(12) STANDARD PATENT (11) Application No. **AU 2022279466 B2**
(19) AUSTRALIAN PATENT OFFICE

(54) Title
Implementation of biometric authentication

(51) International Patent Classification(s)
G06V 40/00 (2022.01)

(21) Application No: **2022279466** (22) Date of Filing: **2022.11.30**

(43) Publication Date: **2023.02.02**
(43) Publication Journal Date: **2023.02.02**
(44) Accepted Journal Date: **2024.01.25**

(62) Divisional of:
2019281965

(71) Applicant(s)
Apple Inc.

(72) Inventor(s)
Devine, Lynne;van Os, Marcel;Mohseni, Daamun;Anton, Peter D.;Paul, Grant;Dye, Alan C.;De Vries, Nathan;Lindmeier, William D.;Malia, Joseph A.

(74) Agent / Attorney
FPA Patent Attorneys Pty Ltd, Level 19, South Tower 80 Collins Street, Melbourne, VIC, 3000, AU

(56) Related Art
US 2015/0074418 A1
US 2013/0015946 A1

2022279466 30 Nov 2022

ABSTRACT

An electronic device performs techniques related to implementing biometric authentication, including providing user interfaces for: providing indications of error conditions during biometric authentication, providing indications about the biometric sensor during biometric authentication, orienting the device to enroll a biometric feature, and providing an indication of the location of the biometric sensor to correct a detected error condition.

IMPLEMENTATION OF BIOMETRIC AUTHENTICATION

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application is claims priority to U.S. Application No. 16/369,355 filed March 29, 2019 and entitled "IMPLEMENTATION OF BIOMETRIC AUTHENTICATION; U.S. Application No. 62/752,234 filed October 29, 2018 and entitled "IMPLEMENTATION OF BIOMETRIC AUTHENTICATION," and 62/679,955, titled "IMPLEMENTATION OF BIOMETRIC AUTHENTICATION," filed June 3, 2018.

[0001a] This application is related to International Application Number PCT/US2019/035092 (International Publication Number WO 2019/236432) filed on 1 June 2019, the contents of which are incorporated herein by reference in their entirety.

FIELD

[0002] The present disclosure relates generally to biometric authentication, and more specifically to interfaces and techniques for enrollment and authentication of biometric features.

BACKGROUND

[0003] Biometric authentication, for instance of a face, iris, or fingerprint, using electronic devices is a convenient and efficient method of authenticating users of the electronic devices. Biometric authentication allows a device to quickly and easily verify the identity of any number of users.

[0003a] Reference to any prior art in the specification is not an acknowledgement or suggestion that this prior art forms part of the common general knowledge in any jurisdiction or that this prior art could reasonably be expected to be combined with any other piece of prior art by a skilled person in the art.

BRIEF SUMMARY

[0004] Some techniques for implementing biometric authentication using electronic devices, however, are generally cumbersome. When a user fails to enroll a biometric feature for biometric authentication or fails to perform biometric authentication, a user is often unaware of the underlying cause for the failure. Thus, the user can be discouraged from using biometric authentication altogether. Moreover, when the user performs additional attempts to

2022279466 18 Dec 2023

enroll a biometric feature or biometrically authenticate after a failure, the user often does so without having the knowledge to correct the underlying cause of the failure. In view of the foregoing drawbacks, existing techniques require more time than necessary, wasting both user time and device energy. This latter consideration is particularly significant in the operation of battery-operated devices.

[0005] Accordingly, the present technique provides electronic devices with faster, more efficient methods and interfaces for implementing biometric authentication. Such methods and interfaces optionally complement or replace other methods for implementing biometric authentication. 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 reduce the number of unnecessary, extraneous, or repetitive input required at computing devices, such as smartphones and smartwatches.

[0005a] According to a first aspect of the invention there is provided a method, comprising: at an electronic device with a biometric sensor and a touch-sensitive display: detecting occurrence of an error condition for detecting biometric information at the biometric sensor; in response to detecting the occurrence of the error condition, displaying, on the touch-sensitive display, an indication of a location of the biometric sensor on the electronic device, wherein the indication is a graphical indicator that is displayed at a respective location on the touch-sensitive display that is a first distance from a first edge of the electronic device, wherein the first edge of the electronic device corresponds to the location of the biometric sensor on the electronic device, and wherein the respective location on the touch-sensitive display is a second distance from a second edge of the electronic device, wherein the second edge is opposite from the first edge, and wherein the second distance is greater than the first distance; while displaying the indication of the location of the biometric sensor on the electronic device, detecting a request to unlock the electronic device using the biometric sensor; and in response to detecting the request to unlock the electronic device using the biometric sensor: in accordance with a determination that the error condition is still occurring at a respective time that occurs after detecting the request to unlock the electronic device: ceasing to display the indication of the location of the biometric sensor; and displaying a touch-based user interface for entering touch-based authentication information; and in

2022279466 18 Dec 2023

accordance with a determination that the error condition is no longer occurring, attempting to unlock the electronic device using the biometric sensor.

[0005b] According to a second aspect of the invention there is provided a computer-readable storage medium storing one or more programs configured to be executed by one or more processors of an electronic device with a biometric sensor and a touch-sensitive display, the one or more programs including instructions for performing the method of the first aspect.

[0005c] According to a third aspect of the invention there is provided an electronic device, comprising: a biometric sensor; a touch-sensitive display; 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 first aspect.

[0006] In accordance with some examples, a method is described, the method comprising: at an electronic device with a display and one or more input devices: receiving, via the one or more input devices, a request to perform an operation that requires authentication; and in response to the request to perform the operation that requires authentication: in accordance with a determination that authentication is successful, performing the operation; and in accordance with a determination that authentication is not successful and that a set of error condition criteria is met: displaying, on the display, an indication of an error condition, wherein the indication includes information about the cause of the error condition; and forgoing performing the operation.

[0007] In accordance with some examples, a non-transitory computer-readable medium is described, the non-transitory computer-readable storage medium comprising one or more programs configured to be executed by one or more processors of an electronic device with a display 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 perform an operation that requires authentication; and in response to the request to perform the operation that requires authentication: in accordance with a determination that authentication is successful, performing the operation; and in accordance with a determination that authentication is not successful and that a set of error condition criteria is met: displaying, on the display, an indication of an error condition, wherein the indication includes information about the cause of the error condition; and forgoing performing the operation.

2022279466 18 Dec 2023

[0008] In accordance with some examples, a transitory computer-readable medium is described, the transitory computer-readable storage medium comprising one or more programs configured to be executed by one or more processors of an electronic device with a display 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 perform an operation that requires authentication; and in response to the request to perform the operation that requires authentication: in accordance with a determination that authentication is successful, performing the operation; and in accordance with a determination that authentication is not successful and that a set of error condition criteria is met: displaying, on the display, an indication of an error condition, wherein the indication includes information about the cause of the error condition; and forgoing performing the operation.

[0009] In accordance with some examples, an electronic device is described, the electronic device comprising: one or more input devices; a display; 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 perform an operation that requires authentication; and in response to the request to perform the operation that requires authentication: in accordance with a determination that authentication is successful, performing the operation; and in accordance with a determination that authentication is not successful and that a set of error condition criteria is met: displaying, on the display, an indication of an error condition, wherein the indication includes information about the cause of the error condition; and forgoing performing the operation.

[0010] In accordance with some examples, an electronic device is described, the electronic device comprising: one or more input devices; a display; means for receiving, via the one or more input devices, a request to perform an operation that requires authentication; and means for, in response to the request to perform the operation that requires authentication: in accordance with a determination that authentication is successful, performing the operation; and in accordance with a determination that authentication is not successful and that a set of error condition criteria is met: displaying, on the display, an indication of an error condition, wherein the indication includes information about the cause of the error condition; and forgoing performing the operation.

[0011] In accordance with some examples, a method is described, the method comprising: at an electronic device with a display and a biometric sensor at a first portion of the electronic device: detecting the existence of an error condition that prevents the biometric sensor from obtaining biometric information about a user of the device; in response to detecting the existence of the error condition, displaying, on the display, an error indication,

wherein the error indication is displayed at a location that is proximate to the first portion of the electronic device, including: in accordance with a determination that a user interface of the electronic device is in a first orientation relative to the biometric sensor, displaying the error indication at a first location in the user interface that is proximate to the first portion of the electronic device; and in accordance with a determination that the user interface of the electronic device is in a second orientation relative to the biometric sensor, displaying the error indication at a second location in the user interface that is proximate to the first portion of the electronic device, the first orientation being different from the second orientation.

[0012] In accordance with some examples, a non-transitory computer-readable medium is described, the non-transitory computer-readable storage medium comprising one or more programs configured to be executed by one or more processors of an electronic device with a display and a biometric sensor at a first portion of the electronic device, the one or more programs including instructions for: detecting the existence of an error condition that prevents the biometric sensor from obtaining biometric information about a user of the device; in response to detecting the existence of the error condition, displaying, on the display, an error indication, wherein the error indication is displayed at a location that is proximate to the first portion of the electronic device, including: in accordance with a determination that a user interface of the electronic device is in a first orientation relative to the biometric sensor, displaying the error indication at a first location in the user interface that is proximate to the first portion of the electronic device; and in accordance with a determination that the user interface of the electronic device is in a second orientation relative to the biometric sensor, displaying the error indication at a second location in the user interface that is proximate to the first portion of the electronic device, the first orientation being different from the second orientation.

[0013] In accordance with some examples, a transitory computer-readable medium is described, the transitory computer-readable storage medium comprising one or more programs configured to be executed by one or more processors of an electronic device with a display and a biometric sensor at a first portion of the electronic device, the one or more programs including instructions for: detecting the existence of an error condition that prevents the biometric sensor from obtaining biometric information about a user of the device; in response to detecting the existence of the error condition, displaying, on the display, an error indication, wherein the error indication is displayed at a location that is

proximate to the first portion of the electronic device, including: in accordance with a determination that a user interface of the electronic device is in a first orientation relative to the biometric sensor, displaying the error indication at a first location in the user interface that is proximate to the first portion of the electronic device; and in accordance with a determination that the user interface of the electronic device is in a second orientation relative to the biometric sensor, displaying the error indication at a second location in the user interface that is proximate to the first portion of the electronic device, the first orientation being different from the second orientation.

[0014] In accordance with some examples, an electronic device is described, the electronic device comprising: a biometric sensor at a first portion of the electronic device; a display; 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: detecting the existence of an error condition that prevents the biometric sensor from obtaining biometric information about a user of the device; in response to detecting the existence of the error condition, displaying, on the display, an error indication, wherein the error indication is displayed at a location that is proximate to the first portion of the electronic device, including: in accordance with a determination that a user interface of the electronic device is in a first orientation relative to the biometric sensor, displaying the error indication at a first location in the user interface that is proximate to the first portion of the electronic device; and in accordance with a determination that the user interface of the electronic device is in a second orientation relative to the biometric sensor, displaying the error indication at a second location in the user interface that is proximate to the first portion of the electronic device, the first orientation being different from the second orientation.

[0015] In accordance with some examples, an electronic device is described, the electronic device comprising: a biometric sensor at a first portion of the electronic device; a display; means for detecting the existence of an error condition that prevents the biometric sensor from obtaining biometric information about a user of the device; means for, in response to detecting the existence of the error condition, displaying, on the display, an error indication, wherein the error indication is displayed at a location that is proximate to the first portion of the electronic device, including: in accordance with a determination that a user interface of the electronic device is in a first orientation relative to the biometric sensor, displaying the error indication at a first location in the user interface that is proximate to the

first portion of the electronic device; and in accordance with a determination that the user interface of the electronic device is in a second orientation relative to the biometric sensor, displaying the error indication at a second location in the user interface that is proximate to the first portion of the electronic device, the first orientation being different from the second orientation.

[0016] In accordance with some examples, a method is described, the method comprising: at an electronic device with a display and one or more biometric sensors: displaying, on the display, a biometric enrollment user interface for initiating biometric enrollment with the one or more biometric sensors; while displaying the biometric enrollment user interface, receiving input corresponding for a request to initiate biometric enrollment; and in response to receiving the input: in accordance with a determination that an orientation of the electronic device satisfies a set of enrollment criteria, initiating a process for enrolling a biometric feature with the one or more biometric sensors; and in accordance with a determination that the orientation of the electronic device does not satisfy the set of enrollment criteria, outputting one or more prompts to change the orientation of the electronic device to a different orientation that satisfies the set of enrollment criteria.

[0017] In accordance with some examples, a non-transitory computer-readable medium is described, the non-transitory computer-readable storage medium comprising one or more programs configured to be executed by one or more processors of an electronic device with a display and one or more biometric sensors, the one or more programs including instructions for: displaying, on the display, a biometric enrollment user interface for initiating biometric enrollment with the one or more biometric sensors; while displaying the biometric enrollment user interface, receiving input corresponding for a request to initiate biometric enrollment; and in response to receiving the input: in accordance with a determination that an orientation of the electronic device satisfies a set of enrollment criteria, initiating a process for enrolling a biometric feature with the one or more biometric sensors; and in accordance with a determination that the orientation of the electronic device does not satisfy the set of enrollment criteria, outputting one or more prompts to change the orientation of the electronic device to a different orientation that satisfies the set of enrollment criteria.

[0018] In accordance with some examples, a transitory computer-readable medium is described, the transitory computer-readable storage medium comprising one or more programs configured to be executed by one or more processors of an electronic device with a

display and one or more biometric sensors, the one or more programs including instructions for: displaying, on the display, a biometric enrollment user interface for initiating biometric enrollment with the one or more biometric sensors; while displaying the biometric enrollment user interface, receiving input corresponding for a request to initiate biometric enrollment; and in response to receiving the input: in accordance with a determination that an orientation of the electronic device satisfies a set of enrollment criteria, initiating a process for enrolling a biometric feature with the one or more biometric sensors; and in accordance with a determination that the orientation of the electronic device does not satisfy the set of enrollment criteria, outputting one or more prompts to change the orientation of the electronic device to a different orientation that satisfies the set of enrollment criteria.

[0019] In accordance with some examples, an electronic device is described, the electronic device comprising: one or more biometric sensors; a display; 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: displaying, on the display, a biometric enrollment user interface for initiating biometric enrollment with the one or more biometric sensors; while displaying the biometric enrollment user interface, receiving input corresponding for a request to initiate biometric enrollment; and in response to receiving the input: in accordance with a determination that an orientation of the electronic device satisfies a set of enrollment criteria, initiating a process for enrolling a biometric feature with the one or more biometric sensors; and in accordance with a determination that the orientation of the electronic device does not satisfy the set of enrollment criteria, outputting one or more prompts to change the orientation of the electronic device to a different orientation that satisfies the set of enrollment criteria.

[0020] In accordance with some examples, an electronic device is described, the electronic device comprising: one or more biometric sensors; a display; means for displaying, on the display, a biometric enrollment user interface for initiating biometric enrollment with the one or more biometric sensors; means for, while displaying the biometric enrollment user interface, receiving input corresponding for a request to initiate biometric enrollment; and means for, in response to receiving the input: in accordance with a determination that an orientation of the electronic device satisfies a set of enrollment criteria, initiating a process for enrolling a biometric feature with the one or more biometric sensors; and in accordance with a determination that the orientation of the electronic device does not satisfy the set of

enrollment criteria, outputting one or more prompts to change the orientation of the electronic device to a different orientation that satisfies the set of enrollment criteria.

[0021] In accordance with some examples, a method is described, the method comprising: at an electronic device with a biometric sensor and a touch-sensitive display: detecting occurrence of an error condition for detecting biometric information at the biometric sensor; in response to detecting the occurrence of the error condition, displaying, on the touch-sensitive display, an indication of a location of the biometric sensor on the electronic device; while displaying the indication of the location of the biometric sensor on the electronic device, detecting a request to unlock the electronic device using the biometric sensor; and in response to detecting the request to unlock the electronic device using the biometric sensor: in accordance with a determination that the error condition is still occurring at a respective time that occurs after detecting the request to unlock the electronic device: ceasing to display the indication of the location of the biometric sensor; and displaying a touch-based user interface for entering touch-based authentication information; and in accordance with a determination that the error condition is no longer occurring, attempting to unlock the electronic device using the biometric sensor.

[0022] In accordance with some examples, a non-transitory computer-readable medium is described, the non-transitory computer-readable storage medium storing one or more programs configured to be executed by one or more processors of an electronic device with a biometric sensor and a touch-sensitive display, the one or more programs including instructions for: detecting occurrence of an error condition for detecting biometric information at the biometric sensor; in response to detecting the occurrence of the error condition, displaying, on the touch-sensitive display, an indication of a location of the biometric sensor on the electronic device; while displaying the indication of the location of the biometric sensor on the electronic device, detecting a request to unlock the electronic device using the biometric sensor; and in response to detecting the request to unlock the electronic device using the biometric sensor: in accordance with a determination that the error condition is still occurring at a respective time that occurs after detecting the request to unlock the electronic device: ceasing to display the indication of the location of the biometric sensor; and displaying a touch-based user interface for entering touch-based authentication information; and in accordance with a determination that the error condition is no longer occurring, attempting to unlock the electronic device using the biometric sensor.

[0023] In accordance with some examples, a transitory computer-readable medium is described, the transitory computer-readable storage medium storing one or more programs configured to be executed by one or more processors of an electronic device with a biometric sensor and a touch-sensitive display, the one or more programs including instructions for: detecting occurrence of an error condition for detecting biometric information at the biometric sensor; in response to detecting the occurrence of the error condition, displaying, on the touch-sensitive display, an indication of a location of the biometric sensor on the electronic device; while displaying the indication of the location of the biometric sensor on the electronic device, detecting a request to unlock the electronic device using the biometric sensor; and in response to detecting the request to unlock the electronic device using the biometric sensor: in accordance with a determination that the error condition is still occurring at a respective time that occurs after detecting the request to unlock the electronic device: ceasing to display the indication of the location of the biometric sensor; and displaying a touch-based user interface for entering touch-based authentication information; and in accordance with a determination that the error condition is no longer occurring, attempting to unlock the electronic device using the biometric sensor.

[0024] In accordance with some examples, an electronic device is described, the electronic device comprising: a biometric sensor; a touch-sensitive display; 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: detecting occurrence of an error condition for detecting biometric information at the biometric sensor; in response to detecting the occurrence of the error condition, displaying, on the touch-sensitive display, an indication of a location of the biometric sensor on the electronic device; while displaying the indication of the location of the biometric sensor on the electronic device, detecting a request to unlock the electronic device using the biometric sensor; and in response to detecting the request to unlock the electronic device using the biometric sensor: in accordance with a determination that the error condition is still occurring at a respective time that occurs after detecting the request to unlock the electronic device: ceasing to display the indication of the location of the biometric sensor; and displaying a touch-based user interface for entering touch-based authentication information; and in accordance with a determination that the error condition is no longer occurring, attempting to unlock the electronic device using the biometric sensor.

[0025] In accordance with some examples, an electronic device is described, the electronic device comprising: a biometric sensor; a touch-sensitive display; means for detecting occurrence of an error condition for detecting biometric information at the biometric sensor; means, in response to detecting the occurrence of the error condition, for displaying, on the touch-sensitive display, an indication of a location of the biometric sensor on the electronic device; means, while displaying the indication of the location of the biometric sensor on the electronic device, for detecting a request to unlock the electronic device using the biometric sensor; and means, in response to detecting the request to unlock the electronic device using the biometric sensor, for: in accordance with a determination that the error condition is still occurring at a respective time that occurs after detecting the request to unlock the electronic device: ceasing to display the indication of the location of the biometric sensor; and displaying a touch-based user interface for entering touch-based authentication information; and in accordance with a determination that the error condition is no longer occurring, attempting to unlock the electronic device using the biometric sensor.

[0026] 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.

[0027] Thus, devices are provided with faster, more efficient methods and interfaces for implementing biometric authentication, thereby increasing the effectiveness, efficiency, and user satisfaction with such devices. Such methods and interfaces optionally complement or replace other methods for implementing biometric authentication.

DESCRIPTION OF THE FIGURES

[0028] For a better understanding of the various described examples, 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.

[0029] FIG. 1A is a block diagram illustrating a portable multifunction device with a touch-sensitive display in accordance with some embodiments.

[0030] FIG. 1B is a block diagram illustrating exemplary components for event handling in accordance with some embodiments.

[0031] FIG. 1C is a block diagram illustrating exemplary components for generating a tactile output, in accordance with some embodiments.

[0032] FIG. 2 illustrates a portable multifunction device having a touch screen in accordance with some embodiments.

[0033] FIG. 3 is a block diagram of an exemplary multifunction device with a display and a touch-sensitive surface in accordance with some embodiments.

[0034] FIG. 4A illustrates an exemplary user interface for a menu of applications on a portable multifunction device in accordance with some embodiments.

[0035] 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.

[0036] FIGS. 4C-4H illustrate exemplary tactile output patterns that have a particular waveform, in accordance with some embodiments.

[0037] FIG. 5A illustrates a personal electronic device in accordance with some embodiments.

[0038] FIG. 5B is a block diagram illustrating a personal electronic device in accordance with some embodiments.

[0039] FIGS. 5C-5D illustrate exemplary components of a personal electronic device having a touch-sensitive display and intensity sensors in accordance with some embodiments.

[0040] FIGS. 5E-5H illustrate exemplary components and user interfaces of a personal electronic device in accordance with some embodiments.

[0041] FIG. 6 illustrates exemplary devices connected via one or more communication channels, in accordance with some embodiments.

[0042] FIGS. 7A-7AD illustrate exemplary user interfaces for providing indications of error conditions during biometric authentication, in accordance with some examples.

[0043] FIGS. 8A-8B are flow diagrams illustrating a method for providing indications of error conditions during biometric authentication, in accordance with some examples

[0044] FIGS. 9A-9U illustrate exemplary user interfaces for providing indications about the biometric sensor during biometric authentication, in accordance with some examples.

[0045] FIGS. 10A-10C are flow diagrams illustrating a method for providing indications about the biometric sensor during biometric authentication, in accordance with some examples.

[0046] FIGS. 11A-11S illustrate exemplary user interfaces for orienting the device to enroll a biometric feature, in accordance with some examples

[0047] FIGS. 12A-12C are flow diagrams illustrating a method for orienting the device to enroll a biometric feature, in accordance with some examples.

[0048] FIGS. 13A-13Z illustrate exemplary user interfaces for providing an indication of the location of the biometric sensor to correct a detected error condition, in accordance with some examples.

[0049] FIGS. 14A-14B are flow diagrams illustrating a method for providing an indication of the location of the biometric sensor to correct a detected error condition, in accordance with some examples.

DESCRIPTION OF EMBODIMENTS

[0050] 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.

[0051] There is a need for electronic devices that provide efficient methods and interfaces for implementing biometric authentication of biometric features. For example, there is a need for electronic devices that provide a convenient and efficient method for enrolling one or

more portions of a biometric feature. For another example, there is a need for electronic devices that provide a quick and intuitive technique for selectively accessing secure data in accordance with biometric authentication. For another example, there is a need for electronic devices that provide a quick and intuitive technique for enabling a function of a device in accordance with biometric authentication. Such techniques can reduce the cognitive burden on a user who enrolls a biometric feature and/or biometrically authenticates with a device, thereby enhancing overall productivity. Further, such techniques can reduce processor and battery power otherwise wasted on redundant user inputs.

