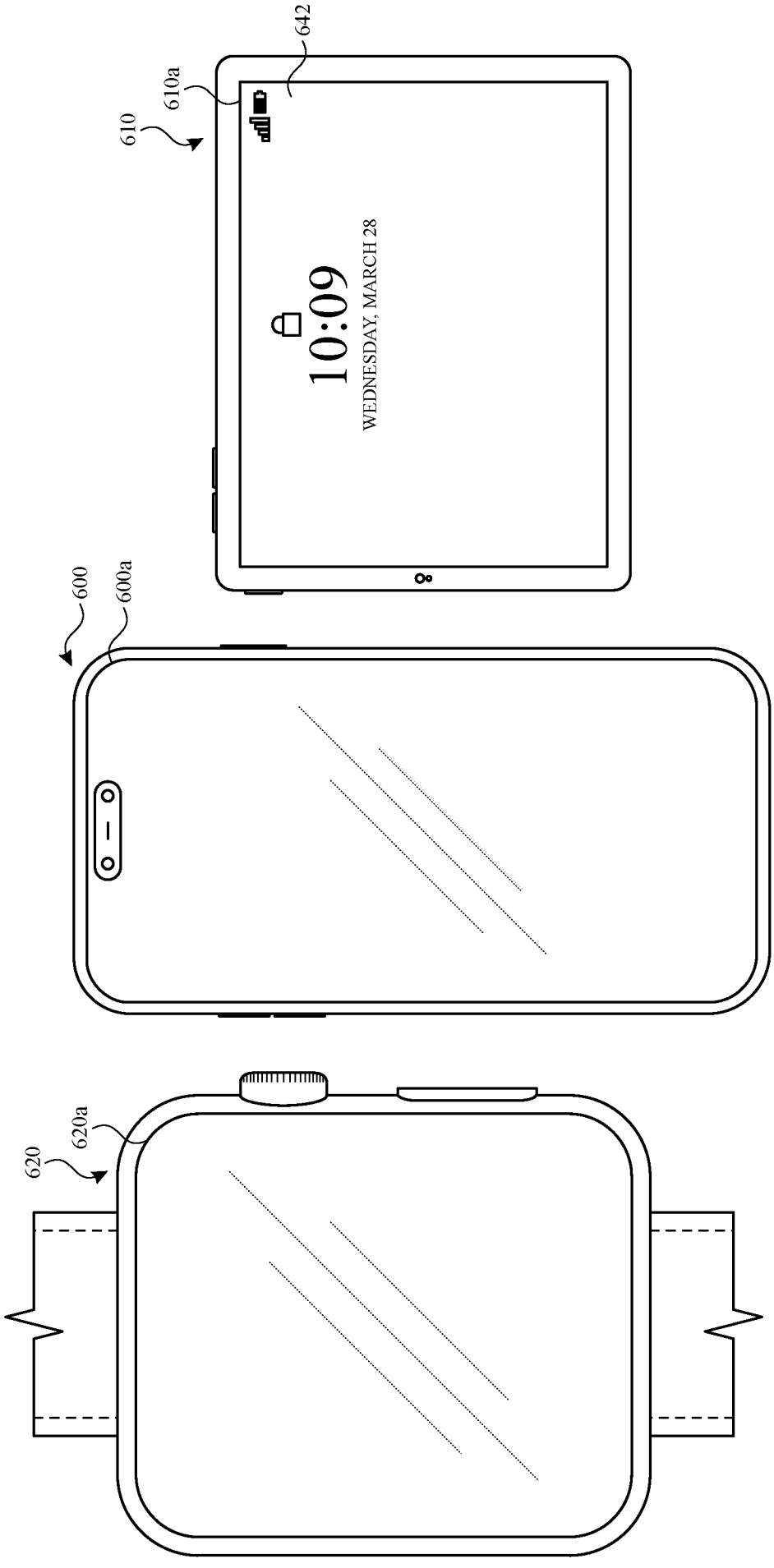


FIG. 6AB

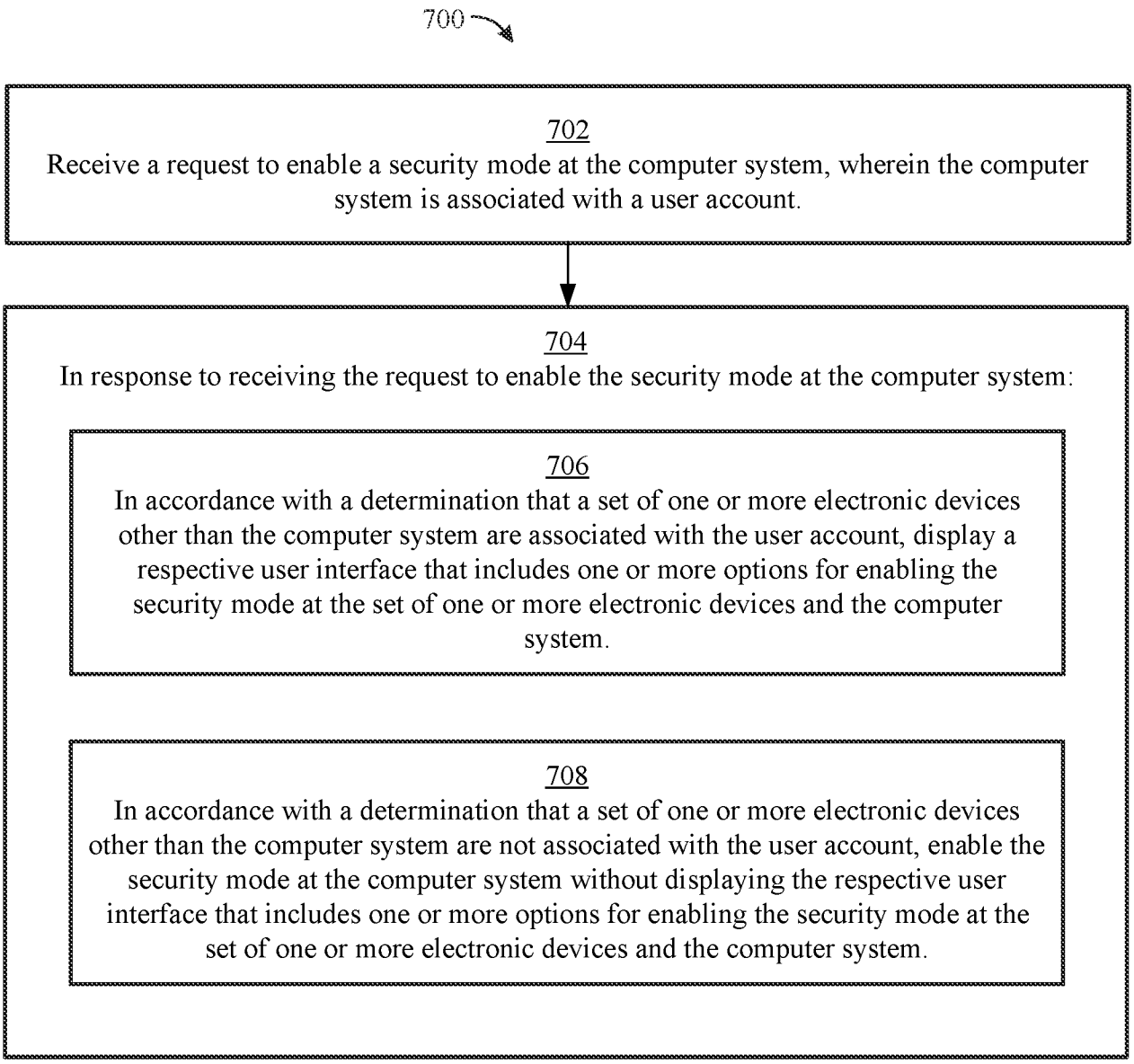

700
702
Receive a request to enable a security mode at the computer system, wherein the computer system is associated with a user account.
704
In response to receiving the request to enable the security mode at the computer system:
706
In accordance with a determination that a set of one or more electronic devices other than the computer system are associated with the user account, display a respective user interface that includes one or more options for enabling the security mode at the set of one or more electronic devices and the computer system.
708
In accordance with a determination that a set of one or more electronic devices other than the computer system are not associated with the user account, enable the security mode at the computer system without displaying the respective user interface that includes one or more options for enabling the security mode at the set of one or more electronic devices and the computer system.

FIG. 7

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2024/031893

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L9/40 H04W12/30 H04W12/60
ADD.

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)
H04L H04W

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)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2019/199752 A1 (GANDHI NIRAJ [US]) 27 June 2019 (2019-06-27)	1,2,4,6, 13-20
Y	paragraph [0001] - paragraph [0002] paragraph [0006] paragraph [0020] - paragraph [0024] paragraph [0028] - paragraph [0030] paragraph [0032] - paragraph [0035] figures 1, 3-7	3,5,7-12