[0052] Below, FIGS. 1A-1C, 2, 3, 4A-4B, and 5A-5H provide a description of exemplary devices for performing the techniques for implementing biometric authentication. FIG. 6 illustrates exemplary devices connected via one or more communication channels, in accordance with some embodiments. FIGS. 7A-7AD illustrate exemplary user interfaces for providing indications of error conditions during biometric authentication. FIGS. 8A-8B are flow diagrams illustrating a method for providing indications of error conditions during biometric authentication. The user interfaces in FIGS. 7A-7AD are used to illustrate the processes described below, including the processes in 8A-8B. FIGS. 9A-9U illustrate exemplary user interfaces for providing indications about the biometric sensor during biometric authentication. FIGS. 10A-10C are flow diagrams illustrating a method for providing indications about the biometric sensor during biometric authentication. The user interfaces in FIGS. 9A-9U are used to illustrate the processes described below, including the processes in FIGS. 10A-10C. FIGS. 11A-11S illustrate exemplary user interfaces for orienting the device to enroll a biometric feature. FIGS. 12A-12C are flow diagrams illustrating a method for orienting the device to enroll a biometric feature. The user interfaces in FIGS. 11A-11S are used to illustrate the processes described below, including the processes in FIGS. 12A-12C. FIGS. 13A-13Z illustrate exemplary user interfaces for providing an indication of the location of the biometric sensor to correct a detected error condition. FIGS. 14A-14B are flow diagrams illustrating a method for providing an indication of the location of the biometric sensor to correct a detected error condition. The user interfaces in FIGS. 13A-13Z are used to illustrate the processes described below, including the processes in FIGS. 14A-14B.

[0053] Although the following description uses terms “first,” “second,” etc. to describe various elements, these elements should not be limited by the terms. These terms are only

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. The first touch and the second touch are both touches, but they are not the same touch.

[0054] 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.

[0055] 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.

[0056] 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).

[0057] 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.

[0058] 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.

[0059] 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.

[0060] 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.

[0061] 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 is, in some circumstances, 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).

[0062] 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. Using tactile outputs to provide haptic feedback to a user enhances the operability of the device and makes the user-device interface more efficient (e.g., by helping the user to provide proper inputs and reducing user mistakes when operating/interacting with the device) which, additionally, reduces power usage and improves battery life of the device by enabling the user to use the device more quickly and efficiently.

[0063] In some embodiments, a tactile output pattern specifies characteristics of a tactile output, such as the amplitude of the tactile output, the shape of a movement waveform of the tactile output, the frequency of the tactile output, and/or the duration of the tactile output.

[0064] When tactile outputs with different tactile output patterns are generated by a device (e.g., via one or more tactile output generators that move a moveable mass to generate tactile outputs), the tactile outputs can invoke different haptic sensations in a user holding or touching the device. While the sensation of the user is based on the user's perception of the tactile output, most users will be able to identify changes in waveform, frequency, and amplitude of tactile outputs generated by the device. Thus, the waveform, frequency and amplitude can be adjusted to indicate to the user that different operations have been performed. As such, tactile outputs with tactile output patterns that are designed, selected, and/or engineered to simulate characteristics (e.g., size, material, weight, stiffness, smoothness, etc.); behaviors (e.g., oscillation, displacement, acceleration, rotation, expansion, etc.); and/or interactions (e.g., collision, adhesion, repulsion, attraction, friction, etc.) of objects in a given environment (e.g., a user interface that includes graphical features and objects, a simulated physical environment with virtual boundaries and virtual objects, a real physical environment with physical boundaries and physical objects, and/or a combination of any of the above) will, in some circumstances, provide helpful feedback to users that reduces input errors and increases the efficiency of the user's operation of the device. Additionally, tactile outputs are, optionally, generated to correspond to feedback that is unrelated to a simulated physical characteristic, such as an input threshold or a selection of an object. Such tactile outputs will, in some circumstances, provide helpful feedback to users that reduces input errors and increases the efficiency of the user's operation of the device.

[0065] In some embodiments, a tactile output with a suitable tactile output pattern serves as a cue for the occurrence of an event of interest in a user interface or behind the scenes in a device. Examples of the events of interest include activation of an affordance (e.g., a real or virtual button, or toggle switch) provided on the device or in a user interface, success or failure of a requested operation, reaching or crossing a boundary in a user interface, entry into a new state, switching of input focus between objects, activation of a new mode, reaching or crossing an input threshold, detection or recognition of a type of input or gesture, etc. In some embodiments, tactile outputs are provided to serve as a warning or an alert for an impending event or outcome that would occur unless a redirection or interruption input is timely detected. Tactile outputs are also used in other contexts to enrich the user experience, improve the accessibility of the device to users with visual or motor difficulties or other accessibility needs, and/or improve efficiency and functionality of the user interface and/or the device. Tactile outputs are optionally accompanied with audio outputs and/or visible user

interface changes, which further enhance a user's experience when the user interacts with a user interface and/or the device, and facilitate better conveyance of information regarding the state of the user interface and/or the device, and which reduce input errors and increase the efficiency of the user's operation of the device.

[0066] FIGS. 4C-4E provide a set of sample tactile output patterns that can be used, either individually or in combination, either as is or through one or more transformations (e.g., modulation, amplification, truncation, etc.), to create suitable haptic feedback in various scenarios and for various purposes, such as those mentioned above and those described with respect to the user interfaces and methods discussed herein. This example of a palette of tactile outputs shows how a set of three waveforms and eight frequencies can be used to produce an array of tactile output patterns. In addition to the tactile output patterns shown in this figure, each of these tactile output patterns is optionally adjusted in amplitude by changing a gain value for the tactile output pattern, as shown, for example for FullTap 80Hz, FullTap 200Hz, MiniTap 80Hz, MiniTap 200Hz, MicroTap 80Hz, and MicroTap 200Hz in FIGS. 4F-4H, which are each shown with variants having a gain of 1.0, 0.75, 0.5, and 0.25. As shown in FIGS. 4F-4H, changing the gain of a tactile output pattern changes the amplitude of the pattern without changing the frequency of the pattern or changing the shape of the waveform. In some embodiments, changing the frequency of a tactile output pattern also results in a lower amplitude as some tactile output generators are limited by how much force can be applied to the moveable mass and thus higher frequency movements of the mass are constrained to lower amplitudes to ensure that the acceleration needed to create the waveform does not require force outside of an operational force range of the tactile output generator (e.g., the peak amplitudes of the FullTap at 230Hz, 270Hz, and 300Hz are lower than the amplitudes of the FullTap at 80Hz, 100Hz, 125Hz, and 200Hz).

[0067] FIGS. 4C-4H show tactile output patterns that have a particular waveform. The waveform of a tactile output pattern represents the pattern of physical displacements relative to a neutral position (e.g., x_{zero}) versus time that an moveable mass goes through to generate a tactile output with that tactile output pattern. For example, a first set of tactile output patterns shown in FIG. 4C (e.g., tactile output patterns of a "FullTap") each have a waveform that includes an oscillation with two complete cycles (e.g., an oscillation that starts and ends in a neutral position and crosses the neutral position three times). A second set of tactile output patterns shown in FIG. 4D (e.g., tactile output patterns of a "MiniTap") each have a

waveform that includes an oscillation that includes one complete cycle (e.g., an oscillation that starts and ends in a neutral position and crosses the neutral position one time). A third set of tactile output patterns shown in FIG. 4E (e.g., tactile output patterns of a "MicroTap") each have a waveform that includes an oscillation that include one half of a complete cycle (e.g., an oscillation that starts and ends in a neutral position and does not cross the neutral position). The waveform of a tactile output pattern also includes a start buffer and an end buffer that represent the gradual speeding up and slowing down of the moveable mass at the start and at the end of the tactile output. The example waveforms shown in FIGS. 4C-4H include x_{min} and x_{max} values which represent the maximum and minimum extent of movement of the moveable mass. For larger electronic devices with larger moveable masses, there can be larger or smaller minimum and maximum extents of movement of the mass. The examples shown in FIGS. 4C-4H describe movement of a mass in 1 dimension, however similar principles would also apply to movement of a moveable mass in two or three dimensions.

[0068] As shown in FIGS. 4C-4E, each tactile output pattern also has a corresponding characteristic frequency that affects the "pitch" of a haptic sensation that is felt by a user from a tactile output with that characteristic frequency. For a continuous tactile output, the characteristic frequency represents the number of cycles that are completed within a given period of time (e.g., cycles per second) by the moveable mass of the tactile output generator. For a discrete tactile output, a discrete output signal (e.g., with 0.5, 1, or 2 cycles) is generated, and the characteristic frequency value specifies how fast the moveable mass needs to move to generate a tactile output with that characteristic frequency. As shown in FIGS. 4C-4H, for each type of tactile output (e.g., as defined by a respective waveform, such as FullTap, MiniTap, or MicroTap), a higher frequency value corresponds to faster movement(s) by the moveable mass, and hence, in general, a shorter time to complete the tactile output (e.g., including the time to complete the required number of cycle(s) for the discrete tactile output, plus a start and an end buffer time). For example, a FullTap with a characteristic frequency of 80Hz takes longer to complete than FullTap with a characteristic frequency of 100Hz (e.g., 35.4ms vs. 28.3ms in FIG. 4C). In addition, for a given frequency, a tactile output with more cycles in its waveform at a respective frequency takes longer to complete than a tactile output with fewer cycles its waveform at the same respective frequency. For example, a FullTap at 150Hz takes longer to complete than a MiniTap at 150Hz (e.g., 19.4ms vs. 12.8ms), and a MiniTap at 150Hz takes longer to complete than a MicroTap at 150Hz (e.g., 12.8ms vs. 9.4ms). However, for tactile output patterns with different frequencies this

rule may not apply (e.g., tactile outputs with more cycles but a higher frequency can take a shorter amount of time to complete than tactile outputs with fewer cycles but a lower frequency, and vice versa). For example, at 300Hz, a FullTap takes as long as a MiniTap (e.g., 9.9 ms).

[0069] As shown in FIGS. 4C-4E, a tactile output pattern also has a characteristic amplitude that affects the amount of energy that is contained in a tactile signal, or a "strength" of a haptic sensation that can be felt by a user through a tactile output with that characteristic amplitude. In some embodiments, the characteristic amplitude of a tactile output pattern refers to an absolute or normalized value that represents the maximum displacement of the moveable mass from a neutral position when generating the tactile output. In some embodiments, the characteristic amplitude of a tactile output pattern is adjustable, e.g., by a fixed or dynamically determined gain factor (e.g., a value between 0 and 1), in accordance with various conditions (e.g., customized based on user interface contexts and behaviors) and/or preconfigured metrics (e.g., input-based metrics, and/or user-interface-based metrics). In some embodiments, an input-based metric (e.g., an intensity-change metric or an input-speed metric) measures a characteristic of an input (e.g., a rate of change of a characteristic intensity of a contact in a press input or a rate of movement of the contact across a touch-sensitive surface) during the input that triggers generation of a tactile output. In some embodiments, a user-interface-based metric (e.g., a speed-across-boundary metric) measures a characteristic of a user interface element (e.g., a speed of movement of the element across a hidden or visible boundary in a user interface) during the user interface change that triggers generation of the tactile output. In some embodiments, the characteristic amplitude of a tactile output pattern can be modulated by an "envelope" and the peaks of adjacent cycles can have different amplitudes, where one of the waveforms shown above is further modified by multiplication by an envelope parameter that changes over time (e.g., from 0 to 1) to gradually adjust amplitude of portions of the tactile output over time as the tactile output is being generated.

[0070] Although specific frequencies, amplitudes, and waveforms are represented in the sample tactile output patterns in FIGS. 4C-4E for illustrative purposes, tactile output patterns with other frequencies, amplitudes, and waveforms can be used for similar purposes. For example, waveforms that have between 0.5 to 4 cycles can be used. Other frequencies in the

range of 60Hz-400Hz can be used as well. Table 1 provides examples of particular haptic feedback behaviors, configurations, and examples of their use.

[0071] 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.

[0072] 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.

[0073] 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 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.

[0074] 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.

[0075] 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).

[0076] 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, intensity sensor controller 159, haptic feedback controller 161, depth camera controller 169, 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 alternate 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).

[0077] 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.

[0078] 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.

[0079] 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.

[0080] 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.

[0081] 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.

[0082] 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.

[0083] 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.

[0084] 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.

[0085] 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.

[0086] 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.

[0087] 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.

[0088] 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).

[0089] 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.

[0090] 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.

[0091] In some embodiments, device 100 also includes (or is in communication with) one or more fingerprint sensors. The one or more fingerprint sensors are coupled to peripherals interface 118. Alternately, the one or more fingerprint sensors are, optionally, coupled to an input controller 160 in I/O subsystem 106. However, in one common embodiment, fingerprint identification operations are performed using secured dedicated computing hardware (e.g., one or more processors, memory and/or communications busses) that has additional security features so as to enhance security of the fingerprint information determined by the one or more fingerprint sensors. As used herein, a fingerprint sensor is a

sensor that is capable of distinguishing fingerprint features (sometimes called "minutia features") of the ridges and valleys of skin such as those found on the fingers and toes of humans. A fingerprint sensor can use any of a variety of techniques to distinguish the fingerprint features, including but not limited to: optical fingerprint imaging, ultrasonic fingerprint imaging, active capacitance fingerprint imaging and passive capacitance fingerprint imaging. In addition to distinguishing fingerprint features in fingerprints, in some embodiments, the one or more fingerprint sensors are capable of tracking movement of fingerprint features over time and thereby determining/characterizing movement of the fingerprint over time on the one or more fingerprint sensors. While the one or more fingerprint sensors can be separate from the touch-sensitive surface (e.g., Touch-Sensitive Display System 112), it should be understood that in some implementations, the touch-sensitive surface (e.g., Touch-Sensitive Display System 112) has a spatial resolution that is high enough to detect fingerprint features formed by individual fingerprint ridges and is used as a fingerprint sensor instead of, or in addition to, the one or more fingerprint sensors. In some embodiments, device 100 includes a set of one or more orientation sensors that are used to determine an orientation of a finger or hand on or proximate to the device (e.g., an orientation of a finger that is over one or more fingerprint sensors). Additionally, in some embodiments, the set of one or more orientation sensors are used in addition to or instead of a fingerprint sensor to detect rotation of a contact that is interacting with the device (e.g., in one or more of the methods described below, instead of using a fingerprint sensor to detect rotation of a fingerprint/contact, the set of one or more orientation sensors is used to detect rotation of the contact that includes the fingerprint, with or without detecting features of the fingerprint).

[0092] In some embodiments, features of fingerprints and comparisons between features of detected fingerprints and features of stored fingerprints are performed by secured dedicated computing hardware (e.g., one or more processors, memory and/or communications busses) that are separate from processor(s) 120, so as to improve security of the fingerprint data generated, stored and processed by the one or more fingerprint sensors. In some embodiments, features of fingerprints and comparisons between features of detected fingerprints and features of enrolled fingerprints are performed by processor(s) 120 using a fingerprint analysis module.

[0093] In some embodiments, during an enrollment process, the device (e.g., a fingerprint analysis module or a separate secure module in communication with the one or more fingerprint sensors) collects biometric information about one or more fingerprints of the user (e.g., identifying relative location of a plurality of minutia points in a fingerprint of the user). After the enrollment process has been completed the biometric information is stored at the device (e.g., in a secure fingerprint module) for later use in authenticating detected fingerprints. In some embodiments, the biometric information that is stored at the device excludes images of the fingerprints and also excludes information from which images of the fingerprints could be reconstructed so that images of the fingerprints are not inadvertently made available if the security of the device is compromised. In some embodiments, during an authentication process, the device (e.g., a fingerprint analysis module or a separate secure module in communication with the one or more fingerprint sensors) determines whether a finger input detected by the one or more fingerprint sensors includes a fingerprint that matches a previously enrolled fingerprint by collecting biometric information about a fingerprint detected on the one or more fingerprint sensors (e.g., identifying relative locations of a plurality of minutia points in the fingerprint detected on the one or more fingerprint sensors) and comparing the biometric information that corresponds to the detected fingerprint to biometric information that corresponds to the enrolled fingerprints(s). In some embodiments, comparing the biometric information that corresponds to the detected fingerprint to biometric information that corresponds to the enrolled fingerprints(s) includes comparing a type and location of minutia points in the biometric information that corresponds to the detected fingerprint to a type and location of minutia points in the biometric information that corresponds to the enrolled fingerprints. However the determination as to whether or not a finger input includes a fingerprint that matches a previously enrolled fingerprint that is enrolled with the device is, optionally, performed using any of a number of well-known fingerprint authentication techniques for determining whether a detected fingerprint matches an enrolled fingerprint.

[0094] 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.

[0095] 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.

[0096] 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.

[0097] 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.

[0098] 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.

[0099] 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).

[0100] 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.

[0101] 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.

[0102] 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.

[0103] 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.

[0104] 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 137, e-mail 140, IM 141, browser 147, and any other application that needs text input).

[0105] GPS module 135 determines the location of the device and provides this information for use in various applications (e.g., to telephone 138 for use in location-based dialing; to camera 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).

[0106] 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.

[0107] 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.

[0108] 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 138, video conference module 139, e-mail 140, or IM 141; and so forth.

[0109] 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.

[0110] 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.

[0111] 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.

[0112] 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).

[0113] 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.

[0114] 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.

[0115] 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.

[0116] 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.

[0117] 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.

[0118] 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).

[0119] 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).

[0120] 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.

[0121] 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.).

[0122] 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.

[0123] 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.

[0124] 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.

[0125] 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, 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.

[0126] 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.

[0127] 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.

[0128] 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).

[0129] 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.

[0130] 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.

[0131] 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.

[0132] 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).

[0133] In some embodiments, event sorter 170 also includes a hit view determination module 172 and/or an active event recognizer determination module 173.

[0134] 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.

[0135] 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.

[0136] 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.

[0137] 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.

[0138] 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.

[0139] 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.

[0140] 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.

[0141] 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).

[0142] 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.

[0143] 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 (187) 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.

[0144] In some embodiments, event definition 187 includes 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.

[0145] 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.

[0146] 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.

[0147] 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.

[0148] 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.

[0149] 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.

[0150] 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.

[0151] 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.

[0152] FIG. 1C is a block diagram illustrating a tactile output module in accordance with some embodiments. In some embodiments, I/O subsystem 106 (e.g., haptic feedback controller 161 (FIG. 1A) and/or other input controller(s) 160 (FIG. 1A)) includes at least some of the example components shown in FIG. 1C. In some embodiments, peripherals interface 118 includes at least some of the example components shown in FIG. 1C.

[0153] In some embodiments, the tactile output module includes haptic feedback module 133. In some embodiments, haptic feedback module 133 aggregates and combines tactile outputs for user interface feedback from software applications on the electronic device (e.g., feedback that is responsive to user inputs that correspond to displayed user interfaces and alerts and other notifications that indicate the performance of operations or occurrence of events in user interfaces of the electronic device). Haptic feedback module 133 includes one or more of: waveform module 123 (for providing waveforms used for generating tactile outputs), mixer 125 (for mixing waveforms, such as waveforms in different channels), compressor 127 (for reducing or compressing a dynamic range of the waveforms), low-pass filter 129 (for filtering out high frequency signal components in the waveforms), and thermal controller 131 (for adjusting the waveforms in accordance with thermal conditions). In some embodiments, haptic feedback module 133 is included in haptic feedback controller 161 (FIG. 1A). In some embodiments, a separate unit of haptic feedback module 133 (or a separate implementation of haptic feedback module 133) is also included in an audio

controller (e.g., audio circuitry 110, FIG. 1A) and used for generating audio signals. In some embodiments, a single haptic feedback module 133 is used for generating audio signals and generating waveforms for tactile outputs.

[0154] In some embodiments, haptic feedback module 133 also includes trigger module 121 (e.g., a software application, operating system, or other software module that determines a tactile output is to be generated and initiates the process for generating the corresponding tactile output). In some embodiments, trigger module 121 generates trigger signals for initiating generation of waveforms (e.g., by waveform module 123). For example, trigger module 121 generates trigger signals based on preset timing criteria. In some embodiments, trigger module 121 receives trigger signals from outside haptic feedback module 133 (e.g., in some embodiments, haptic feedback module 133 receives trigger signals from hardware input processing module 146 located outside haptic feedback module 133) and relays the trigger signals to other components within haptic feedback module 133 (e.g., waveform module 123) or software applications that trigger operations (e.g., with trigger module 121) based on activation of a user interface element (e.g., an application icon or an affordance within an application) or a hardware input device (e.g., a home button or an intensity-sensitive input surface, such as an intensity-sensitive touch screen). In some embodiments, trigger module 121 also receives tactile feedback generation instructions (e.g., from haptic feedback module 133, FIGS. 1A and 3). In some embodiments, trigger module 121 generates trigger signals in response to haptic feedback module 133 (or trigger module 121 in haptic feedback module 133) receiving tactile feedback instructions (e.g., from haptic feedback module 133, FIGS. 1A and 3).

[0155] Waveform module 123 receives trigger signals (e.g., from trigger module 121) as an input, and in response to receiving trigger signals, provides waveforms for generation of one or more tactile outputs (e.g., waveforms selected from a predefined set of waveforms designated for use by waveform module 123, such as the waveforms described in greater detail below with reference to FIGS. 4C-4D).

[0156] Mixer 125 receives waveforms (e.g., from waveform module 123) as an input, and mixes together the waveforms. For example, when mixer 125 receives two or more waveforms (e.g., a first waveform in a first channel and a second waveform that at least partially overlaps with the first waveform in a second channel) mixer 125 outputs a combined waveform that corresponds to a sum of the two or more waveforms. In some embodiments,

mixer 125 also modifies one or more waveforms of the two or more waveforms to emphasize particular waveform(s) over the rest of the two or more waveforms (e.g., by increasing a scale of the particular waveform(s) and/or decreasing a scale of the rest of the waveforms). In some circumstances, mixer 125 selects one or more waveforms to remove from the combined waveform (e.g., the waveform from the oldest source is dropped when there are waveforms from more than three sources that have been requested to be output concurrently by tactile output generator 167).

[0157] Compressor 127 receives waveforms (e.g., a combined waveform from mixer 125) as an input, and modifies the waveforms. In some embodiments, compressor 127 reduces the waveforms (e.g., in accordance with physical specifications of tactile output generators 167 (FIG. 1A) or 357 (FIG. 3)) so that tactile outputs corresponding to the waveforms are reduced. In some embodiments, compressor 127 limits the waveforms, such as by enforcing a predefined maximum amplitude for the waveforms. For example, compressor 127 reduces amplitudes of portions of waveforms that exceed a predefined amplitude threshold while maintaining amplitudes of portions of waveforms that do not exceed the predefined amplitude threshold. In some embodiments, compressor 127 reduces a dynamic range of the waveforms. In some embodiments, compressor 127 dynamically reduces the dynamic range of the waveforms so that the combined waveforms remain within performance specifications of the tactile output generator 167 (e.g., force and/or moveable mass displacement limits).

[0158] Low-pass filter 129 receives waveforms (e.g., compressed waveforms from compressor 127) as an input, and filters (e.g., smooths) the waveforms (e.g., removes or reduces high frequency signal components in the waveforms). For example, in some instances, compressor 127 includes, in compressed waveforms, extraneous signals (e.g., high frequency signal components) that interfere with the generation of tactile outputs and/or exceed performance specifications of tactile output generator 167 when the tactile outputs are generated in accordance with the compressed waveforms. Low-pass filter 129 reduces or removes such extraneous signals in the waveforms.

[0159] Thermal controller 131 receives waveforms (e.g., filtered waveforms from low-pass filter 129) as an input, and adjusts the waveforms in accordance with thermal conditions of device 100 (e.g., based on internal temperatures detected within device 100, such as the temperature of haptic feedback controller 161, and/or external temperatures detected by

device 100). For example, in some cases, the output of haptic feedback controller 161 varies depending on the temperature (e.g. haptic feedback controller 161, in response to receiving same waveforms, generates a first tactile output when haptic feedback controller 161 is at a first temperature and generates a second tactile output when haptic feedback controller 161 is at a second temperature that is distinct from the first temperature). For example, the magnitude (or the amplitude) of the tactile outputs can vary depending on the temperature. To reduce the effect of the temperature variations, the waveforms are modified (e.g., an amplitude of the waveforms is increased or decreased based on the temperature).

[0160] In some embodiments, haptic feedback module 133 (e.g., trigger module 121) is coupled to hardware input processing module 146. In some embodiments, other input controller(s) 160 in FIG. 1A includes hardware input processing module 146. In some embodiments, hardware input processing module 146 receives inputs from hardware input device 145 (e.g., other input or control devices 116 in FIG. 1A, such as a home button or an intensity-sensitive input surface, such as an intensity-sensitive touch screen). In some embodiments, hardware input device 145 is any input device described herein, such as touch-sensitive display system 112 (FIG. 1A), keyboard/mouse 350 (FIG. 3), touchpad 355 (FIG. 3), one of other input or control devices 116 (FIG. 1A), or an intensity-sensitive home button. In some embodiments, hardware input device 145 consists of an intensity-sensitive home button, and not touch-sensitive display system 112 (FIG. 1A), keyboard/mouse 350 (FIG. 3), or touchpad 355 (FIG. 3). In some embodiments, in response to inputs from hardware input device 145 (e.g., an intensity-sensitive home button or a touch screen), hardware input processing module 146 provides one or more trigger signals to haptic feedback module 133 to indicate that a user input satisfying predefined input criteria, such as an input corresponding to a "click" of a home button (e.g., a "down click" or an "up click"), has been detected. In some embodiments, haptic feedback module 133 provides waveforms that correspond to the "click" of a home button in response to the input corresponding to the "click" of a home button, simulating a haptic feedback of pressing a physical home button.

[0161] In some embodiments, the tactile output module includes haptic feedback controller 161 (e.g., haptic feedback controller 161 in FIG. 1A), which controls the generation of tactile outputs. In some embodiments, haptic feedback controller 161 is coupled to a plurality of tactile output generators, and selects one or more tactile output generators of the plurality of tactile output generators and sends waveforms to the selected one or more

tactile output generators for generating tactile outputs. In some embodiments, haptic feedback controller 161 coordinates tactile output requests that correspond to activation of hardware input device 145 and tactile output requests that correspond to software events (e.g., tactile output requests from haptic feedback module 133) and modifies one or more waveforms of the two or more waveforms to emphasize particular waveform(s) over the rest of the two or more waveforms (e.g., by increasing a scale of the particular waveform(s) and/or decreasing a scale of the rest of the waveforms, such as to prioritize tactile outputs that correspond to activations of hardware input device 145 over tactile outputs that correspond to software events).

[0162] In some embodiments, as shown in FIG. 1C, an output of haptic feedback controller 161 is coupled to audio circuitry of device 100 (e.g., audio circuitry 110, FIG. 1A), and provides audio signals to audio circuitry of device 100. In some embodiments, haptic feedback controller 161 provides both waveforms used for generating tactile outputs and audio signals used for providing audio outputs in conjunction with generation of the tactile outputs. In some embodiments, haptic feedback controller 161 modifies audio signals and/or waveforms (used for generating tactile outputs) so that the audio outputs and the tactile outputs are synchronized (e.g., by delaying the audio signals and/or waveforms). In some embodiments, haptic feedback controller 161 includes a digital-to-analog converter used for converting digital waveforms into analog signals, which are received by amplifier 163 and/or tactile output generator 167.

[0163] In some embodiments, the tactile output module includes amplifier 163. In some embodiments, amplifier 163 receives waveforms (e.g., from haptic feedback controller 161) and amplifies the waveforms prior to sending the amplified waveforms to tactile output generator 167 (e.g., any of tactile output generators 167 (FIG. 1A) or 357 (FIG. 3)). For example, amplifier 163 amplifies the received waveforms to signal levels that are in accordance with physical specifications of tactile output generator 167 (e.g., to a voltage and/or a current required by tactile output generator 167 for generating tactile outputs so that the signals sent to tactile output generator 167 produce tactile outputs that correspond to the waveforms received from haptic feedback controller 161) and sends the amplified waveforms to tactile output generator 167. In response, tactile output generator 167 generates tactile outputs (e.g., by shifting a moveable mass back and forth in one or more dimensions relative to a neutral position of the moveable mass).

[0164] In some embodiments, the tactile output module includes sensor 169, which is coupled to tactile output generator 167. Sensor 169 detects states or state changes (e.g., mechanical position, physical displacement, and/or movement) of tactile output generator 167 or one or more components of tactile output generator 167 (e.g., one or more moving parts, such as a membrane, used to generate tactile outputs). In some embodiments, sensor 169 is a magnetic field sensor (e.g., a Hall effect sensor) or other displacement and/or movement sensor. In some embodiments, sensor 169 provides information (e.g., a position, a displacement, and/or a movement of one or more parts in tactile output generator 167) to haptic feedback controller 161 and, in accordance with the information provided by sensor 169 about the state of tactile output generator 167, haptic feedback controller 161 adjusts the waveforms output from haptic feedback controller 161 (e.g., waveforms sent to tactile output generator 167, optionally via amplifier 163).

[0165] 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.

[0166] 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.

[0167] 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.

[0168] 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.

[0169] 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.

[0170] 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 programs (e.g., sets of instructions) need not be implemented as separate software programs, 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.

[0171] Attention is now directed towards embodiments of user interfaces that are, optionally, implemented on, for example, portable multifunction device 100.

[0172] 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.

[0173] 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.

[0174] 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.

[0175] 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.

[0176] 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.

[0177] 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.

[0178] 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.

[0179] 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.

[0180] 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 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.

[0181] 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.

[0182] 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 methods 800, 1000, 1200, and 1400 (FIGS. 8, 10, 12, and 14). 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.

[0183] 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.

[0184] 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).

[0185] 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.

[0186] FIG. 5C illustrates detecting a plurality of contacts 552A-552E on touch-sensitive display screen 504 with a plurality of intensity sensors 524A-524D. FIG. 5C additionally

includes intensity diagrams that show the current intensity measurements of the intensity sensors 524A-524D relative to units of intensity. In this example, the intensity measurements of intensity sensors 524A and 524D are each 9 units of intensity, and the intensity measurements of intensity sensors 524B and 524C are each 7 units of intensity. In some implementations, an aggregate intensity is the sum of the intensity measurements of the plurality of intensity sensors 524A-524D, which in this example is 32 intensity units. In some embodiments, each contact is assigned a respective intensity that is a portion of the aggregate intensity. FIG. 5D illustrates assigning the aggregate intensity to contacts 552A-552E based on their distance from the center of force 554. In this example, each of contacts 552A, 552B, and 552E are assigned an intensity of contact of 8 intensity units of the aggregate intensity, and each of contacts 552C and 552D are assigned an intensity of contact of 4 intensity units of the aggregate intensity. More generally, in some implementations, each contact j is assigned a respective intensity Ij that is a portion of the aggregate intensity, A, in accordance with a predefined mathematical function, $Ij = A \cdot (Dj/\Sigma Di)$, where Dj is the distance of the respective contact j to the center of force, and ΣDi is the sum of the distances of all the respective contacts (e.g., i=1 to last) to the center of force. The operations described with reference to FIGS. 5C-5D can be performed using an electronic device similar or identical to device 100, 300, or 500. In some embodiments, a characteristic intensity of a contact is based on one or more intensities of the contact. In some embodiments, the intensity sensors are used to determine a single characteristic intensity (e.g., a single characteristic intensity of a single contact). It should be noted that the intensity diagrams are not part of a displayed user interface, but are included in FIGS. 5C-5D to aid the reader.

[0187] In some embodiments, a portion of a gesture is identified for purposes of determining a characteristic intensity. For example, a touch-sensitive surface optionally receives a continuous swipe contact transitioning from a start location and reaching an end location, at which point the intensity of the contact increases. In this example, the characteristic intensity of the contact at the end location is, optionally, based on only a portion of the continuous swipe contact, and not the entire swipe contact (e.g., only the portion of the swipe contact at the end location). In some embodiments, a smoothing algorithm is, optionally, applied to the intensities of the swipe contact prior to determining the characteristic intensity of the contact. For example, the smoothing algorithm optionally includes one or more of: an unweighted sliding-average smoothing algorithm, a triangular smoothing algorithm, a median filter smoothing algorithm, and/or an exponential smoothing

algorithm. In some circumstances, these smoothing algorithms eliminate narrow spikes or dips in the intensities of the swipe contact for purposes of determining a characteristic intensity.

[0188] The intensity of a contact on the touch-sensitive surface is, optionally, characterized relative to one or more intensity thresholds, such as a contact-detection intensity threshold, a light press intensity threshold, a deep press intensity threshold, and/or one or more other intensity thresholds. In some embodiments, the light press intensity threshold corresponds to an intensity at which the device will perform operations typically associated with clicking a button of a physical mouse or a trackpad. In some embodiments, the deep press intensity threshold corresponds to an intensity at which the device will perform operations that are different from operations typically associated with clicking a button of a physical mouse or a trackpad. In some embodiments, when a contact is detected with a characteristic intensity below the light press intensity threshold (e.g., and above a nominal contact-detection intensity threshold below which the contact is no longer detected), the device will move a focus selector in accordance with movement of the contact on the touch-sensitive surface without performing an operation associated with the light press intensity threshold or the deep press intensity threshold. Generally, unless otherwise stated, these intensity thresholds are consistent between different sets of user interface figures.

[0189] An increase of characteristic intensity of the contact from an intensity below the light press intensity threshold to an intensity between the light press intensity threshold and the deep press intensity threshold is sometimes referred to as a "light press" input. An increase of characteristic intensity of the contact from an intensity below the deep press intensity threshold to an intensity above the deep press intensity threshold is sometimes referred to as a "deep press" input. An increase of characteristic intensity of the contact from an intensity below the contact-detection intensity threshold to an intensity between the contact-detection intensity threshold and the light press intensity threshold is sometimes referred to as detecting the contact on the touch-surface. A decrease of characteristic intensity of the contact from an intensity above the contact-detection intensity threshold to an intensity below the contact-detection intensity threshold is sometimes referred to as detecting liftoff of the contact from the touch-surface. In some embodiments, the contact-detection intensity threshold is zero. In some embodiments, the contact-detection intensity threshold is greater than zero.

[0190] In some embodiments described herein, one or more operations are performed in response to detecting a gesture that includes a respective press input or in response to detecting the respective press input performed with a respective contact (or a plurality of contacts), where the respective press input is detected based at least in part on detecting an increase in intensity of the contact (or plurality of contacts) above a press-input intensity threshold. In some embodiments, the respective operation is performed in response to detecting the increase in intensity of the respective contact above the press-input intensity threshold (e.g., a "down stroke" of the respective press input). In some embodiments, the press input includes an increase in intensity of the respective contact above the press-input intensity threshold and a subsequent decrease in intensity of the contact below the press-input intensity threshold, and the respective operation is performed in response to detecting the subsequent decrease in intensity of the respective contact below the press-input threshold (e.g., an "up stroke" of the respective press input).

[0191] FIGS. 5E-5H illustrate detection of a gesture that includes a press input that corresponds to an increase in intensity of a contact 562 from an intensity below a light press intensity threshold (e.g., "IT_L") in FIG. 5E, to an intensity above a deep press intensity threshold (e.g., "IT_D") in FIG. 5H. The gesture performed with contact 562 is detected on touch-sensitive surface 560 while cursor 576 is displayed over application icon 572B corresponding to App 2, on a displayed user interface 570 that includes application icons 572A-572D displayed in predefined region 574. In some embodiments, the gesture is detected on touch-sensitive display 504. The intensity sensors detect the intensity of contacts on touch-sensitive surface 560. The device determines that the intensity of contact 562 peaked above the deep press intensity threshold (e.g., "IT_D"). Contact 562 is maintained on touch-sensitive surface 560. In response to the detection of the gesture, and in accordance with contact 562 having an intensity that goes above the deep press intensity threshold (e.g., "IT_D") during the gesture, reduced-scale representations 578A-578C (e.g., thumbnails) of recently opened documents for App 2 are displayed, as shown in FIGS. 5F-5H. In some embodiments, the intensity, which is compared to the one or more intensity thresholds, is the characteristic intensity of a contact. It should be noted that the intensity diagram for contact 562 is not part of a displayed user interface, but is included in FIGS. 5E-5H to aid the reader.

[0192] In some embodiments, the display of representations 578A-578C includes an animation. For example, representation 578A is initially displayed in proximity of

application icon 572B, as shown in FIG. 5F. As the animation proceeds, representation 578A moves upward and representation 578B is displayed in proximity of application icon 572B, as shown in FIG. 5G. Then, representations 578A moves upward, 578B moves upward toward representation 578A, and representation 578C is displayed in proximity of application icon 572B, as shown in FIG. 5H. Representations 578A-578C form an array above icon 572B. In some embodiments, the animation progresses in accordance with an intensity of contact 562, as shown in FIGS. 5F-5G, where the representations 578A-578C appear and move upwards as the intensity of contact 562 increases toward the deep press intensity threshold (e.g., "IT_D"). In some embodiments, the intensity, on which the progress of the animation is based, is the characteristic intensity of the contact. The operations described with reference to FIGS. 5E-5H can be performed using an electronic device similar or identical to device 100, 300, or 500.

[0193] In some embodiments, the device employs intensity hysteresis to avoid accidental inputs sometimes termed "jitter," where the device defines or selects a hysteresis intensity threshold with a predefined relationship to the press-input intensity threshold (e.g., the hysteresis intensity threshold is X intensity units lower than the press-input intensity threshold or the hysteresis intensity threshold is 75%, 90%, or some reasonable proportion of the press-input intensity threshold). Thus, in some embodiments, the press input includes an increase in intensity of the respective contact above the press-input intensity threshold and a subsequent decrease in intensity of the contact below the hysteresis intensity threshold that corresponds to the press-input intensity threshold, and the respective operation is performed in response to detecting the subsequent decrease in intensity of the respective contact below the hysteresis intensity threshold (e.g., an "up stroke" of the respective press input). Similarly, in some embodiments, the press input is detected only when the device detects an increase in intensity of the contact from an intensity at or below the hysteresis intensity threshold to an intensity at or above the press-input intensity threshold and, optionally, a subsequent decrease in intensity of the contact to an intensity at or below the hysteresis intensity, and the respective operation is performed in response to detecting the press input (e.g., the increase in intensity of the contact or the decrease in intensity of the contact, depending on the circumstances).

[0194] For ease of explanation, the descriptions of operations performed in response to a press input associated with a press-input intensity threshold or in response to a gesture

including the press input are, optionally, triggered in response to detecting either: an increase in intensity of a contact above the press-input intensity threshold, an increase in intensity of a contact from an intensity below the hysteresis intensity threshold to an intensity above the press-input intensity threshold, a decrease in intensity of the contact below the press-input intensity threshold, and/or a decrease in intensity of the contact below the hysteresis intensity threshold corresponding to the press-input intensity threshold. Additionally, in examples where an operation is described as being performed in response to detecting a decrease in intensity of a contact below the press-input intensity threshold, the operation is, optionally, performed in response to detecting a decrease in intensity of the contact below a hysteresis intensity threshold corresponding to, and lower than, the press-input intensity threshold.

[0195] As used herein, an "installed application" refers to a software application that has been downloaded onto an electronic device (e.g., devices 100, 300, and/or 500) and is ready to be launched (e.g., become opened) on the device. In some embodiments, a downloaded application becomes an installed application by way of an installation program that extracts program portions from a downloaded package and integrates the extracted portions with the operating system of the computer system.

[0196] As used herein, the terms "open application" or "executing application" refer to a software application with retained state information (e.g., as part of device/global internal state 157 and/or application internal state 192). An open or executing application is, optionally, any one of the following types of applications:

- an active application, which is currently displayed on a display screen of the device that the application is being used on;
- a background application (or background processes), which is not currently displayed, but one or more processes for the application are being processed by one or more processors; and
- a suspended or hibernated application, which is not running, but has state information that is stored in memory (volatile and non-volatile, respectively) and that can be used to resume execution of the application.

[0197] As used herein, the term "closed application" refers to software applications without retained state information (e.g., state information for closed applications is not stored

in a memory of the device). Accordingly, closing an application includes stopping and/or removing application processes for the application and removing state information for the application from the memory of the device. Generally, opening a second application while in a first application does not close the first application. When the second application is displayed and the first application ceases to be displayed, the first application becomes a background application.

[0198] 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.

[0199] FIG. 6 illustrates exemplary devices connected via one or more communication channels to participate in a transaction in accordance with some embodiments. One or more exemplary electronic devices (e.g., devices 100, 300, and 500) are configured to optionally detect input (e.g., a particular user input, an NFC field) and optionally transmit payment information (e.g., using NFC). The one or more electronic devices optionally include NFC hardware and are configured to be NFC-enabled.

[0200] The electronic devices (e.g., devices 100, 300, and 500) are optionally configured to store payment account information associated with each of one or more payment accounts. Payment account information includes, for example, one or more of: a person's or company's name, a billing address, a login, a password, an account number, an expiration date, a security code, a telephone number, a bank associated with the payment account (e.g., an issuing bank), and a card network identifier. In some examples, payment account information includes include an image, such as a picture of a payment card (e.g., taken by the device and/or received at the device). In some examples, the electronic devices receive user input including at least some payment account information (e.g., receiving user-entered credit, debit, account, or gift card number and expiration date). In some examples, the electronic devices detect at least some payment account information from an image (e.g., of a payment card captured by a camera sensor of the device). In some examples, the electronic devices receive at least some payment account information from another device (e.g., another user device or a server). In some examples, the electronic device receives payment account information from a server associated with another service for which an account for a user or user device previously made a purchase or identified payment account data (e.g., an app for renting or selling audio and/or video files).

[0201] In some embodiments, a payment account is added to an electronic device (e.g., device 100, 300, and 500), such that payment account information is securely stored on the electronic device. In some examples, after a user initiates such process, the electronic device transmits information for the payment account to a transaction-coordination server, which then communicates with a server operated by a payment network for the account (e.g., a payment server) to ensure a validity of the information. The electronic device is optionally configured to receive a script from the server that allows the electronic device to program payment information for the account onto the secure element.

[0202] In some embodiments, communication among electronic devices 100, 300, and 500 facilitates transactions (e.g., generally or specific transactions). For example, a first electronic device (e.g., 100) can serve as a provisioning or managing device, and can send notifications of new or updated payment account data (e.g., information for a new account, updated information for an existing account, and/or an alert pertaining to an existing account) to a second electronic device (e.g., 500). In another example, a first electronic device (e.g., 100) can send data to a second election device, wherein the data reflects information about payment transactions facilitated at the first electronic device. The information optionally includes one or more of: a payment amount, an account used, a time of purchase, and whether a default account was changed. The second device (e.g., 500) optionally uses such information to update a default payment account (e.g., based on a learning algorithm or explicit user input).

[0203] Electronic devices (e.g., 100, 300, 500) are configured to communicate with each other over any of a variety of networks. For example, the devices communicate using a Bluetooth connection 608 (e.g., which includes a traditional Bluetooth connection or a Bluetooth Low Energy connection) or using a WiFi network 606. Communications among user devices are, optionally, conditioned to reduce the possibility of inappropriately sharing information across devices. For example, communications relating to payment information requires that the communicating devices be paired (e.g., be associated with each other via an explicit user interaction) or be associated with a same user account.

[0204] In some embodiments, an electronic device (e.g., 100, 300, 500) is used to communicate with a point-of-sale (POS) payment terminal 600, which is optionally NFC-enabled. The communication optionally occurs using a variety of communication channels and/or technologies. In some examples, electronic device (e.g., 100, 300, 500) communicates

with payment terminal 600 using an NFC channel 610. In some examples, payment terminal 600 communicates with an electronic device (e.g., 100, 300, 500) using a peer-to-peer NFC mode. Electronic device (e.g., 100, 300, 500) is optionally configured transmit a signal to payment terminal 600 that includes payment information for a payment account (e.g., a default account or an account selected for the particular transaction).

[0205] In some embodiments, proceeding with a transaction includes transmitting a signal that includes payment information for an account, such as a payment account. In some embodiments, proceeding with the transaction includes reconfiguring the electronic device (e.g., 100, 300, 500) to respond as a contactless payment card, such as an NFC-enabled contactless payment card, and then transmitting credentials of the account via NFC, such as to payment terminal 600. In some embodiments, subsequent to transmitting credentials of the account via NFC, the electronic device reconfigures to not respond as a contactless payment card (e.g., requiring authorization before again reconfigured to respond as a contactless payment card via NFC).

[0206] In some embodiments, generation of and/or transmission of the signal is controlled by a secure element in the electronic device (e.g., 100, 300, 500). The secure element optionally requires a particular user input prior to releasing payment information. For example, the secure element optionally requires detection that the electronic device is being worn, detection of a button press, detection of entry of a passcode, detection of a touch, detection of one or more option selections (e.g., received while interacting with an application), detection of a fingerprint signature, detection of a voice or voice command, and or detection of a gesture or movement (e.g., rotation or acceleration). In some examples, if a communication channel (e.g., an NFC communication channel) with another device (e.g., payment terminal 600) is established within a defined time period from detection of the input, the secure element releases payment information to be transmitted to the other device (e.g., payment terminal 600). In some examples, the secure element is a hardware component that controls release of secure information. In some examples, the secure element is a software component that controls release of secure information.

[0207] In some embodiments, protocols related to transaction participation depend on, for example, device types. For example, a condition for generating and/or transmitting payment information can be different for a wearable device (e.g., device 500) and a phone (e.g., device 100). For example, a generation and/or transmission condition for a wearable device includes

detecting that a button has been pressed (e.g., after a security verification), while a corresponding condition for a phone does not require button-depression and instead requires detection of particular interaction with an application. In some examples, a condition for transmitting and/or releasing payment information includes receiving particular input on each of multiple devices. For example, release of payment information optionally requires detection of a fingerprint and/or passcode at the device (e.g., device 100) and detection of a mechanical input (e.g., button press) on another device (e.g., device 500).

[0208] Payment terminal 600 optionally uses the payment information to generate a signal to transmit to a payment server 604 to determine whether the payment is authorized. Payment server 604 optionally includes any device or system configured to receive payment information associated with a payment account and to determine whether a proposed purchase is authorized. In some examples, payment server 604 includes a server of an issuing bank. Payment terminal 600 communicates with payment server 604 directly or indirectly via one or more other devices or systems (e.g., a server of an acquiring bank and/or a server of a card network).

[0209] Payment server 604 optionally uses at least some of the payment information to identify a user account from among a database of user accounts (e.g., 602). For example, each user account includes payment information. An account is, optionally, located by locating an account with particular payment information matching that from the POS communication. In some examples, a payment is denied when provided payment information is not consistent (e.g., an expiration date does not correspond to a credit, debit or gift card number) or when no account includes payment information matching that from the POS communication.

[0210] In some embodiments, data for the user account further identifies one or more restrictions (e.g., credit limits); current or previous balances; previous transaction dates, locations and/or amounts; account status (e.g., active or frozen), and/or authorization instructions. In some examples, the payment server (e.g., 604) uses such data to determine whether to authorize a payment. For example, a payment server denies a payment when a purchase amount added to a current balance would result in exceeding an account limit, when an account is frozen, when a previous transaction amount exceeds a threshold, or when a previous transaction count or frequency exceeds a threshold.