Y	US 2018/288066 A1 (BROCKHUUS OLE [DK] ET AL) 4 October 2018 (2018-10-04)	3,5,7,10
A	paragraph [0001] paragraph [0052] paragraph [0057]	1,2,4,6, 8,9, 11-20

	-/--	

[x] Further documents are listed in the continuation of Box C.

[x] See patent family annex.

* 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	Date of mailing of the international search report
14 August 2024	03/09/2024

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Bharucha, Zubin

1

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2024/031893

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	Enoch Root: "So funktioniert Apples neuer Lockdown Mode", , 10 August 2022 (2022-08-10), pages 1-14, XP093195245, Retrieved from the Internet: URL:https://web.archive.org/web/20230530012450/https://www.kaspersky.de/blog/apple-lockdown-mode/29117/ [retrieved on 2024-08-14]	8,9,11, 12
A	the whole document	1-7,10, 13-20

A	US 2016/330218 A1 (HUSSEY ROBERT MICHAEL [US] ET AL) 10 November 2016 (2016-11-10) paragraph [0001] - paragraph [0006] paragraph [0023] - paragraph [0026] paragraph [0029] paragraph [0037] paragraph [0051] paragraph [0055] paragraph [0066] figure 2	1-20

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2024/031893

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2019199752 A1	27-06-2019	CN 111801921 A	20-10-2020
		EP 3732851 A1	04-11-2020
		US 2019199752 A1	27-06-2019
		WO 2019133444 A1	04-07-2019
US 2018288066 A1	04-10-2018	CN 107548547 A	05-01-2018
		DK 3257226 T3	29-10-2018
		EP 3257226 A1	20-12-2017
		US 2018288066 A1	04-10-2018
		WO 2016174261 A1	03-11-2016
US 2016330218 A1	10-11-2016	US 2016330218 A1	10-11-2016
		US 2018248897 A1	30-08-2018