[0211] In some embodiments, payment server 604 responds to POS payment terminal 600 with an indication as to whether a proposed purchase is authorized or denied. In some examples, POS payment terminal 600 transmits a signal to the electronic device (e.g., 100, 300, 500) to identify the result. For example, POS payment terminal 600 sends a receipt to the electronic device (e.g., 100, 300, 500) when a purchase is authorized (e.g., via a transaction-coordination server that manages a transaction app on the user device). In some instances, POS payment terminal 600 presents an output (e.g., a visual or audio output) indicative of the result. Payment can be sent to a merchant as part of the authorization process or can be subsequently sent.

[0212] In some embodiments, the electronic device (e.g., 100, 300, 500) participates in a transaction that is completed without involvement of POS payment terminal 600. For example, upon detecting that a mechanical input has been received, a secure element in the electronic device (e.g., 100, 300, 500) releases payment information to allow an application on the electronic device to access the information (e.g., and to transmit the information to a server associated with the application).

[0213] In some embodiments, the electronic device (e.g., 100, 300, 500) is in a locked state or an unlocked state. In the locked state, the electronic device is powered on and operational but is prevented from performing a predefined set of operations in response to the user input. The predefined set of operations optionally includes navigation between user interfaces, activation or deactivation of a predefined set of functions, and activation or deactivation of certain applications. The locked state can be used to prevent unintentional or unauthorized use of some functionality of the electronic device or activation or deactivation of some functions on the electronic device. In the unlocked state, the electronic device 100 is power on and operational and is not prevented from performing at least a portion of the predefined set of operations that cannot be performed while in the locked state.

[0214] When the device is in the locked state, the device is said to be locked. In some embodiments, the device in the locked state optionally responds to a limited set of user inputs, including input that corresponds to an attempt to transition the device to the unlocked state or input that corresponds to powering the device off.

[0215] In some examples, a secure element (e.g., 115) is a hardware component (e.g., a secure microcontroller chip) configured to securely store data or an algorithm such that the

securely stored data is not accessible by the device without proper authentication information from a user of the device. Keeping the securely stored data in a secure element that is separate from other storage on the device prevents access to the securely stored data even if other storage locations on the device are compromised (e.g., by malicious code or other attempts to compromise information stored on the device). In some examples, the secure element provides (or releases) payment information (e.g., an account number and/or a transaction-specific dynamic security code). In some examples, the secure element provides (or releases) the payment information in response to the device receiving authorization, such as a user authentication (e.g., fingerprint authentication; passcode authentication; detecting double-press of a hardware button when the device is in an unlocked state, and optionally, while the device has been continuously on a user's wrist since the device was unlocked by providing authentication credentials to the device, where the continuous presence of the device on the user's wrist is determined by periodically checking that the device is in contact with the user's skin). For example, the device detects a fingerprint at a fingerprint sensor (e.g., a fingerprint sensor integrated into a button) of the device. The device determines whether the fingerprint is consistent with a registered fingerprint. In accordance with a determination that the fingerprint is consistent with the registered fingerprint, the secure element provides (or releases) payment information. In accordance with a determination that the fingerprint is not consistent with the registered fingerprint, the secure element forgoes providing (or releasing) payment information.

[0216] 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.

[0217] FIGS. 7A-7AD illustrate exemplary user interfaces for providing indications of error conditions during biometric authentication, in accordance with some examples. The user interfaces in these figures are used to illustrate the processes described below, including the processes in FIGS. 8A-8B.

[0218] FIG. 7A illustrates electronic device 700 (e.g., portable multifunction device 100, device 300, or device 500). In the exemplary example illustrated in FIGS. 7A-7AD, electronic device 700 is a smartphone. In other examples, electronic device 700 can be a different type of electronic device, such as a tablet (e.g., electronic device 900). Electronic device 700 includes display 702, one or more input devices (e.g., touchscreen of display 702,

button 704, and a microphone), a wireless communication radio, and biometric sensor 703. Electronic device 700 includes biometric sensor 703. In some examples, biometric sensor 703 includes one or more biometric sensors that can include a camera, such as a depth camera (e.g., an infrared camera), a thermographic camera, or a combination thereof. In some examples, biometric sensor 703 includes a biometric sensor (e.g., facial recognition sensor), such as those described in U.S. Ser. No. 14/341,860, "Overlapping Pattern Projector," filed July 14, 2014, U.S. Pub. No. 2016/0025993 and U.S. Ser. No. 13/810,451, "Scanning Projects and Image Capture Modules For 3D Mapping," U.S. Patent 9,098,931, which are hereby incorporated by reference in their entirety for any purpose. In some examples, biometric sensor 703 includes one or more fingerprint sensors (e.g., a fingerprint sensor integrated into a button). In some examples, electronic device 700 further includes a light-emitting device (e.g., light projector), such as an IR flood light, a structured light projector, or a combination thereof. The light-emitting device is, optionally, used to illuminate the biometric feature (e.g., the face) during capture of biometric data of biometric features by biometric sensor 703. In some examples, electronic device 700 includes a plurality of cameras separate from biometric sensor 703. In some examples, electronic device 700 includes only one camera separate from biometric sensor 703.

[0219] At FIG. 7A, a user learns from notification 708 that she has received a message from John Appleseed. The user wishes to view the restricted content of notification 708 (e.g., the message from John Appleseed), but is unable to do so, as electronic device 700 is currently in a locked state. Electronic device 700 displays a locked state user interface (UI) with lock icon 706, which provides an indication that electronic device 700 is in a locked state. Viewing the restricted content of notification 708 requires successful authentication (e.g., determining that information (or data) about a biometric feature obtained using biometric sensor 703 corresponds to (or matches) stored authorized credentials). To view the restricted content of notification 708, the user lifts (or raises) electronic device 700 (e.g., from a substantially horizontal orientation to the orientation of the device as depicted in the user's hand in FIG. 7A). Electronic device 700 detects the change in orientation of electronic device 700 and, in response, initiates biometric authentication. In some examples, after initiating biometric authentication, electronic device 700 determines that biometric authentication is successful. In some examples, upon determining that biometric authentication is successful, electronic device 700 transitions from a locked state to an unlocked state, and displays the restricted content of notification 708.

[0220] After initiating biometric authentication (e.g., prior to successful authentication), electronic device 700 determines whether a face is detected by biometric sensor 703. At FIG. 7B, upon determining that a face is detected, electronic device700 displays authentication glyph 710, which includes a plurality of rings that rotate spherically. Authentication glyph 710 provides an indication that biometric authentication is being performed. In some examples, electronic device 700 displays an animation of lock icon 706 morphing into authentication glyph 710. In some examples, upon determining that no face is detected using biometric sensor 703, electronic device 700 maintains a locked state, and does not display authentication glyph 710.

[0221] After detecting the presence of a face, electronic device 700 determines that authentication is unsuccessful due to failure to obtain sufficient information about the user's face using biometric sensor 703. Specifically, as depicted by FIG. 7B, biometric sensor 703 is positioned outside acceptable distance range 712 (e.g., above the maximum threshold range), resulting in a failure to obtain sufficient information about the user's face. Upon determining that biometric authentication is unsuccessful due to the user's face being outside acceptable distance range 712, electronic device 700 maintains the device in a locked state and does not display the restricted content of notification 708. In some examples, electronic device 700 maintains the device in a locked state and does not display the restricted content of notification 708 upon determining authentication is unsuccessful and that no error condition exists. In some examples, upon determining that authentication is unsuccessful (e.g., due to captured biometric information not matching an authorized biometric information profile (e.g., stored authorized credentials)) and that no error condition exists (e.g., no condition preventing capture of sufficient biometric information), electronic device 700 maintains a locked state and automatically retries biometric authentication. In some examples, while retrying biometric authentication, electronic device 700 continues to display authentication glyph 710 in FIG. 7B.

[0222] As depicted in FIGS. 7C-7G, upon determining that biometric authentication is unsuccessful due to the user's face being outside acceptable distance range 712, electronic device 700 displays an animation of authentication glyph 710 morphing into error indication 714A such that error indication 714A replaces the display of authentication glyph 710. At FIG. 7G, electronic device 700 displays error indication 714A, which prompts the user to take an action to correct the error condition underlying error indication 714A. Specifically,

error indication 714A prompts the user to move her face closer to biometric sensor 703. Error indication 714A also suggests to the user that the user's face is too far away from biometric sensor 703, which is the cause of error indication 714A. As long as the user's face is outside acceptable distance range 712, electronic device 700 will continue to determine that error indication 714A exists. Upon determining that error indication 714A still exists, electronic device 700 does not attempt retrying biometric authentication. It is noted that electronic device 700 displays error indication 714A at a position coinciding with the position of lock icon 706 in FIG. 7A. Further, electronic device 700 displays error indication 714A on a portion of display 702 that is adjacent to biometric sensor 703 to suggest to the user that error indication 714A is associated with (or corresponds to) biometric sensor 703.

[0223] As depicted in FIG. 7H, after being prompted to correct error indication 714A, the user moves her face closer to biometric sensor 703 such that the user's face is within acceptable distance range 712. At FIG. 7H, electronic device determines that error indication 714A no longer exists. Upon determining that error indication 714A no longer exists, electronic device 700 enables biometric authentication on the device and automatically retries biometric authentication using biometric sensor 703.

[0224] In response to automatically retrying biometric authentication, electronic device 700 displays error indication 714A with a shimmer effect (e.g., animating the error indication such that one or more portions of the error indication moves side to side so as produce an effect where the error indication appears to shine) to indicate that electronic device 700 is attempting to biometrically authenticate the user again. FIGS. 7H-7L depict an animation of error indication 714A with the shimmer effect. In some examples, instead of displaying error indication 714A with a shimmer effect, electronic device 700 displays (e.g., replaces display of error indication 714A with) authentication glyph 710 to indicate that electronic device 700 is attempting to biometrically authenticate the user again. Accordingly, in some examples, electronic device 700 displays an animation of authentication glyph 710 morphing into lock icon 706 instead of error indication 714A morphing into lock icon 706.

[0225] At FIG. 7L, after retrying biometric authentication, electronic device 700 successfully biometrically authenticates the user. In response to successful biometric authentication, electronic device 700 transitions the device from a locked state to an unlocked state. While transitioning from a locked state to an unlocked state, electronic device 700 displays an animation of error indication 714A morphing into lock icon 706, as depicted in

FIGS. 7L-7N. After displaying an animation of error indication 714A morphing into lock icon 706, electronic device 700 displays an animation of lock icon 706 transitioning to unlock icon 716, as depicted in FIGS. 7N-7O. Unlock icon 716 provides an indication that electronic device 700 is in an unlocked state. Additionally, as depicted in FIG. 7O, electronic device 700 displays the restricted content (e.g., "Hey, is our meeting still on?") of notification 708 in response to biometric authentication being successful.

[0226] At FIG. 7P, instead of determining that the user's face is outside acceptable distance range 712 as discussed above with respect to FIG. 7B, electronic device 700 determines that biometric authentication is not available on the device. Upon determining that biometric authentication is not available, electronic device 700 displays error indication 714B in FIG. 7P, which provides an indication that biometric authentication is not currently available on the device. Biometric authentication can be unavailable for a variety of reasons, including that biometric authentication has failed more than a predefined number of times (e.g., 5, 10, 15) since the last successful authentication.

[0227] Due to biometric authentication being unavailable, a user must use an alternative method to authenticate the user. For example, the user can authenticate by entering a passcode at electronic device 700. While displaying error indication 714B in FIG. 7P, electronic device 700 receives input 720 at error indication 714B.

[0228] At FIG. 7Q, in response to receiving input 720 at error indication 714B, electronic device 700 displays passcode entry UI 722A with a plurality of entry affordances for entering a passcode (or password).

[0229] In some examples, instead of determining that authentication is successful as a result of retrying biometric authentication, as discussed above with respect to FIGS. 7L-7O, electronic device 700 determines that authentication is unsuccessful. In some examples, upon determining that authentication is unsuccessful, electronic device 700 maintains a locked state, and displays an animation of lock icon 706 in FIG. 7R alternating between different positions to simulate a "shake" effect. The shake animation provides an indication to the user that biometric authentication has failed and that electronic device 700 remains in a locked state.

[0230] After determining that authentication is unsuccessful, a user can perform an action at electronic device 700 to trigger retrying biometric authentication. At FIG. 7S, a user triggers retrying biometric authentication by swiping up starting from a region near the bottom edge of display 702. Electronic device 700 receives input 724, and in response, retries biometric authentication. In some examples, after retrying biometric authentication, electronic device 700 determines that authentication is successful. In some examples, upon determining that authentication is successful as a result of retrying biometric authentication, electronic device 700 transitions from a locked state to an unlocked state.

[0231] At FIGS. 7S-7T, electronic device 700 determines that authentication is unsuccessful as a result of retrying biometric authentication, in response to input 724. Upon determining that authentication is unsuccessful as a result of retrying biometric authentication, electronic device 700 displays passcode entry UI 722B in FIG. 7T and/or maintains a locked state.

[0232] At FIG. 7U, electronic device 700 determines that authentication is successful as a result of retrying biometric authentication at passcode entry UI 722B. Upon determining that authentication is successful, electronic device transitions from a locked state to an unlocked state, as depicted in FIGS. 7U-7W. In some examples, at FIG. 7U, electronic device determines that authentication is not successful as a result of retrying biometric authentication at passcode entry UI 722B. In some examples, upon making this determination, electronic device maintains a locked state.

[0233] FIGS. 7X-7AD illustrate various error conditions that electronic device 700 can detect while attempting to biometrically authenticate a user. Instead of displaying error indication 714A as described above with respect to FIG. 7G, electronic device 700 can display any one of the error indications described below (e.g., error indication 714C-I). FIGS. 7X-7AD also depict electronic device 700 coaching a user (e.g., via error indication 714C-I) to take an action to correct the detected error condition so that electronic device 700 can retry biometrically authenticating the user.

[0234] At FIG. 7X, a user's face is positioned too close to biometric sensor 703. As a result, electronic device 700 determines that the user's face is positioned outside acceptable distance range 712 (e.g., below the minimum threshold range). Upon determining that the user's face is positioned outside acceptable distance range 712, electronic device 700 displays

error indication 714C, which prompts the user to move her face farther away from biometric sensor 703. Error indication 714C also provides an indication of the cause of the error condition (e.g., an indication that the user's face is too close to biometric sensor 703.)

[0235] At FIG. 7Y, a user's hand is covering biometric sensor 703. As a result, electronic device 700 determines that an object (e.g., a user's hand) is covering biometric sensor 703 such that the sensor is unable to obtain any information about the user's face. Upon determining that an object is covering biometric sensor 703, electronic device 700 displays error indication 714D, which prompts the user to move the user to move her hand away from biometric sensor 703. Error indication 714D also provides an indication of the cause of the error condition (e.g., an indication that biometric sensor 703 is covered).

[0236] At FIG. 7Z, a user is not looking at electronic device 700. As a result, electronic device 700 determines that the user's eyes are not looking at the device. Upon determining that the user's eyes are not looking at the device, electronic device 700 displays error indication 714E, which prompts the user to look at the device to correct the error condition. Error indication 714E also provides an indication of the cause of the error condition (e.g., an indication that the user is not looking at the device.

[0237] At FIG. 7AA, a user's face is within field of view 728, but the user is wearing a hat. As a result, electronic device 700 determines that a portion of the user's face is obscured (or occluded). For example, electronic device 700 obtains partial information about a user's face using biometric sensor 703, where the partial information is below the threshold amount needed for comparison with the stored authorized credentials. Upon determining that a portion of the user's face is obscured, electronic device 700 displays error indication 714F, which prompts the user to remove the hat. Error indication 714F also provides an indication of the cause of the error condition (e.g., an indication that a portion of the user's face is obscured).

[0238] At FIG. 7AB, a user's face is outside field of view 728 of biometric sensor 703. As a result, electronic device 700 determines that the user's face is outside field of view 728 of biometric sensor 703. In some examples, the user's face is outside field of view 728 when more than a threshold portion of the face is outside the field of view. In some examples, the user's face is outside field of view 728 when no face is detected within the field of view. Upon determining that the user's face is outside field of view 728, electronic device 700

displays error indication 714G, which prompts the user to move her face to within field of view 728. Error indication 714G also provides an indication of the cause of the error condition (e.g., an indication that the user's face is outside field of view 728).

[0239] At FIG. 7AC, a user's face is within field of view 728, but is turned away from biometric sensor 703. As a result, electronic device 700 determines that the user's face is turned away from biometric sensor 703. Upon determining that the user's face is turned away from biometric sensor 703, electronic device 700 displays error indication 714H, which prompts the user to turn her face towards the sensor. Error indication 714H also provides an indication of the cause of the error condition (e.g., an indication that the user's face is turned away from biometric sensor 703).

[0240] At FIG. 7AD, a user's face is positioned appropriately within the field of view and acceptable distance range of biometric sensor 703. However, the lighting conditions of the environment in which the user is located are not suitable for performing biometric authentication. Specifically, the amount of light is so great that it interferes with performing biometric authentication. As a result, electronic device 700 determines (e.g., via one or more ambient light sensors) that the amount of light exceeds a predefined threshold. Upon determining that the amount of light exceeds the threshold, electronic device 700 displays error indication 714I, which prompts the user to seek improved lighting conditions with a lower amount of light. Error indication 714I also provides an indication of the cause of the error condition (e.g., an indication that the light conditions are not suitable for performing biometric authentication).

[0241] FIGS. 8A-8B are flow diagrams illustrating a method for providing indications of error conditions during biometric authentication, in accordance with some examples. Method 800 is performed at an electronic device (e.g., 100, 300, 500, 700) with a display (e.g., 702) and one or more input devices (e.g., an accelerometer (e.g., 168), a touchscreen of a display (e.g., 702)). In some examples, the electronic device includes one or more biometric sensors (e.g., a fingerprint sensor, a contactless biometric sensor (e.g., a biometric sensor that does not require physical contact, such as a thermal or optical facial recognition sensor), an iris scanner). In some examples, the one or more biometric sensors include one or more cameras. Some operations in method 800 are, optionally, combined, the orders of some operations are, optionally, changed, and some operations are, optionally, omitted.

[0242] As described below, method 800 provides an intuitive way for providing indications of error conditions during biometric authentication. The method reduces the cognitive burden on a user for performing biometric authentication, thereby creating a more efficient human-machine interface. For battery-operated computing devices, enabling a user to perform biometric authentication faster and more efficiently conserves power and increases the time between battery charges.

[0243] The electronic device (e.g., 100, 300, 500, 700) receives (802), via the one or more input devices (e.g., an accelerometer (e.g., 168), a touchscreen of a display (e.g., 702)), a request to perform an operation that requires authentication (e.g., biometric authentication). In some examples, the request to perform an operation that requires authentication includes a request to unlock the device (e.g., a swipe at a predefined location). In some examples, the request is triggered by lifting the device from a substantially horizontal position.

[0244] In response (804) to the request to perform the operation that requires authentication (e.g., biometric authentication) and in accordance (806) with a determination that authentication (e.g., biometric authentication) is successful, the electronic device performs the operation. In some examples, authentication is successful when a user input (e.g., data obtained from one or more biometric sensors that correspond to a biometric feature (e.g., face, finger) of a user, passcode) corresponds to (e.g., matches) an authorized credential (e.g., an enrolled fingerprint, face, or passcode). In some examples, a user input corresponds to an authorized credential when the user input matches the authorized credential.

[0245] In response (804) to the request to perform the operation that requires authentication (e.g., biometric authentication) and in accordance (808) with a determination that authentication (e.g., biometric authentication) is not successful and that a set of error condition criteria is met (e.g., an error condition exists), the electronic device (e.g., 100, 300, 500, 700) displays (810), on the display (e.g., 702), an indication of an error condition (e.g., 714A-I) (e.g., of the set of error condition criteria) and forgoes (816) performing the operation. The indication includes (812) information about the cause of the error condition. In some examples, authentication is not successful when a user input (e.g., data obtained from one or more biometric sensors that correspond to a biometric feature (e.g., face, finger) of a user, passcode) does not correspond to (e.g., match) an authorized credential (e.g., an enrolled fingerprint, face, or passcode). In some examples, a user input does not correspond to an authorized credential when the user input does not match the authorized credential. In some

examples, the set of error condition criteria includes only one criterion. Displaying the indication of the error condition provides the user with feedback about the current state of the device (e.g., that an error condition is preventing successful biometric authentication) and prompts the user to take further action to correct the error condition. Providing improved feedback to the user enhances the operability of the device and makes the user-device interface more efficient (e.g., by helping the user to provide proper inputs and reducing user mistakes when operating/interacting with the device) which, additionally, reduces power usage and improves battery life of the device by enabling the user to use the device more quickly and efficiently. Moreover, forgoing performing the operation when biometric authentication has failed and an error condition is detected enhances security and reduces the instances of multiple resource-intensive re-attempts of biometric authentication that is likely to fail due to the error condition. Providing improved security enhances the operability of the device and makes the user-device interface more efficient (e.g., by restricting unauthorized access) which, additionally, reduces power usage and improves battery life of the device by limiting the performance of restricted operations.

[0246] In some examples, in response (804) to the request to perform the operation that requires authentication and in accordance (826) with a determination that authentication (e.g., biometric authentication) is not successful and that the set of error condition criteria is not met, the electronic device (e.g., 100, 300, 500, 700) forgoes (828) displaying, on the display (e.g., 702), the indication of the error condition and forgoes (830) performing the operation.

[0247] In some examples, the indication (e.g., 714A-I) of the error condition includes (814) an indication of a user action (e.g., visible indication (e.g., graphic or text)) that can be performed to correct the error condition (e.g., for a subsequent authentication attempt). In some examples, the indication of the user action indicates how to correct the error condition for a subsequent authentication attempt. Displaying an indication of a user action that can be performed to correct the error condition provides feedback to the user as to what course of action to take so that the user can be biometrically authenticated in a subsequent authentication attempt. Providing improved visual feedback to the user enhances the operability of the device and makes the user-device interface more efficient (e.g., by helping the user to provide proper inputs and reducing user mistakes when operating/interacting with the device) which, additionally, reduces power usage and improves battery life of the device

by enabling the user to use the device more quickly and efficiently. In some examples, no indicator is displayed during biometric authentication.

[0248] In some examples, the indication (e.g., 714A-I) of the error condition includes information (e.g., an indication of a user action and/or device condition, visible indication (e.g., graphic or text)) about a cause of the error condition. Displaying an indication of the cause of the error condition provides feedback to the user as to what course of action to take so that the user can be biometrically authenticated in a subsequent authentication attempt. Providing improved visual feedback to the user enhances the operability of the device and makes the user-device interface more efficient (e.g., by helping the user to provide proper inputs and reducing user mistakes when operating/interacting with the device) which, additionally, reduces power usage and improves battery life of the device by enabling the user to use the device more quickly and efficiently. In some examples, no indicator is displayed during biometric authentication.

[0249] In some examples, the set of error condition criteria includes a requirement that is met when a biometric feature (e.g., a fingerprint, a face) of a first type (e.g., a type that corresponds to authorized biometric features) is detected using one or more biometric sensors (e.g., 703) of the electronic device. In some examples, the indication of the error condition (e.g., 714A-I) is not displayed if a potentially valid biometric feature is not detected (e.g., signifying that a user is not currently engaging with the device). Forgoing displaying the indication of the error condition when no biometric feature is detected prevents potentially confusing the user, for it is likely that the user did not intend to perform biometric authentication if no biometric feature is detected. Thus, forgoing displaying the indication in this scenario makes the user-device interface more efficient (e.g., by helping the user to provide proper inputs and reducing user mistakes when operating/interacting with the device) which, additionally, reduces power usage and improves battery life of the device by enabling the user to use the device more quickly and efficiently.

[0250] In some examples, in accordance with a determination that authentication (e.g., biometric authentication) is successful, the electronic device (e.g., 100, 300, 500, 700) forgoes displaying, on the display (e.g., 702), the indication of the error condition (e.g., 714A-I).

[0251] In some examples, subsequent to displaying the indication of the error condition (e.g., 714A-I) and in accordance with a determination that the set of error condition criteria continues to be met, the electronic device (e.g., 100, 300, 500, 700) forgoes (818) attempting (and, optionally, disabling further attempts at) biometric authentication on the electronic device (e.g., biometric authentication functionality is not available on the device while the set of error conditions are met). In some examples, subsequent to displaying the indication of the error condition and in accordance with a determination that the set of error condition criteria is no longer met, the electronic device enables (822) retrying biometric authentication on the electronic device (e.g., the error condition is no longer present (e.g., has been corrected (e.g., due to the user taking an action to correct the error condition))). Automatically retrying biometric authentication when the set of error condition criteria is no longer met allows the user to quickly attempt to biometrically authenticate herself without requiring that the user explicitly request biometric authentication. Performing an optimized operation when a set of conditions has been met without requiring further user input enhances the operability of the device and makes the user-device interface more efficient (e.g., by helping the user to provide proper inputs and reducing user mistakes when operating/interacting with the device) which, additionally, reduces power usage and improves battery life of the device by enabling the user to use the device more quickly and efficiently.

[0252] In some examples, subsequent to displaying the indication of the error condition and in response to the determination that the set of error condition criteria is no longer met, the electronic device retries (824) authentication (e.g., biometric authentication) (e.g., automatically retrying authentication). In some examples, retrying authentication includes attempting to match biometric information obtained by one or more biometric sensors with authorized credentials (e.g., stored data that has been authorized for use in biometric authentication). In some examples, the determination that the error condition is not met occurs subsequent to (or in response to) receiving an input to correct the error condition. In some examples, retrying authentication occurs (or only occurs) in accordance with a determination that the error condition is not met due to detecting a user input that causes the error condition to not be met.

[0253] In some examples, subsequent to the determination that the set of error condition criteria is no longer met (e.g., detecting that the error condition has been corrected), the electronic device (e.g., 100, 300, 500, 700) receives, via the one or more input devices, an

input (e.g., 724, 726) corresponding to a request to retry authentication. In some examples, the input is a touch gesture input (e.g., tap, a swipe (e.g., an upward swipe)) or an activation of a hardware button (e.g., power button). In some examples, in response to receiving the input corresponding to the request to retry authentication, the electronic device retries authentication (e.g., biometric authentication) (e.g., automatically retrying authentication). In some examples, retrying authentication includes attempting to match biometric information obtained by one or more biometric sensors with authorized credentials (e.g., stored data that has been authorized for use in biometric authentication). In some examples, retrying authentication includes using one or more biometric sensors to obtain data of a biometric feature (e.g., face, fingerprint) of the user.

[0254] In some examples, displaying the indication of the error condition (e.g., 714A-I) includes an animation (e.g., shimmering) indicating that an attempt to authenticate is ongoing. In some examples, the attempt to authenticate includes attempting to detect biometric information using one or more biometric sensors. Displaying a shimmering animation indicating that an attempt to authenticate is ongoing provides feedback to the user as to the current state of the device and that no further action is required at this time. Providing improved visual feedback to the user enhances the operability of the device and makes the user-device interface more efficient (e.g., by helping the user to provide proper inputs and reducing user mistakes when operating/interacting with the device) which, additionally, reduces power usage and improves battery life of the device by enabling the user to use the device more quickly and efficiently. In some examples, no indicator is displayed during biometric authentication

[0255] In some examples, subsequent to (or in response to) receiving the request to perform the operation that requires authentication and prior to displaying the indication of the error condition (e.g., 714A-I), the electronic device (e.g., 100, 300, 500, 700) performs authentication. In some examples, while performing authentication, electronic device 700 displays, on the display (e.g., 702), a first indication (e.g., 710, 714A-I) (e.g., rings that rotate around a sphere, a user interface object that shimmers, where the user interface object includes the indication of the error condition) that the electronic device is using one or more biometric sensors (e.g., 703) of the electronic device to obtain information about a biometric feature. In some examples, displaying the indication of the error condition includes replacing the display of the first indication with the display of the indication of the error condition.

Displaying an indication that biometric authentication is occurring provides the user with feedback about the current state of the device (e.g., biometric authentication is being performed) and that the user does not need to take any action at this time. Providing improved feedback to the user enhances the operability of the device and makes the user-device interface more efficient (e.g., by helping the user to provide proper inputs and reducing user mistakes when operating/interacting with the device) which, additionally, reduces power usage and improves battery life of the device by enabling the user to use the device more quickly and efficiently.

[0256] In some examples, while performing the authentication, the electronic device (e.g., 100, 300, 500, 700) displays, on the display (e.g., 702), a first lock icon (e.g., 706) (e.g., an icon indicative of the locked state of the electronic device) and a first animation that transitions from the first lock icon to the first indication. In some examples, subsequent to displaying the indication of the error condition (e.g., and in accordance with a determination that authentication is successful) and subsequent to displaying the first animation, the electronic device displays, on the display (e.g., 702), a second animation that transitions from the indication of the error condition to an unlock icon (e.g., 716) (e.g., an icon indication of the locked state of the electronic device). In some examples, the first animation and the second animation show a morphing from one object to the next object. In some examples, the second animation includes displaying a first lock icon subsequent to the indication of the error condition and prior to the unlock icon.

[0257] In some examples, subsequent to displaying the indication of the error condition, the electronic device displays, on the display (e.g., 702), an animation that transitions from the indication of the error condition to a second lock icon (e.g., 706) or from a second indication (e.g., 710, 714A-I) (e.g., rings that rotate around a sphere) that the electronic device is using one or more biometric sensors of the electronic device to obtain information about a biometric feature to the second lock icon (e.g., an icon indicative of the locked state of the electronic device). In some examples, the second lock icon is the first lock icon. In some examples, the second indication is the first indication.

[0258] In some examples, while retrying authentication and subsequent to displaying the indication of the error condition and in accordance with a determination that the error condition is absent, the electronic device displays, on the display, a third indication (e.g., 710, 714A-I) (e.g., rings that rotate around a sphere, a user interface object that shimmers, where

the user interface object includes the indication of the error condition) that the electronic device is using one or more biometric sensors of the electronic device to obtain information about a biometric feature. In some examples, the third indication is the first indication.

[0259] In some examples, prior to displaying the indication of the error condition, the electronic device (e.g., 100, 300, 500, 700) displays, on the display (e.g., 702), a third lock icon (e.g., 706) at a location on the display (e.g., an icon indicative of the locked state of the electronic device). In some examples, the indication of the error condition (e.g., 714A-I) is displayed proximate to (e.g., near, adjacent to, at, within a predetermined distance of) the location on the display. In some examples, the third lock icon is the first lock icon and/or the second lock icon.

[0260] In some examples, when the electronic device is in a locked state while receiving the request to perform the operation that requires authentication and in accordance with the determination that authentication is successful, the electronic device (e.g., 100, 300, 500, 700) transitions from the locked state to an unlocked state. In some examples, the operation that requires authentication is transitioning the electronic device from a locked state to an unlocked state. In some examples, when the electronic device is in a locked state while receiving the request to perform the operation that requires authentication and in accordance with the determination that authentication is not successful, the electronic device maintains the locked state. Maintaining the device in the locked state when authentication is unsuccessful enhances device security by preventing fraudulent and/or unauthorized access to the device. Improving security measures of the device enhances the operability of the device by preventing unauthorized access to content and operations and, additionally, reduces power usage and improves battery life of the device by enabling the user to use the device more efficiently.

[0261] In some examples, when the electronic device is in a locked state while receiving the request to perform the operation that requires authentication and in accordance with the determination that authentication is not successful, the electronic device (e.g., 100, 300, 500, 700) maintains the locked state and retries authentication (e.g., biometric authentication) (e.g., automatically retrying authentication). In some examples, retrying authentication includes attempting to obtain information about a biometric feature (e.g., face, fingerprint) using one or more biometric sensors of the electronic device. In some examples, retrying authentication includes attempting to match biometric information obtained by one or more

biometric sensors with authorized credentials (e.g., stored data that has been authorized for use in biometric authentication). In some examples, after retrying authentication and in accordance with a determination that authentication resulting from retrying authentication is successful, the electronic device transitions from the locked state to an unlocked state. In some examples, after retrying authentication and in accordance with a determination that authentication resulting from retrying authentication is not successful, the electronic device maintains the locked state.

[0262] In some examples, subsequent to (or in response to) receiving the request to perform the operation that requires authentication, the electronic device (e.g., 100, 300, 500, 700) attempts authentication (e.g., biometric authentication). In some examples, while attempting authentication, the electronic device displays, on the display (e.g., 702), a third indication (e.g., 710, 714A-I) (e.g., rings that rotate around a sphere) that the electronic device is using one or more biometric sensors of the electronic device to obtain information about a biometric feature (e.g., face, fingerprint). In some examples, the indication is a scanning animation. In some examples, the third indication is the first indication and/or the second indication. In some examples, while retrying authentication, the electronic device maintains display of the third indication on the display (e.g., 702).

[0263] In some examples, in accordance with the determination that authentication resulting from retrying authentication is not successful, the electronic device displays, on the display (e.g., 702), an animation with a lock icon (e.g., 706) (e.g., an icon indicative of the locked state of the electronic device) alternating between a first position and a second position, the second position being different from the first position. In some examples, the animation with the lock icon is an animation of the lock icon shaking (e.g., side to side, rotating back and forth). In some examples, the electronic device displays an animation involving the lock icon to indicate that biometric authentication has failed. In some examples, a tactile output is provided in combination with the shaking lock icon. In some examples, no tactile output is provided. In some examples, in accordance with a determination that the biometric information captured using the one or more biometric sensors does not correspond to or does not match the authorization credentials, the electronic device (e.g., 100, 300, 500, 700) maintains the locked state of the electronic device. Displaying an animation of the lock icon shaking provides the user with feedback about the current state of the device (e.g., that biometric authentication has failed) and prompts the user

to take further action. Providing improved feedback to the user enhances the operability of the device and makes the user-device interface more efficient (e.g., by helping the user to provide proper inputs and reducing user mistakes when operating/interacting with the device) which, additionally, reduces power usage and improves battery life of the device by enabling the user to use the device more quickly and efficiently.

[0264] In some examples, the electronic device (e.g., 100, 300, 500, 700) includes a biometric sensor (e.g., 703) and the set of error condition criteria includes one or more of the following error condition criterions:

- A distance of the biometric feature from the biometric sensor exceeds a first predetermined threshold distance (e.g., the biometric feature (e.g., face) is too far from the biometric sensor) or exceeds the maximum of a distance range (e.g., 712). In some examples, exceeding the first predetermined threshold or the maximum of a distance range is highly correlated with degradation or reduced accuracy of the information about the biometric feature obtained by the biometric sensor). In some examples, the user can correct this error condition by moving the user's face closer to the biometric sensor.

- A distance of the biometric feature from the biometric sensor is below a second predetermined threshold distance (e.g., the biometric feature (e.g., face) is too close to the biometric sensor) or falls below the minimum of a distance range (e.g., 712). In some examples, falling below the second predetermined threshold or the minimum of a distance range is highly correlated with degradation or reduced accuracy of the information about the biometric feature obtained by the biometric sensor. In some examples, the user can correct this error condition by moving the user's face farther away from the biometric sensor.

- The biometric sensor (e.g., 703) is occluded (e.g., partially occluded, fully occluded, occluded to a degree sufficient to inhibit operation of the sensor) (e.g., occluded by a portion of the user (e.g., a hand), while interacting with the electronic device). In some examples, the user can correct this error condition by moving the user's hand away from the biometric sensor.

- A sub-portion of a detected biometric feature (e.g., eyes of a detected face) is not oriented towards the biometric sensor (e.g., one or more eyes are not focused on the electronic device (e.g., biometric sensor)). In some examples, the user can correct this error condition by opening the user's eyes or looking at the electronic device (e.g., biometric sensor).

- At least a portion of the detected biometric feature is occluded (e.g., partially occluded, fully occluded, occluded to a degree sufficient to result in incomplete information about the biometric feature). In some examples, the user can correct this error condition by removing the accessory (e.g., sunglasses) or article of clothing (e.g., scarf, hat) that is blocking the user's face.

- No biometric feature is detected within a field of view (e.g., 728) of the biometric sensor.

- A pose (e.g., an orientation with respect to the biometric sensor) of the detected biometric feature exceeds a threshold range (e.g., the biometric feature (e.g., face) is turned away from the biometric sensor). In some examples, exceeding the threshold range is highly correlated with degradation or reduced accuracy of the information about the biometric feature obtained by the biometric sensor. In some examples, the user can correct this error condition by turning the user's face toward the electronic device (e.g., biometric sensor).

- The electronic device detects (e.g., via one or more ambient light sensors) an amount of light (e.g., ambient light) that exceeds a predetermined light threshold (e.g., exceeding the predetermined light threshold is highly correlated with degradation or reduced accuracy of the information about the biometric feature obtained by the biometric sensor). In some examples, the user can correct this error condition by turning the user's back towards the sun so as to reduce the amount of light detected by the electronic device or move to a new location that has less ambient light (e.g., indoors).

[0265] In some examples, the set of error condition criteria can be a first subset of the error conditions listed above. For example, the first subset can include one or more error condition criterion selected from the group consisting of: the distance of the biometric feature

exceeds a first predetermined threshold distance, the distance of the biometric feature is below a second predetermined threshold distance, the biometric feature is out of the field of view of the biometric sensor, and the pose of the biometric feature exceeds a threshold range. The first subset is focused on guiding the user to correct error conditions involving the positioning and/or orientation of the face. As a further example, a second subset can include one or more error condition criterion selected from the group consisting of: the biometric sensor is occluded, and no biometric feature is detected within a field of view of the biometric sensor. The second subset is focused on guiding the user to correct error conditions where the biometric sensor is unable to obtain any information about the biometric feature of the user. For another example, a third subset can include one or more error condition criterion selected from the group consisting of: the pose of the detected biometric feature exceeds a threshold range and the biometric sensor is occluded. The third subset is focused on the error conditions that are likely to occur for devices of a certain form factor/size (e.g., a tablet device (e.g., iPad)).

[0266] In some examples, the electronic device (e.g., 100, 300, 500, 700) includes a biometric sensor (e.g., 703) at a portion (e.g., a location) of the electronic device (e.g., a portion that is not on the display). In some examples, in response to the request to perform the operation that requires authentication, the electronic device displays, on the display (e.g., 702), a progress indicator (e.g., 714A-I) proximate to (e.g., adjacent to, near, within a predetermined distance of) the portion of the electronic device, the progress indicator including the indication of the error condition. Displaying the progress indicator near the biometric sensor provides the user with feedback as to the association of the biometric sensor with the processes occurring at the device (e.g., attempted authentication). Specifically, the user becomes aware of the biometric sensor during biometric authentication such that the user is less likely to perform an action that interferes with the biometric sensor or alternatively, the user is prompted to take corrective action. Providing improved feedback to the user enhances the operability of the device and makes the user-device interface more efficient (e.g., by helping the user to provide proper inputs and reducing user mistakes when operating/interacting with the device) which, additionally, reduces power usage and improves battery life of the device by enabling the user to use the device more quickly and efficiently.

[0267] In some examples, the indication of the error condition (e.g., 714B) includes an indication that biometric authentication is currently not enabled on the electronic device in

accordance with a determination that biometric authentication is currently not enabled on the electronic device. In some examples, biometric authentication can become unavailable (or not enabled on the electronic device) when one or more of the following conditions have been met: the electronic device has not been successfully authenticated since being turned on or restarted; the electronic device has not been unlocked for more than a predetermined amount of time (e.g., 48 hours); the passcode has not been used to unlock the device for more than a predetermined amount of time (e.g., 156 hours); biometric authentication using a biometric feature (e.g., face, fingerprint) has not been used to unlock device for more than predetermined amount of time (e.g., 4 hours); the electronic device has received a remote lock command; biometric authentication has failed more than a predetermined number of times (e.g., 5, 10, 15) since the last successful authentication with the device; the electronic device has received a power off and/or emergency SOS command, and an explicit request by the user to disable biometric authentication has been detected. Displaying an indication that biometric authentication is currently not enabled provides feedback to the user of the current state of the device and prompts the user to pursue an alternative method to authenticate herself. Providing improved feedback to the user enhances the operability of the device and makes the user-device interface more efficient (e.g., by helping the user to provide proper inputs and reducing user mistakes when operating/interacting with the device) which, additionally, reduces power usage and improves battery life of the device by enabling the user to use the device more quickly and efficiently.

[0268] In some examples, the indication that biometric authentication is currently not enabled includes an affordance (e.g., 714B) (e.g., the indication is an affordance). In some examples, the electronic device (e.g., 100, 300, 500, 700) receives an input (e.g., 720) corresponding to the affordance and in response to receiving the input corresponding to the affordance, the electronic device (e.g., 100, 300, 500, 700) displays, on the display (e.g., 702), a credential entry user interface (e.g., 722A) with a plurality of character entry keys. In some examples, the credential entry user interface includes a virtual keypad or virtual keyboard. In some examples, the virtual keypad or virtual keyboard includes a plurality of character entry keys.

[0269] In some examples, the electronic device (e.g., 100, 300, 500, 700) detects a condition that triggers attempting authentication (e.g., biometric authentication). In some examples, the request to perform an operation that requires authentication includes a request

to unlock the device (e.g., a swipe at a predefined location). In some examples, in response to detecting the condition that triggers attempting authentication (e.g., biometric authentication) and in accordance with a determination that the condition corresponds to an alert (e.g., 708) generated by the device without user input directed to the device (e.g., based on the satisfaction of criteria other than detection of user input) while a biometric feature is available for detection by the one or more biometric sensors (e.g., a face is detected in the field of view of one or more face detection sensors such as a depth camera), the electronic device displays a fifth indication (e.g., 710) (e.g., rings that rotate around a sphere) that the electronic device is using the one or more biometric sensors of the electronic device to obtain information about a biometric feature. In some examples, in accordance with a determination that the condition corresponds to an alert generated by the device without user input directed to the device (e.g., based on the satisfaction of criteria other than detection of user input) while a biometric feature is not available for detection by the one or more biometric sensors (e.g., no face is detected in the field of view of one or more face detection sensors such as a depth camera), the electronic device forgoes displaying the fifth indication (e.g., rings that rotate around a sphere) that the electronic device is using the one or more biometric sensors of the electronic device to obtain information about a biometric feature. In some examples, in accordance with a determination that the condition corresponds to a user input directed to the device (e.g., a request that is not associated with a notification; a request that is a touch gesture input (e.g., tap, a swipe (e.g., 724) (e.g., an upward swipe) or an activation of a hardware button (e.g., power button) or sensor data indicative of movement (e.g., lifting) of the device)), the electronic device displays the fifth indication that the electronic device is using one or more biometric sensors of the electronic device to obtain information about a biometric feature (e.g., without regard to whether or not the biometric feature is available for detection by the one or more biometric sensors). Forgoing displaying the indication when no face is detected prevents potentially confusing the user, for it is likely that the user does not intend to initiate biometric authentication if no biometric feature is detected. Thus, forgoing displaying the indication in this scenario makes the user-device interface more efficient (e.g., by helping the user to provide proper inputs and reducing user mistakes when operating/interacting with the device) which, additionally, reduces power usage and improves battery life of the device by enabling the user to use the device more quickly and efficiently.

[0270] Note that details of the processes described above with respect to method 800 (e.g., FIGS. 8A-8B) are also applicable in an analogous manner to the methods described

below. For example, method 1000, method 1200, and/or method 1400 optionally include one or more of the characteristics of the various methods described above with reference to method 800. For example, the error indications (e.g., 714A-I) as described with respect to method 800 can be used to provide indications of error conditions during biometric authentication that is performed in processes described with respect to method 1000, method 1200, and method 1400. For brevity, these details are not repeated below.

[0271] FIGS. 9A-9U illustrate exemplary user interfaces for providing indications about the biometric sensor during biometric authentication, in accordance with some examples. The user interfaces in these figures are used to illustrate the processes described below, including the processes in FIGS. 10A-10C.

[0272] FIG. 9A illustrates electronic device 900 (e.g., portable multifunction device 100, device 300, device 500). In the exemplary examples illustrated in FIGS. 9A-9U, electronic device 900 is a tablet computer. In other examples, electronic device 900 can be a different type of electronic device, such as a smartphone (e.g., electronic device 700). Electronic device 900 includes display 902, one or more input devices (e.g., touchscreen of display 902, button 904, and a microphone), a wireless communication radio, and biometric sensor 903. Electronic device 900 includes biometric sensor 903. In some examples, biometric sensor 903 includes one or more biometric sensors that can include a camera, such as an infrared camera, a thermographic camera, or a combination thereof. In some examples, biometric sensor 903 includes some or all of the features of biometric sensor 703. In some examples, biometric sensor 903 includes one or more fingerprint sensors (e.g., a fingerprint sensor integrated into a button). In some examples, electronic device 900 further includes a light-emitting device (e.g., light projector), such as an IR flood light, a structured light projector, or a combination thereof. The light-emitting device is, optionally, used to illuminate the biometric feature (e.g., the face) during capture of biometric data of biometric features by biometric sensor 903. In some examples, electronic device 900 includes a plurality of cameras separate from biometric sensor 903. In some examples, electronic device 900 includes only one camera separate from biometric sensor 903.

[0273] At FIG. 9A, a user wishes to purchase goods using payment information stored on electronic device 900. As depicted in FIG. 9A, electronic device 900 is in a split screen (e.g., multitasking) mode. While in the split screen mode, electronic device 900 concurrently displays app store user interface (UI) 906 in left region 907 of display 902 and browser UI

908 in right region 909 of display 902. While concurrently displaying app store UI 906 and browser UI 908, electronic device 900 receives input 910 at purchase affordance 912.

[0274] At FIG. 9B, in response to receiving input 910 at purchase affordance 912, electronic device 900 swaps the applications being displayed in left region 907 and right region 909 of display 902. Specifically, electronic device 900 displays browser UI 908 in left region 907, and displays app store UI 906 in right region 909. Electronic device 900 swaps the applications in order to place the application associated with the goods being purchased in the region that is closer to biometric sensor 903. By placing browser UI 908 in left region 907, electronic device 900 provides an indication to the user of the location of biometric sensor 903, which is used to authenticate the user prior to authorizing payment for purchasing the goods. As shown in FIG. 9B, swapping the applications also places the application associated with the goods being purchased in the region that is closer to button 904. In some examples, when the button 904 and the biometric sensor 903 are not in close proximity (e.g., on the same side), electronic device 900 swaps applications, when necessary, to place the application associated with the goods being purchased in the region that is closer to the biometric sensor 903. In some examples, when button 904 and biometric sensor 903 are not in close proximity (e.g., on the same side), electronic device 900 swaps applications, when necessary, to place the application associated with the goods being purchased in the region that is closer to the button 904.

[0275] Additionally, as depicted in FIG. 9B, in response to receiving input 910 at purchase affordance 912, electronic device 900 darkens browser UI 908 while darkening app store UI 906 to a greater degree than that of browser UI 908. By darkening browser UI 908 less than app store UI 906, electronic device 900 indicates to the user which application is associated with pay sheet interface 914 and the goods the user wishes to purchase.

[0276] Moreover, in response to receiving input 910 at purchase affordance 912, electronic device 900 concurrently displays pay sheet interface 914 with information about the goods being purchased and prompt 916 to prompt the user to double-click button 904 to initiate a process for authorizing payment for the goods. Further in response to receiving input 910 at purchase affordance 912, electronic device 900 displays dynamic indication 918 to emphasize the location of button 904. While displaying pay sheet interface 914, electronic device receives input 920 at button 904 (e.g., double-press of button 904). Prompt 916 instructs the user to provide one or more activations of button 904 (e.g., a double press of

button 904). In some examples, prompt 916 is emphasized relative to one or more other displayed objects (on pay sheet interface 914). In some examples, dynamic indication 918 emphasizes the location of button 904 on the device by continuously changing in size (e.g., continuously alternating between becoming wider and becoming narrower, or otherwise continuously changing in size) adjacent to the location of button 904 on the display, thereby allowing the user to more easily locate the button corresponding to the request of prompt 916. In some examples, pay sheet interface 914 includes the name of the application to which it corresponds (e.g., the name of the application from which the user initiated the process for authorizing payment).

[0277] At FIG. 9C, in response to receiving input 920 at button 904, electronic device 900 initiates a process for authorizing payment for the goods. Authorizing payment for the goods requires successfully authenticating the user. As a result, in response to receiving input 920, electronic device 900 initiates biometric authentication using biometric sensor 903. After initiating biometric authentication, electronic device 900 displays face glyph 922, which provides an indication that electronic device 900 is attempting to biometrically authenticate the user (e.g., attempting to obtain biometric information about the user using biometric sensor 903). In some examples, face glyph 922 includes a simulation of a representation of a biometric feature. In some examples, in response to receiving input 920 at button 904, electronic device displays an animation of face glyph 922 moving from the location of prompt 916 to the location of face glyph 922, as depicted in FIG. 9C. In some examples, the animation is such that face glyph 922 appears to slide out of prompt 916.

[0278] At FIG. 9D, after displaying face glyph 922, electronic device transitions to displaying authentication glyph 924, which provides an indication that electronic device 900 is attempting to biometrically authenticate the user (e.g., continuing to try to obtain biometric information, attempting to match obtained information with stored authorized credentials). Authentication glyph 924 includes a plurality of rings that rotate spherically. In some examples, authentication glyph 924 provides an indication that biometric data is being processed (e.g., compared against stored authorized credentials).

[0279] While displaying authentication glyph 924, electronic device 900 detects that an error condition exists (e.g., a condition that prevents biometric sensor 903 from obtaining sufficient information about the user's face). Specifically, electronic device 900 detects that biometric sensor 903 is covered by a physical object (e.g., the user's hand)). In some

examples, electronic device 900 does not detect an error condition, and is able to obtain sufficient information about the user's face. In some examples, after obtaining sufficient information about the user's face and while displaying authentication glyph 924, electronic device 900 determines whether the obtained information satisfies biometric authentication criteria (e.g., determines whether the obtained biometric information matches, within a threshold, a biometric template associated with the user (e.g., stored authorized credentials)). In some examples, upon determining that biometric authentication is successful (e.g., biometric authentication criteria is satisfied), electronic device 900 transitions to an unlocked state.

[0280] At FIG. 9E, in response to detecting that an error condition exists, electronic device 900 displays error indication 926 at a location at the top of display 902 (e.g., with respect to the ground, with respect to the user). Error indication 926 provides an indication of the error condition that currently exists. Further in response to detecting that an error conditions exists, electronic device 900 displays error icon 928 at a location of display 902 that is adjacent to biometric sensor 903, thereby providing an indication of the location of biometric sensor 903. By providing an indication of the location of biometric sensor 903, error icon 928 suggests to the user the cause of the error condition. In some examples, in response to detecting that an error condition exists, electronic device 900 displays error indication 926 at a location adjacent to biometric sensor 903. In some examples, error indication 926 includes some or all of the features of error indication 714A, including a shimmer effect.

[0281] At FIG. 9F, further in response to detecting that an error condition exists, electronic device 900 displays an animation of pay sheet interface 914 moving from its initial location in FIG. 9E to the location in FIG. 9F, which is closer to biometric sensor 903. By moving pay sheet interface towards biometric sensor 903, electronic device 900 indicates to the user the existence of error icon 928 in addition to indicating the location of biometric sensor 903 (and thus suggesting to the user the cause of the error condition).

[0282] In some examples, error icon 928 is displayed at different location of display 902 depending on the positioning of the user's hand on display 902. As illustrated in FIG. 9F, the user's hand is covering a portion of display 902 that is adjacent to biometric sensor 903. While the user's hand is in contact with display 902, electronic device 900 detects an input as a result of the contact from the user's hand. In response to detecting this input, electronic

device 900 displays error icon 928 at a location at which the input is not detected. As another example, in FIG. 9G, the user's hand is covering less of display 902 than the user's hand in FIG. 9F. In some examples, in response to detecting the input of the user's hand in FIG. 9G, electronic device 900 displays error icon 928 at a location that is different from the location in FIG. 9F, where the location in FIG. 9G is closer to biometric sensor 903 than that of FIG. 9F. As yet another example, in FIG. 9H, the user's hand is covering a large portion of the upper-left side of display 902. In some examples, in response to detecting the input of the user's hand in FIG. 9H, electronic device 900 displays error icon 928 at a location that is different from the locations in FIGS. 9F-9G. Specifically, in some examples, electronic device 900 displays error icon 928 at a location that is close to (or substantially near) biometric sensor 903 without being at a location where the input of the user's hand is detected.

[0283] At FIG. 9I, the user removes her hand such that it no longer covers biometric sensor 903. While displaying error indication 926 and error icon 928, electronic device 900 detects that the error condition no longer exists.

[0284] At FIG. 9J, in response to detecting that the error condition no longer exists, electronic device 900 automatically retries biometric authentication. While retrying biometric authentication, electronic device 900 displays authentication glyph 924. While displaying authentication glyph 924, electronic device 900 attempts to biometrically authenticate the user. Specifically, electronic device 900 obtains information about the user's face using biometric sensor 903, and determines whether biometric authentication is successful (e.g., the obtained information matches stored authorized credentials).

[0285] While retrying biometric authentication, electronic device 900 determines that biometric authentication is successful. At FIG. 9K, upon determining biometric authentication is successful, electronic device 900 displays success glyph 930, which provides an indication that biometric authentication was successful. In some examples, success glyph 930 replaces authentication glyph 924.

[0286] At FIG. 9L, further in response to determining that biometric authentication is successful, electronic device 900 displays processing indicator 932, which provides an indication that the payment transaction is being processed (e.g., electronic device 900 is transmitting payment information (e.g., credentials) to an external device (e.g., server) to

authorize payment). In some examples, processing indicator 932 has a similar or identical pattern to authentication glyph 924.

[0287] At FIG. 9M, upon receiving an indication that payment has been completed (e.g., authorized), electronic device 900 displays completed indication 934, which provides an indication that payment has been completed. Completed indication 934 includes a checkmark to indicate completion.

[0288] FIGS. 9N-9S illustrate a technique for displaying error indication 926 and error icon 928 when error indication 926 and error icon 928 are to be displayed in approximately the same location. At FIG. 9N, a user wishes to unlock the device to access restricted content (e.g., a home screen, a most recently used application). FIG. 9N depicts electronic device 900 in a portrait orientation with respect to the ground, where a user is covering biometric sensor 903 with her hand. Additionally, electronic device 900 displays locked state UI 936 with lock icon 938. Lock icon 938 provides an indication that electronic device 900 is in a locked state.

[0289] While displaying locked state UI 936, electronic device 900 receives a request to unlock the device. For example, electronic device 900 detects the user lifting the device from a substantially horizontal position.

[0290] At FIG. 9O, in response to receiving the request to unlock the device, electronic device 900 attempts to biometrically authenticate the user. While attempting to biometrically authenticate the user, electronic device 900 displays authentication glyph 924. Additionally, while attempting to biometrically authenticate the user, electronic device 900 detects that an error condition exists (e.g., a condition that prevents biometric sensor 903 from obtaining sufficient information about the user's face). Specifically, electronic device 900 detects that biometric sensor 903 is covered by a physical object (e.g., the user's hand)).

[0291] At FIG. 9P, in response to detecting that an error condition exists, electronic device 900 displays error icon 928 at a location of display 902 that is near biometric sensor 903 (e.g., at the top of display 902). Further in response to detecting that an error condition exists, electronic device 900 determines that error indication 926 is to be displayed at approximately the same location as error icon 928. Upon determining that error indication 926 is to be displayed at approximately the same location, electronic device 900 does not

immediately display error indication 926, and instead displays error indication 926 as part of an animation that transitions from error icon 928 to error indication 926 to lock icon 938, as described below with respect to FIGS. 9Q-9R.

[0292] At FIG. 9Q, after displaying error icon 928, electronic device 900 displays (e.g., replaces display of error icon 928 with) error indication 926, which as discussed above, provides an indication of the cause of the error condition.

[0293] While displaying error indication 926, the user removes her hand from biometric sensor 903 such that it no longer covers biometric sensor 903. In response to detecting that the error condition no longer exists, electronic device 900 automatically retries biometric authentication.

[0294] At FIGS. 9R-9S, upon determining that authentication is successful as a result of retrying biometric authentication, electronic device 900 transitions from a locked state to an unlocked state. Specifically, electronic device 900 displays (e.g., replaces display of error indication 926 with) an animation of lock icon 938 transitioning to unlock icon 940, which provides an indication to the user that electronic device 900 has transitioned to an unlocked state. In some examples, instead of successful biometric authentication, electronic device 900 determines that authentication is unsuccessful as a result of retrying biometric authentication. In some examples, upon determining that authentication is unsuccessful, electronic device 900 displays a passcode entry UI with an affordance which, when activated, triggers retrying biometric authentication. In some examples, while retrying biometric authentication, electronic device 900 darkens all portions of display 902 except for the user interface associated with retrying biometric authentication.

[0295] FIG. 9T illustrates a technique for displaying error icon 928 when error icon 928 is to be displayed at approximately the same location as one of the notifications being displayed (e.g., 944A-D). In some examples, a user wishes to view the restricted content of one or more of the notifications (e.g., 944A-D) that are displayed while electronic device 900 is in a locked state. As depicted in FIG. 9T, a user is covering biometric sensor 903 with her hand when the electronic device is a portrait orientation, where biometric sensor 903 is located near the bottom of the device. In some examples, while attempting to biometrically authenticate a user to access the restricted content of the notifications, electronic device 900 detects that an error condition exists as a result of the user covering biometric sensor 903 with

her hand. In response to detecting that an error condition exists, electronic device 900 determines that error icon 928 is to be displayed at approximately the same location as one of the notifications (e.g., 944A-D). Upon making this determination and in response to detecting that the error condition exists, electronic device 900 displays UI element 942 (e.g., a background) concurrently with error icon 928 to provide a background on which to overlay the display of error icon 928. As depicted in FIG. 9T, UI element 942 is opaque such that the notification on which error icon 928 is overlaid (e.g., 944D) is not visible to the user. In some examples, UI element 942 is transparent such that the notification on which error icon 928 is overlaid is visible to the user.

[0296] FIG. 9T also illustrates a technique for hiding unlock indication 905 of FIG. 9U when error icon 928 is to be displayed at approximately the same location as unlock indication 905. In some examples, electronic device 900 displays unlock indication 905, which provides an indication of an approximate location on display 902 from which a user can start an upward swipe to initiate biometric authentication. In some examples, while displaying unlock indication 905, electronic device 900 detects that an error condition exists as a result of the user covering biometric sensor 903 with her hand. In some examples, in response to detecting that an error condition exists, electronic device 900 determines that error icon 928 is to be displayed at approximately the same location as unlock indication 905. In some examples, upon making this determination and in response to detecting that the error condition exists, electronic device 900 ceases to display unlock indication 905, and displays error icon 928 at approximately the same location at which unlock indication 905 was displayed.

[0297] While displaying error icon 928, electronic device 900 detects that the error condition no longer exists (e.g., due to the user removing her hand from biometric sensor 903). As depicted in FIG. 9U, the user has removed her hand from biometric sensor 903. At FIG. 9U, upon detecting that the error condition no longer exists, electronic device 900 ceases to display error icon 928, and re-displays unlock indication 905 at the location at which it was previously displayed.

[0298] FIGS. 10A-10C are flow diagrams illustrating a method for providing indications about the biometric sensor during biometric authentication, in accordance with some examples. Method 1000 is performed at an electronic device (e.g., 100, 300, 500, 900) with a display (e.g., 902) and a biometric sensor (e.g., 903) (e.g., a first biometric sensor of a device

with a plurality of biometric sensors) (e.g., a fingerprint sensor, a contactless biometric sensor (e.g., a biometric sensor that does not require physical contact, such as a thermal or optical facial recognition sensor), an iris scanner) at a first portion of the electronic device (e.g., a portion that is not a part of the display). In some examples, the biometric sensor includes one or more cameras. Some operations in method 1000 are, optionally, combined, the orders of some operations are, optionally, changed, and some operations are, optionally, omitted.

[0299] As described below, method 1000 provides an intuitive way for providing indications about the biometric sensor during biometric authentication. The method reduces the cognitive burden on a user for performing biometric authentication, thereby creating a more efficient human-machine interface. For battery-operated computing devices, enabling a user to perform biometric authentication faster and more efficiently conserves power and increases the time between battery charges.

[0300] The electronic device (e.g., 100, 300, 500, 900) detects (1002) (e.g., detects in response to a request to perform an operation that requires authentication) the existence of an error condition that prevents the biometric sensor from obtaining biometric information about a user of the device (e.g., a contactless biometric sensor such as a thermal or optical facial recognition sensor) is occluded (e.g., partially occluded, fully occluded, occluded to a degree sufficient to inhibit operation of the sensor) (e.g., occluded by a portion of the user (e.g., a hand), while interacting with the electronic device).

[0301] In response (1004) to detecting the existence of the error condition, the electronic device (e.g., 100, 300, 500, 900) displays, on the display (e.g., 902), an error indication (e.g., 928) (e.g., a graphical icon). In some examples, the error indication includes text (e.g., indicating that the sensor is occluded. In some examples, the error indication does not include text. The error indication is displayed (1006) at a location that is proximate to the first portion of the electronic device. In some examples, the location is at or near the portion of the display that is closest to the location of the biometric sensor (e.g., 903). Displaying the error indication provides the user with feedback about the current state of the device (e.g., that an error condition is preventing successful biometric authentication) and prompts the user to take further action to correct the error condition. Providing improved feedback to the user enhances the operability of the device and makes the user-device interface more efficient (e.g., by helping the user to provide proper inputs and reducing user mistakes when operating/interacting with the device) which, additionally, reduces power usage and improves

battery life of the device by enabling the user to use the device more quickly and efficiently. Displaying the error indication near the biometric sensor provides the user with feedback as to the association of the biometric sensor with the processes occurring at the device (e.g., attempted authentication). Specifically, the user becomes aware of the biometric sensor during biometric authentication such that the user is less likely to perform an action that interferes with the biometric sensor or alternatively, the user is prompted to take corrective action. Providing improved feedback to the user enhances the operability of the device and makes the user-device interface more efficient (e.g., by helping the user to provide proper inputs and reducing user mistakes when operating/interacting with the device) which, additionally, reduces power usage and improves battery life of the device by enabling the user to use the device more quickly and efficiently.

[0302] In some examples, the error indication (e.g., 928) includes (1008) a biometric sensor occluded icon and a reticle, the error indication providing an indication that the biometric sensor is occluded. In some examples, the error indication is associated with the electronic device performing biometric authentication (e.g., using the biometric sensor to obtain biometric information about a biometric feature (e.g., face, fingerprint). Providing an indication that the biometric sensor is occluded provides the user with feedback about the current state of the device (e.g., that the biometric sensor is occluded) and prompts the user to take further action to correct the error condition. Providing improved feedback with instructions on proper movements of the biometric feature therefore enhances the operability of the device and makes the user-device interface more efficient (e.g., by helping the user to provide proper inputs and reducing user mistakes when operating/interacting with the device), which, additionally, reduces power usage and improves battery life of the device by enabling the user to use the device more quickly and efficiently.

[0303] In accordance (1010) with a determination that a user interface of the electronic device is in a first orientation relative to the biometric sensor, the electronic device (e.g., 100, 300, 500, 900) displays the error indication at a first location in the user interface that is proximate to (e.g., adjacent to, near to, within a predetermined distance of) the first portion of the electronic device.

[0304] In accordance (1012) with a determination that the user interface of the electronic device is in a second orientation relative to the biometric sensor, the electronic device (e.g., 100, 300, 500, 900) displays the error indication (e.g., 928) at a second location in the user

interface that is proximate to (e.g., adjacent to, near to, within a predetermined distance of) the first portion of the electronic device, the first orientation being different from the second orientation.

[0305] In some examples, while attempting (1014) to obtain biometric information using the biometric sensor (e.g., 903), the electronic device (e.g., 100, 300, 500, 900) displays (1016), on the display (e.g., 902), a first progress indicator (e.g., 924, 926, 938, 940). In some examples, the first progress indicator provides an indication of the current state of the electronic device (e.g., locked state, unlocked state, performing biometric authentication, error state, error condition). In some examples, in accordance (1018) with a determination that the user interface (e.g., 906, 908) of the electronic device is in a third orientation relative to the biometric sensor, the user interface in the third orientation having a first top side, the electronic device displays the first progress indicator proximate to (e.g., adjacent to, near to, within a predetermined distance of) the first top side of the user interface in the third orientation. In some examples, in accordance (1020) with a determination that the user interface of the electronic device is in a fourth orientation relative to the biometric sensor, the user interface in the fourth orientation having a second top side, the electronic device displays the first progress indicator proximate to (e.g., adjacent to, near to, within a predetermined distance of) the second top side of the user interface in the fourth orientation, the third orientation being different from the fourth orientation. In some examples, the first progress indicator is displayed on the display at a location that is closest to or proximate to (e.g., adjacent to, near to, within a predetermined distance of) the biometric sensor. Displaying the first progress indicator near the top of the display regardless of orientation ensures that the user is more likely to be aware of the provided feedback to the user (e.g., the progress indicator). Providing improved visual feedback to the user enhances the operability of the device and makes the user-device interface more efficient (e.g., by helping the user to provide proper inputs and reducing user mistakes when operating/interacting with the device) which, additionally, reduces power usage and improves battery life of the device by enabling the user to use the device more quickly and efficiently. In some examples, no indicator is displayed during biometric authentication.

[0306] In some examples, the electronic device (e.g., 100, 300, 500, 900) displays, on the display (e.g., 902), a second progress indicator (e.g., 924, 926, 938, 940) of the electronic device. In some examples, the second progress indicator provides an indication of the current

state of the electronic device (e.g., locked state, unlocked state, performing biometric authentication, error state). In some examples, the first progress indicator is the second progress indicator. In some examples, the second progress indicator is an animation with a first portion (e.g., an indication that the electronic device is performing biometric authenticating using the biometric sensor (e.g., 924) (e.g., rotating rings)) and a second portion (e.g., an indication of an error condition or error state (e.gg., 926), an indication of the current lock or unlock state of the electronic device (e.g., lock icon (e.g., 938), unlock icon (e.g., 940))) that is different from the first portion. In some examples, in accordance with a determination that the second progress indicator is displayed at the location that is proximate to the first portion of the electronic device, the electronic device displays the error indication (e.g., 928) as part of the animation subsequent to the first portion and prior to the second portion.

[0307] In some examples, the electronic device (e.g., 100, 300, 500, 900) displays, on the display (e.g., 902), a home affordance (e.g., 905) (e.g., an indication of a location of a gesture that when performed, results in displaying a home screen such as a swipe up gesture from an edge of the display or a tap gesture on the affordance) at a third location (e.g., a location proximate to a side (e.g., bottom side) of the user interface) in the user interface. In some examples, in accordance with a determination that the error indication (e.g., 928) is displayed at the third location, the electronic device ceases to display the home affordance (e.g., 905) while displaying the error indication at the third location. Ceasing display of the home affordance while displaying an error indication allows the user to quickly realize the home affordance is not accessible because there is an error and prompts the user to take further action to correct the error condition. Providing improved visual feedback to the user enhances the operability of the device and makes the user-device interface more efficient (e.g., by helping the user to provide proper inputs and reducing user mistakes when operating/interacting with the device) which, additionally, reduces power usage and improves battery life of the device by enabling the user to use the device more quickly and efficiently. In some examples, no indicator is displayed during biometric authentication.

[0308] In some examples, after ceasing to display the home affordance (e.g., 905), the electronic device (e.g., 100, 300, 500, 900) detects a correction of the error condition that prevents the biometric sensor (e.g., 903) from obtaining biometric information about the user of the device. In some examples, the electronic device detects the absence of the error

condition subsequent to displaying the error indication (e.g., 928) at the third location. In some examples, in response to detecting the correction of the error condition, the electronic device displays, on the display (e.g., 902), the home affordance at the third location in the user interface (e.g., and ceases to display the error indication (e.g., 928)).

[0309] In some examples, the electronic device (e.g., 100, 300, 500, 900) detects an input (e.g., palm, finger) at the location that is proximate to (e.g., adjacent to, near to, within a predetermined distance of) the first portion of the electronic device. In some examples, in response to detecting the input at the location that is proximate to the first portion of the electronic device, the electronic device displays, on the display, the error indication (e.g., 928) at a different location. In some examples, the different location is a location at which the input is not detected. In some examples, prior to displaying the error indication at the new location, the electronic device determines the different location based on the location of the input with respect to the display. In some examples, the different location is proximate to the location that is proximate to the first portion of the electronic device. In some examples, the error indication is moved to the different location after being initially displayed at a first location that is proximate to the first portion of the electronic device. In some examples, the error indication is initially displayed at a location selected so as to be away from any regions of the display that are known to be occluded (e.g., occluded by a detected touch input). Displaying the error indication at a different location depending on the location of the input (e.g., a user's hand) provides the user with feedback about the current state of the device (e.g., that an error condition is preventing successful biometric authentication) and prompts the user to take further action to correct the error condition. Further, by adjusting the location, the device ensures that the error indication is visible to the user and thus, the user is more likely to take corrective action at the device. Providing improved feedback to the user enhances the operability of the device and makes the user-device interface more efficient (e.g., by helping the user to provide proper inputs and reducing user mistakes when operating/interacting with the device) which, additionally, reduces power usage and improves battery life of the device by enabling the user to use the device more quickly and efficiently.

[0310] In some examples, the electronic device (e.g., 100, 300, 500, 900) displays, on the display (e.g., 902), a first transaction interface (e.g., 914) (e.g., a transaction (or payment) interface that is separate from (or overlaid on top of) the user interface and includes transaction information such as a credit card number, billing address, etc.) at a position that is

proximate to (e.g., adjacent to, near to, within a predetermined distance of) the first portion of the electronic device. In some examples, the first transaction interface is displayed in response to receiving an input (e.g., 910) corresponding to an affordance (e.g., 912) of the user interface (e.g., 908) (e.g., an affordance for making a payment or completing a transaction).

[0311] In some examples, displaying the first transaction interface (e.g., 914) includes displaying an animation of the first transaction interface transitioning (e.g., translating) from an initial position that is substantially centered with respect to the display to the position that is proximate to the first portion of the electronic device. In some examples, the animation includes displaying (e.g., maintaining the display of) the first transaction interface while the first transaction interface transitions (e.g., translates) from the initial position to the position that is proximate to the first portion of the electronic device. In some examples, the animation includes a visual effect where the first transaction interface appears to float while transitioning.

[0312] In some examples, the electronic device (e.g., 100, 300, 500, 900) displays, on the display (e.g., 902), a prompt (e.g., 916) to provide one or more activations of a hardware button (e.g., 904) of the electronic device. In some examples, the electronic device prompts the user by displaying "double click for Apple Pay". In some examples, the prompt is displayed adjacent to the button. In some examples, the prompt is displayed when the device is displaying a transaction user interface region (e.g., 914) but without receiving any indication that a transaction terminal is nearby and is requesting transaction credentials (e.g., the prompt to provide the one or more activations of the button are displayed before the device has been placed in an NFC field of an NFC reader that is requesting payment information). In some examples, the hardware button is a mechanical button or a solid state button. In some examples, the button is a switch or any other type of toggle. In some examples, the button has a fixed position relative to the electronic device, and in particular, relative to the display of the electronic device such that the electronic device may display prompts based on a position of the button. In some examples, the button is a solid-state button that operates according to capacitive and/or resistive touch, and/or is responsive to changes in the intensity of input without having a mechanical switch that is depressed to activate the button and instead monitors whether an intensity of the input is above an intensity threshold that corresponds to activation of the solid-state button. In some

examples, the electronic device (e.g., 100, 300, 500, 900) receives one or more activations (e.g., 920) of the hardware button of the electronic device, and in response to receiving the one or more activations of the hardware button, the electronic device displays, on the display (e.g., 902), an authentication progress indicator (e.g., 922, 924, 930, 932, 934). In some examples, displaying the authentication progress indicator includes displaying an animation of the authentication progress indicator transitioning from a location of the prompt (e.g., 916) to a final position of the authentication progress indicator. In some examples, the authentication indicator provides a status of the authentication (e.g., in progress, successful, unsuccessful). In some examples, the animation includes displaying (e.g., maintaining the display of) the authentication progress indicator while the authentication progress indicator transitions (e.g., translates) from the location of the prompt to the final position. In some examples, the animation includes a visual effect where the authentication progress indicator appears to slide out of the prompt. In some examples, the authentication progress indicator is displayed with (or overlaid on) the user interface (e.g., 914) (or the transaction user interface region). Prompting the user to activate a hardware button guides the user to perform an action at the device in order to complete a transaction. Prompting the user in this manner enhances the operability of the device and makes the user-device interface more efficient (e.g., by helping the user to provide proper inputs and reducing user mistakes when operating/interacting with the device), which, additionally, reduces power usage and improves battery life of the device by enabling the user to use the device more quickly and efficiently. Displaying an authentication progress indicator provides feedback to the user regarding the status of the authentication. Improved feedback enhances the operability of the device and makes the user-device interface more efficient (e.g., by helping the user to provide proper inputs and reducing user mistakes when operating/interacting with the device), which, additionally, reduces power usage and improves battery life of the device by enabling the user to use the device more quickly and efficiently.

[0313] In some examples, the electronic device (e.g., 100, 300, 500, 900) concurrently displays (1022), on the display (e.g., 902), a first application (e.g., corresponding to 906, 908) in a first region (e.g., 907, 909) and a second application (e.g., corresponding to 906, 908) in a second region (e.g., 907, 909), the second application being adjacent to (e.g., next to, proximate to, within a predetermined distance of) the first application. In some examples, the electronic device displays (1024), on the display, a second transaction interface (e.g., 914). In some examples, the second transaction interface is the first transaction interface. In some

examples, the second transaction interface is displayed overlaid on the first application and/or the second application. In some examples, in accordance (1026) with a determination that the second transaction interface corresponds to the first application, the electronic device modifies a first visual characteristic (e.g., obscure, darken, blur) of the first application. In some examples, the second transaction interface corresponds to the first application when the first application includes information about the good or service (or transaction) that is being purchased (or completed) using (or via) the second transaction interface. In some examples, this determination is made while displaying the second transaction interface. In some examples, in accordance (1030) with a determination that the second transaction interface corresponds to the second application, the electronic device (e.g., 100, 300, 500, 900) modifies a first visual characteristic (e.g., obscure, darken, blur) of the second application. In some examples, the second transaction interface corresponds to the first application when the first application includes information about the good or service (or transaction) that is being purchased (or completed) using (or via) the second transaction interface. In some examples, this determination is made while displaying the second transaction interface.

[0314] In some examples, modifying the first visual characteristic of the first application includes modifying a second visual characteristic of the second application. In some examples, modifying the second visual characteristic of the second application includes increasing darkening and/or increasing blur radius of a blur effect applied to the second application to a greater degree (or amount) than with respect to the first application. In some examples, modifying the first visual characteristic of the second application includes modifying a second visual characteristic of the first application. In some examples, modifying the second visual characteristic of the first application includes increasing darkening and/or increasing blur radius of a blur effect applied to the first application to a greater degree (or amount) than with respect to the second application. Modifying the visual characteristic of one application to a greater degree than with respect to another application provides feedback to the user as to which application is more relevant at the time. Providing improved visual feedback to the user enhances the operability of the device and makes the user-device interface more efficient (e.g., by helping the user to provide proper inputs and reducing user mistakes when operating/interacting with the device) which, additionally, reduces power usage and improves battery life of the device by enabling the user to use the device more quickly and efficiently. In some examples, no indicator is displayed during biometric authentication.

[0315] In some examples, modifying the first visual characteristic of the first application includes displaying (1028) the first application in the second region in accordance with a determination that the second region is closer (e.g., nearer) to the first portion of the electronic device (e.g., biometric sensor) than the first region. In some examples, displaying the first application in the second region includes ceasing to display the first application in the first region. In some examples, modifying the first visual characteristic of the second application includes displaying (1032) the second application in the first region in accordance with a determination that the first region is closer (e.g., nearer) to the first portion of the electronic device (e.g., biometric sensor) than the second region. In some examples, displaying the second application in the first region includes ceasing to display the second application in the second region. In some examples, the electronic device displays an animation of the first application swapping places with the second application.

[0316] In some examples, in accordance with the determination that the second transaction interface (e.g., 914) corresponds to the first application, the second transaction interface includes an indication of the first application (e.g., the name of the first application). In some examples, in accordance with the determination that the second transaction interface corresponds to the second application, the second transaction interface includes an indication of the second application (e.g., the name of the second application).

[0317] Note that details of the processes described above with respect to method 1000 (e.g., FIGS. 10A-10C) are also applicable in an analogous manner to the methods described below/above. For example, method 800, method 1200, and/or method 1400 optionally include one or more of the characteristics of the various methods described above with reference to method 1000. For example, error icon 928, as described in method 1000, can be used to indicate that the biometric sensor is obstructed when biometric authentication is being performed in the processes described with respect to method 800, method 1200, and method 1400. For brevity, these details are not repeated below.

[0318] FIGS. 11A-11S illustrate exemplary user interfaces for orienting the device to enroll a biometric feature (e.g., a face for later use in biometric authentication), in accordance with some examples. The user interfaces in these figures are used to illustrate the processes described below, including the processes in FIGS. 12A-12C.

[0319] FIG. 11A illustrates electronic device 900 (e.g., portable multifunction device 100, device 300, device 500). In the exemplary examples illustrated in FIGS. 11A-11S, electronic device 900 is a tablet computer. In other examples, electronic device 900 can be a different type of electronic device, such as a smartphone (e.g., electronic device 700). Electronic device 900 includes display 902, one or more input devices (e.g., touchscreen of display 902, button 904, and a microphone), a wireless communication radio, and biometric sensor 903. Electronic device 900 includes biometric sensor 903. In some examples, biometric sensor 903 includes one or more biometric sensors that can include a camera, such as an infrared camera, a thermographic camera, or a combination thereof. In some examples, biometric sensor 903 includes some or all of the features of biometric sensor 703. In some examples, biometric sensor 903 includes one or more fingerprint sensors (e.g., a fingerprint sensor integrated into a button). In some examples, electronic device 900 further includes a light-emitting device (e.g., light projector), such as an IR flood light, a structured light projector, or a combination thereof. The light-emitting device is, optionally, used to illuminate the biometric feature (e.g., the face) during capture of biometric data of biometric features by biometric sensor 903. In some examples, electronic device 900 includes a plurality of cameras separate from biometric sensor 903. In some examples, electronic device 900 includes only one camera separate from biometric sensor 903.

[0320] At FIG. 11A, a user wishes to set up biometric (e.g., face) authentication on electronic device 900. Successfully setting up biometric authentication on the device enables a user to perform operations on the device that require authentication (e.g., unlocking the device) by presenting the user's face for biometric authentication. To set up biometric authentication on the electronic device, a user must first enroll her face. The process for enrolling the face can include some or all of the features (or processes) of FIGS. 11A-11O.

[0321] As illustrated in FIG. 11A, electronic device 900 displays introduction user interface (UI) 1106 with initiate affordance 1108. Electronic device 900 receives input 1110 at initiate affordance 1108 to start the process of enrolling the user's face for biometric authentication.

[0322] At FIG. 11B, in response to receiving input 1110 at initiate affordance 1108, electronic device 900 determines that the orientation of the device is not suitable for enrolling the user's face. In some examples, a suitable orientation for enrolling the user's face is a portrait orientation that is upright (e.g., vertical), where the portrait orientation is such that

biometric sensor 903 is at the top of the device (e.g., the side of the device that is farthest away from the ground). In response to determining that the orientation of the device is not suitable for enrolling the user's face, electronic device 900 displays (e.g., replaces display of introduction UI 1106 with) one or more prompts to prompt the user to orient electronic device 900 to a suitable orientation. More specifically, electronic device 900 determines that electronic device 900 is in a substantially horizontal orientation (e.g., approximately parallel to the ground). As a result, as depicted in FIG. 11B, electronic device 900 displays prompt 1112A to prompt the user to lift electronic device 900 to an upright position.

[0323] In some examples, in response to receiving input 1110 at initiate affordance 1108, electronic device determines that the orientation of the device is suitable for enrolling the user's face. In some examples, upon determining that the orientation is suitable for enrolling the user's face, electronic device 900 automatically initiates a process for enrolling the user's face, as described below with respect to FIG. 11D.

[0324] At FIG. 11C, in response to determining that electronic device 900 is in an upright position but not in a portrait orientation (e.g., the user has lifted the device off the table in response to prompt 1112A), electronic device 900 displays (e.g., replaces display of prompt 1112A with) prompt 1112B to prompt the user to rotate electronic device 900 to a portrait orientation (e.g., with the biometric sensor 903 at the top). Specifically, prompt 1112B prompts the user to rotate in a specific direction (e.g., using text and/or an arrow) such that minimal rotation is required to achieve the desired (or suitable) orientation. For example, prompt 1112B prompts the user to rotate electronic device 900 clockwise because rotating clockwise requires less rotation to achieve the desired orientation than rotating the device counterclockwise. In some examples, prompt 1112B includes an animation of a representation of electronic device 900 rotating clockwise 90 degrees to indicate to the user the action needed to orient the device to a suitable orientation for enrolling the user's face.

[0325] In some examples, electronic device 900 displays a different prompt based on the orientation of the device. For example, if biometric sensor 903 is located adjacent to the right edge of the device (e.g., with respect to the user), electronic device 900 displays prompt 1112C in FIG. 11Q. In some examples, prompt 1112C prompts the user to rotate the device counterclockwise (e.g., via text and/or a pictorial illustration of the direction in which to rotate the device). In some examples, prompt 1112C includes an animation of a representation of electronic device 900 rotating counterclockwise 90 degrees to indicate to

the user the action needed to orient the device to a suitable orientation for enrolling the user's face. As another example, if biometric sensor 903 is located adjacent to the bottom edge of the device (e.g., with respect to the user), electronic device 900 displays prompt 1112D in FIG. 11R. In some examples, prompt 1112D prompts the user to rotate the device 180 degrees (e.g., via text and/or a pictorial illustration of the direction in which to rotate the device). In some examples, prompt 1112D includes an animation of a representation of electronic device 900 rotating clockwise or counterclockwise 180 degrees to indicate to the user the action needed to orient the device to a suitable orientation for enrolling the user's face.

[0326] At FIG. 11D, in response to determining that electronic device 900 is in a suitable orientation, electronic device 900 automatically initiates a process for enrolling the user's face. As illustrated in FIGS. 11D-11F, after initiating the process for enrolling the user's face, electronic device 900 displays face enrollment UI 1114. Face enrollment UI 1114 includes a facial image of the user. In some examples, the facial image is an image of the user captured by one or more cameras on device 900. For example, the facial image optionally is live preview of the image data captured by the one or more cameras (e.g., a digital viewfinder) that updates continuously as the field of view of the camera and/or the field of view's contents change. In some examples, background content is removed such that only the user's face is visible in the facial image. Face enrollment UI 1114 also optionally includes an orientation guide that is superimposed (e.g., overlaid) on the facial image. The orientation guide is, optionally, a set of curved lines that extend into a virtual z-dimension (e.g., along an axis normal to the plane of the display) and intersect over the center of the facial image. Thus, the curved lines of the orientation guide appear to bulge outwards relative to the plane of display 902 to give a sense of the position of the user's head in three-dimensional space.

[0327] Face enrollment UI 1114 also includes an enrollment progress meter. The enrollment progress meter includes a set of display elements (e.g., progress elements) that are arranged around the facial image and the orientation guide. In the example of FIG. 11D, the progress elements are a set of lines that extend radially outward from the facial image arranged in a circular pattern. In some examples, the progress elements indicate an orientation of the user's face needed to enroll corresponding facial features. For example, progress elements in the upper portion of the enrollment progress meter optionally move, fill

in, elongate, and/or change color when the user's head is tilted upwards, which allows the one or more cameras on device 900 to capture image data of the under-side of the user's face. In some examples, device 900 displays progress elements in the enrollment progress meter in an unenrolled state (e.g., the progress elements are greyed out, unchanged).

[0328] Face enrollment UI 1114 also includes a text prompt, which instructs the user to move (e.g., rotate and/or tilt) their head in a circular motion during the enrollment process. In some examples, the text prompt is optionally accompanied by tactile and/or auditory prompt depending on device settings and/or user selections. In some examples, device 900 displays the text prompt on face enrollment UI 1114 through the facial enrollment process.

[0329] In some examples, instead of automatically initiating a process for enrolling the user's face (and displaying face enrollment UI 1114), electronic device 900 displays enrollment introduction UI 1146 in FIG. 11S in response to determining that electronic device 900 is in a suitable orientation. Enrollment introduction UI 1146 includes a face glyph (e.g., a representation of a biometric feature (e.g., face)), and an enrollment progress meter. The enrollment progress meter includes a set of display elements (e.g., progress elements) that are arranged around the glyph. In some examples, the progress elements includes some or all of the features of the progress elements described above with respect to FIG. 11D. In some examples, to trigger display of face enrollment UI 1114 and proceed with enrollment of the user's face, the user activates continue affordance 1148 on enrollment introduction UI 1146. For example, as shown in FIG. 11S, electronic device 900 detects activation (e.g., selection) of continue affordance 1148 via input 1150 (e.g., tap gesture). In some examples, in response to detecting activation of continue affordance 1148, electronic device 900 initiates the process for enrolling the user's face, as described above with respect to FIG. 11D.

[0330] At FIG. 11G, after successfully completing the enrollment of the user's face, electronic device 900 displays (e.g., replaces display of face enrollment UI 1114 with) scan completion interface 1116, which includes continue affordance 1118. Scan completion interface 1116 includes a facial image and a success-state meter. In the example of FIG. 11G, the facial image is blurred, faded, darkened or otherwise obscured to indicate that additional image data is no longer being collected as part of the facial scan. In some examples, the success-state meter is a solid, continuous green circle surrounding the facial image that provides a visual indication that the first scan is complete. To provide a further

visual notification, scan completion interface 1116 also includes a text prompt (e.g., a completion message).

[0331] After completing enrollment of the user's face, a second iteration of the enrollment process is performed without requiring that the user re-orient the device. As depicted in FIG. 11G, while displaying scan completion interface 1116, electronic device 900 receives input 1120 at continue affordance 1118 to initiate the second iteration of the enrollment process.

[0332] At FIG. 11H, in response to receiving input 1120 at continue affordance 1118, electronic device 900 initiates a second iteration of the enrollment process, analogous to the processes described above with respect to FIGS. 11D-11F. Electronic device 900 initiates the second iteration without prompting the user to re-orient the device to an orientation different from its current orientation. Initiating the second iteration of the enrollment process includes displaying second face enrollment UI 1122. Second face enrollment UI 1122 includes some or all of the features of face enrollment UI 1114.

[0333] At FIG. 11I, after successfully completing the second iteration of the enrollment process, electronic device 900 displays (e.g., replaces display of second face enrollment UI 1122 with) second scan completion interface 1124, which includes continue affordance 1126. Second scan completion interface 1124 includes some or all of the features of scan completion interface 1116. As illustrated in FIG. 11I, electronic device 900 receives input 1128 at continue affordance 1126.

[0334] At FIG. 11J, in response to receiving input 1128 at continue affordance 1126, electronic device 900 displays (e.g., replaces display of second scan completion interface 1124 with) enrollment completion interface 1130, providing an indication to the user that biometric authentication has been successfully set up on electronic device 900. Enrollment completion interface 1130 includes a biometric authentication glyph. For example, the biometric authentication glyph is, optionally, a line drawing of all or part of a face (e.g., a stylized face graphic). In the example of FIG. 11J, enrollment completion interface 1130 also includes a text prompt indicating that the enrollment process is complete and face authentication at the device is set-up and/or enabled. In some examples, enrollment completion interface 1130 also includes a completion affordance, activation of which causes device 900 to exit face authentication set-up. In some examples, enrollment completion

interface 1130 includes a visual indication (e.g., checkmark) that the enrollment process is complete.

[0335] At FIG. 11K, after biometric authentication has been set up on electronic device 900, a user can unlock electronic device 900 (e.g., transition the device from a locked state to an unlocked state) using biometric authentication by presenting the user's face to biometric sensor 903. In some examples, the user initiates biometric authentication to unlock the device by lifting (or raising) electronic device 900 (e.g., from a substantially horizontal orientation). While electronic device 900 is being lifted, electronic device 900 detects a change in orientation of the device, and in response, initiates biometric authentication to unlock the device. It is noted that while electronic device 900 is in a locked state, electronic device 900 displays locked state interface 1132 including biometric sensor indicator 1134, which provides an indication to the user of the location of biometric sensor 903, and lock icon 1136, which provides an indication that electronic device 900 is in a locked state. In some examples, electronic device 900 does not display biometric sensor indicator 1134 while electronic device 900 is in a locked state.

[0336] As depicted in FIG. 11L, when electronic device 900 initiates biometric authentication, the user is holding electronic device 900 such that the user's face is outside field of view 1138 of biometric sensor 903. In some examples, the user's face is outside field of view 1138 when more than a threshold portion of the face is outside the field of view. In some examples, the user's face is outside field of view 1138 when no face is detected within the field of view. While attempting to biometrically authenticate the user's face, electronic device 900 is unable to obtain sufficient information about the user's face using biometric sensor 903. As a result, electronic device 900 does not have sufficient information for comparison with the stored authorized credentials, which were generated from the enrollment process described above with respect to FIGS. 11D-11J.

[0337] At FIG. 11M, upon determining that the user's face is outside field of view 1138, electronic device 900 displays error indication 1140, which provides an indication to the user that the user's face is outside field of view 1138. (Error indication 1140 includes some or all of the features of error indication 714G.) Additionally, upon determining that the user's face is outside field of view 1138, electronic device 900 does not automatically retry authentication. In some examples, electronic device 900 also displays biometric sensor indicator 1134. In some examples, if sufficient information had been obtained but

authentication nevertheless failed (e.g., the obtained information did not match the stored authorized credentials), electronic device 900 automatically retries biometric authentication.

[0338] As depicted in FIG. 11N, after learning from error indication 1140 that the user's face is outside field of view 1138 of biometric sensor 903, the user moves her face into field of view 1138 such that the user's face is within field of view 1138. In response to detecting that the cause of error indication 1140 has been corrected (e.g., detects more than a threshold amount of the user's face), electronic device 900 automatically retries biometric authentication. Upon determining that authentication is successful as a result of retrying biometric authentication (e.g., the information obtained using biometric sensor 903 matches the stored authorized credentials), electronic device 900 transitions from a locked state to an unlocked state. After transitioning to the unlocked state, electronic displays unlocked state interface 1142.

[0339] In some examples, while displaying unlocked state interface 1142, electronic device 900 receives a request (e.g., an upward swipe starting from within a region adjacent to the bottom edge of display 902) to access restricted content on the device (e.g., home screen 1144 of FIG. 11O, the most recently used application). In response to receiving the request to access restricted content, electronic device 900 displays home screen 1144, including a plurality of icons that, when activated, result in launching an application corresponding to the activated icon. In some examples, instead of displaying home screen 1144, electronic device 900 displays the most recently used application (e.g., a user interface of the application). It is noted that the above processes described above with respect to FIGS. 11K-11O are performed when electronic device 900 is in a landscape orientation. However, in some examples, some or all of the processes described above with respect to FIGS. 11K-11N can be performed when electronic device 900 is in a portrait orientation.

[0340] In some examples, instead of transitioning to an unlocked state as described with respect to FIG. 11N, electronic device 900 maintains a locked state if the obtained information does not match the stored authorized credentials. In some examples, as depicted in FIG. 11P, upon determining that the obtained information does not match the stored authorized credentials, electronic device 900 displays locked state interface 1132 while alternating the position of lock icon 1136 such that it simulates a "shake" effect, thereby providing an indication to the user that electronic device 900 remains in a locked state.

[0341] FIGS. 12A-12C are flow diagrams illustrating a method for orienting the device to enroll a biometric feature (e.g., a face for later use in biometric authentication), in accordance with some examples. Method 1200 is performed at an electronic device (e.g., 100, 300, 500, 900) with a display (e.g., 902) and one or more biometric sensors (e.g., 903) (e.g., a biometric sensor of a device with a plurality of biometric sensors) (e.g., a fingerprint sensor, a contactless biometric sensor (e.g., a biometric sensor that does not require physical contact, such as a thermal or optical facial recognition sensor), an iris scanner). In some examples, the one or more biometric sensors include one or more cameras. Some operations in method 1200 are, optionally, combined, the orders of some operations are, optionally, changed, and some operations are, optionally, omitted.

[0342] As described below, method 1200 provides an intuitive way for prompting a user to orient a device to enroll a biometric feature. The method reduces the cognitive burden on a user for enrolling a biometric feature (e.g., a face for later use in biometric authentication), thereby creating a more efficient human-machine interface. For battery-operated computing devices, enabling a user to enroll a biometric feature faster and more efficiently conserves power and increases the time between battery charges.

[0343] The electronic device (e.g., 100, 300, 500, 900) displays (1202), on the display (e.g., 902), a biometric enrollment user interface (e.g., 1106) for initiating biometric enrollment with the one or more biometric sensors.

[0344] While displaying (1204) the biometric enrollment user interface, the electronic device receives input (e.g., 1110) (e.g., touch gesture (e.g., tap), spoken user input) corresponding to a request to initiate biometric enrollment.

[0345] In response (1206) to receiving the input (e.g., 1110) and in accordance (1208) with a determination that an orientation of the electronic device (e.g., current orientation, an orientation of the electronic device at (or near) the time of the input) satisfies a set of enrollment criteria, the electronic device initiates a process for enrolling a biometric feature with the one or more biometric sensors (e.g., 903). In some examples, the set of enrollment criteria includes whether the electronic device is oriented in a portrait orientation with respect to a frame of reference (e.g., Earth, ground), whether the one or more biometric sensors are oriented (or located) at a particular side of the electronic device in the portrait orientation (e.g., the side furthest away from Earth), or whether the electronic device is oriented such that

it is not approximately parallel with respect to the ground. In some examples, the set of enrollment criteria includes whether the electronic device is in a certain (e.g., proper) orientation relative to a biometric feature (e.g., face) (e.g., a primary plane of the device (e.g., a plane defined by the display of the device) is facing the biometric feature). In some examples, initiating a process for enrolling a biometric feature includes capturing data corresponding to a face of a user using the one or more biometric sensors. In some examples, the set of enrollment criteria includes a requirement that the device is in an orientation that is suitable for enrolling a biometric feature for biometric authentication. In some examples, initiating a process for enrolling a biometric feature includes (or triggers) displaying a enrollment user interface (e.g., 1114) for capturing information about a biometric feature.

[0346] In response (1206) to receiving the input (e.g., 1110) and in accordance (1222) with a determination that the orientation of the electronic device does not satisfy the set of enrollment criteria, outputting one or more prompts (e.g., 1112A-B) (e.g., a visual, audio and/or tactile prompt) to change the orientation of the electronic device to a different orientation that satisfies the set of enrollment criteria. Outputting one or more prompts when the set of enrollment criteria are not satisfied provides the user with feedback as to what corrective actions to take to continue enrolling a biometric feature. Providing improved feedback to the user enhances the operability of the device and makes the user-device interface more efficient (e.g., by helping the user to provide proper inputs and reducing user mistakes when operating/interacting with the device) which, additionally, reduces power usage and improves battery life of the device by enabling the user to use the device more quickly and efficiently. In some examples, no indicator is displayed during biometric authentication.

[0347] In some examples, outputting the one or more prompts includes outputting (1224) a first prompt (e.g., 1112A) to orient the electronic device to an initial orientation. In some examples, the initial orientation is an orientation such that the electronic device is not approximately parallel with respect to the ground. In some examples, the initial orientation is an orientation such that the electronic device is approximately parallel to the force of gravity. In some examples, the set of enrollment criteria includes a requirement that a primary plane of a device be substantially aligned with a predetermined plane (e.g., a plane that is substantially normal to the ground) such that the display of the device is substantially vertical. In some examples, the set of enrollment criteria includes a requirement that the

primary plane of the device is not substantially aligned with a (second) predetermined plane (e.g., a plane that is substantially parallel to the ground) such that the device is not resting on a horizontal surface while attempting to enroll a biometric feature. In some examples, outputting the one or more prompts includes, subsequent to outputting the first prompt (e.g., 1112A), outputting (1226) a second prompt (e.g., 1112B) to orient the electronic device to the different orientation that satisfies the set of enrollment criteria, the first prompt being different from the second prompt. In some examples, the electronic device outputs the first prompt without outputting the second prompt. In some examples, the electronic device ceases outputting the first prompt when the orientation of the electronic device changes to the initial orientation. In some examples, the electronic device outputs the second prompt when the orientation of the electronic device changes to the initial orientation. In some examples, the electronic device outputs the second prompt without outputting the first prompt (e.g., when the electronic device is already in the initial orientation). In some examples, the set of enrollment criteria includes whether the electronic device is oriented in a portrait orientation with respect to a frame of reference (e.g., Earth, ground), whether the one or more biometric sensors are oriented (or located) at a particular side of the electronic device in the portrait orientation (e.g., the side furthest away from Earth), or whether the electronic device is oriented such that it is not approximately parallel with respect to the ground. Outputting the first prompt without outputting the second prompt provides improved feedback to the user as it reduces the chances of confusion when the user is taking corrective actions to trigger enrollment of a biometric feature. Providing improved visual feedback to the user enhances the operability of the device and makes the user-device interface more efficient (e.g., by helping the user to provide proper inputs and reducing user mistakes when operating/interacting with the device) which, additionally, reduces power usage and improves battery life of the device by enabling the user to use the device more quickly and efficiently. In some examples, no indicator is displayed during biometric authentication.

[0348] In some examples, outputting the one or more prompts includes outputting a third prompt (e.g., 1112B) to rotate the electronic device (e.g., about an axis perpendicular to the electronic device) to the different orientation that satisfies the set of enrollment criteria, the third prompt being based on the orientation of the electronic device while receiving the input. In some examples, the third prompt is the second prompt. In some examples, in accordance with a determination that the orientation of the electronic device is in a first orientation, the electronic device outputs a first rotation prompt to rotate the electronic device to the different

orientation that satisfies the set of enrollment criteria. In some examples, in accordance with a determination that the orientation of the electronic device is in a second orientation that is different from the first orientation, the electronic device outputs a second rotation prompt to rotate the electronic device to the different orientation that satisfies the set of enrollment criteria, the second rotation prompt being different from the first rotation prompt. In some examples, the first rotation prompt or the second rotation prompt is the second prompt. In some examples, the set of enrollment criteria includes whether the electronic device is oriented in a portrait orientation with respect to a frame of reference (e.g., Earth, ground), whether the one or more biometric sensors are oriented (or located) at a particular side of the electronic device in the portrait orientation (e.g., the side furthest away from Earth), or whether the electronic device is oriented such that it is not approximately parallel with respect to the ground. Outputting a prompt based on the orientation of the device provides feedback to the user as to an efficient process for achieving a suitable orientation of the device for enrolling a biometric feature. Providing improved feedback to the user enhances the operability of the device and makes the user-device interface more efficient (e.g., by helping the user to provide proper inputs and reducing user mistakes when operating/interacting with the device) which, additionally, reduces power usage and improves battery life of the device by enabling the user to use the device more quickly and efficiently.

[0349] In some examples, outputting the one or more prompts includes outputting a fourth prompt (e.g., 1112B) to rotate (e.g., along an axis parallel to a primary plane (e.g., a plane defined by the display of the device) of the device) the electronic device (e.g., about an axis perpendicular to the electronic device) to the different orientation that satisfies the set of enrollment criteria, the fourth prompt being based on an alignment of a primary plane of the device (e.g., a plane defined by the display of the device) to a predetermined plane (e.g., a plane that is substantially normal to the ground; a plane that is substantially parallel to the ground). In some examples, the electronic device outputs the fourth prompt in accordance with a determination that the electronic device is oriented substantially parallel to the ground. In some examples, the set of enrollment criteria includes a requirement that a primary plane of a device be substantially aligned with a predetermined plane (e.g., a plane that is substantially normal to the ground) such that the display of the device is substantially vertical. In some examples, the set of enrollment criteria includes a requirement that the primary plane of the device is not substantially aligned with a (second) predetermined plane

(e.g., a plane that is substantially parallel to the ground) such that the device is not resting on a horizontal surface while attempting to enroll a biometric feature.

[0350] In some examples, the orientation of the electronic device (e.g., 900) does not satisfy the set of enrollment criteria due to the orientation resulting in the one or more biometric sensors (e.g., 903) being located (substantially) near (at or adjacent to) the right side of the electronic device (e.g., located (substantially) to the right of the center of the electronic device). In some examples, the location of the biometric sensor is with respect to the user. In some examples, the one or more prompts (e.g., 1112C) includes an animation of a representation of a device rotating by less than a first amount in a first direction (e.g., approximately 90 degrees counter-clockwise (e.g., to the left)). In some examples, the animation shows the representation rotating counter-clockwise such that the representation ends in a portrait orientation with the representation of a biometric sensor located near the top side of the representation. In some examples, the one or more prompts includes a textual indication and/or a pictorial illustration of the direction (and/or amount (e.g., degrees)) in which to rotate the device. Displaying an animation of a representation of a device rotating provides the user with feedback as to what corrective action to take to continue enrolling a biometric feature. Providing improved feedback to the user enhances the operability of the device and makes the user-device interface more efficient (e.g., by helping the user to provide proper inputs and reducing user mistakes when operating/interacting with the device) which, additionally, reduces power usage and improves battery life of the device by enabling the user to use the device more quickly and efficiently.

[0351] In some examples, the orientation of the electronic device (e.g., 900) does not satisfy the set of enrollment criteria due to the orientation resulting in the one or more biometric sensors (e.g., 903) being located (substantially) near (at or adjacent to) the left side of the electronic device (e.g., located (substantially) to the left of the center of the electronic device. In some examples, the location of the biometric sensor is with respect to the user. In some examples, the one or more prompts (e.g., 1112B) includes an animation of a representation of a device rotating by less than the first amount in a second direction that is different from the first direction (e.g., approximately 90 degrees clockwise (e.g., to the right). In some examples, the animation shows the representation rotating clockwise such that the representation ends in a portrait orientation with the representation of a biometric sensor located near the top side of the representation. In some examples, the one or more prompts

includes a textual indication and/or a pictorial illustration of the direction (and/or amount (e.g., degrees)) in which to rotate the device.

[0352] In some examples, the orientation of the electronic device (e.g., 900) does not satisfy the set of enrollment criteria due to the orientation resulting in the one or more biometric sensors (e.g., 903) being located (substantially) near (at or adjacent to) the bottom side of the electronic device (e.g., located (substantially) below the center of the electronic device). In some examples, the location of the biometric sensor is with respect to the user. In some examples, the one or more prompts (e.g., 1112D) includes an animation of a representation of a device rotating by more than the first amount (e.g., rotating upside down or approximately 180 degrees either clockwise or counterclockwise (e.g., to the right or to the left). In some examples, the animation shows the representation rotating clockwise or counter-clockwise 180 degrees such that the representation ends in a portrait orientation with the representation of a biometric sensor located near the top side of the representation. In some examples, the one or more prompts includes a textual indication and/or a pictorial illustration of the direction (and/or amount (e.g., degrees)) in which to rotate the device.

[0353] In some examples, subsequent to outputting the one or more prompts (e.g., 1112B-D) to change the orientation of the electronic device to a different orientation that satisfies the set of enrollment criteria, the electronic device detects a change in orientation of the electronic device. In some examples, in response to detecting the change in orientation of the electronic device: in accordance with a determination that the orientation of the electronic device still does not satisfy the set of enrollment criteria, the electronic device outputs one or more new prompts (e.g., 1112B-D) to change the orientation of the electronic device to a different orientation that satisfies the set of enrollment criteria. In some examples, the one or more new prompts (e.g., 1112B-D) are different from the one or more prompts described above. In some examples, the one or more new prompts (e.g., 1112B-D) can include any one of the animations described above (e.g., rotate clockwise, rotate counter-clockwise, rotate 180 degrees). In some examples, in response to detecting the change in orientation of the electronic device: in accordance with a determination that the orientation of the electronic device satisfies the set of enrollment criteria, the electronic device initiates a process for enrolling a biometric feature with the one or more biometric sensors, such as by displaying a biometric enrollment introduction interface (e.g., 1146).

[0354] In some examples, subsequent to initiating the process for enrolling the biometric feature (e.g., subsequent to successfully enrolling a biometric feature), the electronic device (e.g., 100, 300, 500, 900) receives a request to perform an operation that requires authentication (e.g., a request to unlock the device (e.g., perform a swipe at a predefined location)). In some examples, the electronic device receives the request to perform the operation that requires authentication subsequent to performing (or completing) biometric enrollment. In some examples, the electronic device receives the request to perform the operation that requires authentication subsequent to outputting the one or more prompts (e.g., 1112A-B) (e.g., a visual, audio and/or tactile prompt) to change the orientation of the electronic device to the different orientation that satisfies the set of enrollment criteria. In some examples, in response to receiving the request to perform the operation that requires authentication, the electronic device attempts authentication using the one or more biometric sensors (e.g., 903) (e.g., that includes obtaining data by the one or more biometric sensors). In some examples, after attempting (e.g., unsuccessfully attempting) authentication using the one or more biometric sensors and in accordance with a determination that data obtained by the one or more biometric sensors corresponds to less than a threshold amount of a biometric feature (e.g., part of a face/fingerprint, not a whole face/fingerprint) (e.g., due to the face being outside the field of view (e.g., 1138), the electronic device forgoes retrying authentication. In some examples, the electronic device forgoes automatically retrying authentication. In some examples, after attempting authentication using the one or more biometric sensors, the electronic device forgoes retrying authentication due to biometric authentication having failed more than a predetermined number of times (e.g., 5, 10, 15) since the last successful authentication with the device. In some examples, the electronic device forgoes retrying authentication without an explicit request to perform an operation that requires authentication (e.g., a request to unlock the device (e.g., perform a swipe at a predefined location)). In some examples, after an initial attempt at authentication does not succeed, the electronic device retries biometric authentication if a determination is not made that data obtained by the one or more biometric sensors corresponds to only a portion of a biometric feature. Forgoing retrying authentication when less than a threshold amount of a biometric feature is obtained avoids the user consuming the permitted number of attempts on repeated requests (e.g., repeated requests of the same type), thereby conserving at least one attempt for requests for other operations that require biometric authentication. Conserving at least one attempt enhances the operability of the device and makes the user-device interface

more efficient (e.g., by avoiding exhaustion of authentication attempts on repeated, similar requests) which, additionally, reduces power usage and improves battery life of the device by enabling the user to use the device more quickly and efficiently.

[0355] In some examples, after attempting (e.g., unsuccessfully attempting) authentication using the one or more biometric sensors and in accordance with a determination that the data obtained by the one or more biometric sensors corresponds to not less (e.g., more) than the threshold amount of the biometric feature, the electronic device retries authentication. Automatically retrying authentication when a threshold amount of the biometric feature is obtained provides the user the ability to attempt authentication when the conditions are appropriate without requiring the user to explicitly request retrying authentication. Performing an operation when a set of conditions has been met without requiring further user input enhances the operability of the device (e.g., increases the chances of successful authentication) and makes the user-device interface more efficient (e.g., by helping the user to provide proper inputs and reducing user mistakes when operating/interacting with the device) which, additionally, reduces power usage and improves battery life of the device by enabling the user to use the device more quickly and efficiently.

[0356] In some examples, in accordance with a determination that authentication resulting from retrying authentication is successful, the electronic device (e.g., 100, 300, 500, 900) performs an operation corresponding to the request. In some examples, in accordance with a determination that authentication resulting from retrying authentication is not successful, the electronic device forgoes performing the operation corresponding to the request. In some examples, authentication is successful when the biometric information captured using the one or more biometric sensors corresponds to (or matches) authorized credentials (e.g., stored information about a biometric feature (e.g., face, fingerprint) that are authorized for use in biometric authentication). In some examples, authentication is unsuccessful when the biometric information captured using the one or more biometric sensors does not correspond to (or match) authorized credentials (e.g., stored information about a biometric feature (e.g., face, fingerprint) that are authorized for use in biometric authentication). Forgoing performing the operation when authentication is not successful enhances device security by preventing fraudulent and/or unauthorized access to the device. Improving security measures of the device enhances the operability of the device by preventing unauthorized access to content and operations and, additionally, reduces power

usage and improves battery life of the device by enabling the user to use the device more efficiently.

[0357] In some examples, subsequent to outputting the one or more prompts (e.g., 1112A-B) (e.g., a visual, audio and/or tactile prompt) to change the orientation of the electronic device to the different orientation that satisfies the set of enrollment criteria, the electronic device (e.g., 100, 300, 500, 900) detects (1228) that the current orientation of the electronic device satisfies the set of enrollment criteria. In some examples, in response (1230) to determining that the current orientation of the electronic device satisfies the set of enrollment criteria, the electronic device initiates the process for enrolling the biometric feature with the one or more biometric sensors. In some examples, the set of enrollment criteria includes whether the electronic device is oriented in a portrait orientation with respect to a frame of reference (e.g., Earth, ground), whether the one or more biometric sensors are oriented (or located) at a particular side of the electronic device in the portrait orientation (e.g., the side furthest away from Earth), or whether the electronic device is oriented such that it is not approximately parallel with respect to the ground. In some examples, the set of enrollment criteria includes a requirement that a primary plane of a device be substantially aligned with a predetermined plane (e.g., a plane that is substantially normal to the ground) such that the display of the device is substantially vertical. In some examples, the set of enrollment criteria includes a requirement that the primary plane of the device is not substantially aligned with a (second) predetermined plane (e.g., a plane that is substantially parallel to the ground) such that the device is not resting on a horizontal surface while attempting to enroll a biometric feature. In some examples, the set of enrollment criteria includes whether the electronic device is in a certain (e.g., proper) orientation relative to a biometric feature (e.g., face) (e.g., a primary plane of the device (e.g., a plane defined by the display of the device) is facing the biometric feature).

[0358] In some examples, initiating the process for enrolling a biometric feature with the one or more biometric sensors includes displaying a biometric enrollment introduction interface (e.g., 1146). In some examples, the biometric enrollment interface includes concurrently displaying a representation of a simulation of a biometric feature and a simulated progress indicator.

[0359] In some examples, initiating the process for enrolling the biometric feature with the one or more biometric sensors includes successfully enrolling the biometric feature. In

some examples, subsequent to successfully enrolling the biometric feature, the electronic device (e.g., 100, 300, 500, 900) outputs (1212) a prompt (e.g., corresponding to 1122) to enroll the biometric feature for a second time with the one or more biometric sensors. In some examples, the electronic device outputs the prompt to enroll the biometric feature without prompting to change the orientation of the electronic device.

[0360] In some examples, initiating the process for enrolling the biometric feature with the one or more biometric sensors includes (1210) successfully enrolling the biometric feature. In some examples, subsequent to successfully enrolling the biometric feature, the electronic device (e.g., 100, 300, 500, 900) receives (1214) a request to perform an operation that requires authentication (e.g., a request to unlock the device (e.g., perform a swipe at a predefined location), request to access home screen (e.g., 1144)). In some examples, in response (1216) to receiving the request to perform the operation that requires authentication and in accordance (1218) with a determination that data obtained by the one or more biometric sensors corresponds to (e.g., matches) the enrolled biometric feature, the electronic device performs the operation that requires authentication. In some examples, in response to receiving the request to perform the operation that requires authentication, the electronic device performs authentication (or attempts to authenticate) using the one or more biometric sensor (e.g., 903). In some examples, in response (1216) to receiving the request to perform the operation that requires authentication and in accordance (1220) with a determination that data obtained by the one or more biometric sensors does not correspond to (e.g., does not match) the enrolled biometric feature, the electronic device forgoes performing the operation that requires authentication.

[0361] FIGS. 13A-13Z illustrate exemplary user interfaces for prompting a user to correct an error condition that is detected while attempting to biometrically authenticate the user, in accordance with some examples. The user interfaces in these figures are used to illustrate the processes described below, including the processes in FIGS. 14A-14B.

[0362] FIG. 13A illustrates electronic device 900 (e.g., portable multifunction device 100, device 300, device 500). In the exemplary examples illustrated in FIGS. 13A-13Z, electronic device 900 is a tablet computer. In other examples, electronic device 900 can be a different type of electronic device, such as a smartphone (e.g., electronic device 700). Electronic device 900 includes display 902, one or more input devices (e.g., touchscreen of display 902, button 904, and a microphone), a wireless communication radio, and biometric

sensor 903. Electronic device 900 includes biometric sensor 903. In some examples, biometric sensor 903 includes one or more biometric sensors that can include a camera, such as an infrared camera, a thermographic camera, or a combination thereof. In some examples, biometric sensor 903 includes some or all of the features of biometric sensor 703. In some examples, biometric sensor 903 includes one or more fingerprint sensors (e.g., a fingerprint sensor integrated into a button). In some examples, electronic device 900 further includes a light-emitting device (e.g., light projector), such as an IR flood light, a structured light projector, or a combination thereof. The light-emitting device is, optionally, used to illuminate the biometric feature (e.g., the face or an iris) during capture of biometric data of biometric features by biometric sensor 903. In some examples, electronic device 900 includes a plurality of cameras separate from biometric sensor 903. In some examples, electronic device 900 includes only one camera separate from biometric sensor 903.

[0363] FIGS. 13A-13J illustrate a scenario where electronic device 900 detects an error condition while attempting to unlock the device using biometric sensor 903. A user wishes to access restricted content on electronic device 900. For example, the restricted content can be home screen 1324A of FIG. 13G, the most recently used application, or the content associated with notifications 1306, 1308, and/or 1310. To access the restricted content, the user must unlock the device, which requires successful authentication of the user.

[0364] To initiate the process of accessing restricted content on electronic device 900, the user lifts (or raises) electronic device 900 (e.g., from a substantially horizontal orientation to the orientation of the device as depicted in the user's hand in FIG. 13A). Due to the change in orientation of the device, electronic device 900 detects (e.g., via accelerometer 168) a request to perform an operation that requires authentication (e.g., a request to unlock the device). In response to detecting the request to unlock the device, electronic device 900 attempts to biometrically authenticate the user using biometric sensor 903. Attempting to biometrically authenticate the user using biometric sensor 903 includes attempting to capture information about a potentially valid biometric feature (e.g., a biometric feature that can be used for biometric authentication) using biometric sensor 903 and/or determining whether the captured information about the potentially valid biometric feature corresponds to, or matches, stored authorized credentials (e.g., a biometric template).

[0365] As depicted in FIG. 13A, the user's face is not substantially facing biometric sensor 903, largely due to the orientation in which electronic device 900 is being held. In

particular, the orientation of the device results in biometric sensor 903 being located adjacent to the bottom edge of electronic device 900 (e.g., with respect to the user) and having only a partial view of the user's face, due to the angle of the device relative to the user (e.g., the chin and nose of the user are visible to the sensor from the bottom of the user's face, but the eyes and mouth are not visible or are visible at an angle that makes it difficult to consistently recognize the features when the face was enrolled from an angle where the eyes and mouth were closer to being directly facing the camera). While attempting to biometrically authenticate the user using biometric sensor 903, electronic device 900 detects that an error condition has occurred. In some examples, detecting that an error condition has occurred requires determining that a potentially valid biometric feature is not substantially facing biometric sensor 903. For example, electronic device 900 detects the presence of a face, but determines that the face is directed to a location that is substantially above biometric sensor 903. Given the orientation of the face, biometric sensor 903 can capture some information about the face. For example, biometric sensor 903 captures information about the lower portion of the face (e.g., chin, bottom of the nose, etc.), but not the upper portion (e.g., eyes, eyebrows, upper portion of the nose, etc.). However, electronic device 900 does not use this information to biometrically authenticate the user (e.g., determine whether the captured information matches stored authorized credentials). In some examples, electronic device 900 does not use this information for biometrically authenticating the user because information captured while the face is not substantially facing biometric sensor 903 is highly correlated with degradation or reduced accuracy of the captured information.

[0366] In some examples, detecting that the error condition has occurred requires determining that electronic device 900 is in an orientation that results in biometric sensor 903 being located adjacent to the bottom edge of the device (e.g., with respect to the user). In some examples, detecting that the error condition has occurred requires detecting that display 902 is on (e.g., active). In other words, if electronic device 900 detects that display 902 is off (e.g., inactive), electronic device 900 will not detect an error condition even if biometric sensor 903 is occluded. In some examples, detecting that the error condition has occurred requires detecting a request to unlock the device. In some examples, a request to unlock the device is, or includes, a request to initiate (or attempt) biometric authentication. In some examples, detecting that the error condition has occurred requires determining that a maximum (e.g., threshold) number of failed biometric authentication attempts has not been reached (e.g., at least one biometric authentication attempt is available).

[0367] In some examples, if a maximum number of failed attempts has been reached, the device does not perform biometric authentication until successful non-biometric authentication (e.g., passcode authentication) has been performed. In some examples, a request to perform an operation that requires authentication (e.g., a request to unlock the device) after the maximum number of failed biometric authentication attempts has been reached triggers display of an alternative authentication user interface (e.g., passcode entry UI 1320A).

[0368] At FIG. 13A, in response to detecting that the error condition has occurred, electronic device 900 maintains a locked state. Because electronic device 900 is in a locked state, the user is unable to access the restricted content. Electronic device 900 displays locked state UI 1300A with lock icon 1302, which provides an indication that the device is in a locked state.

[0369] Further in response to detecting that an error condition has occurred, electronic device 900 initially displays location indication 1304A (e.g., location indication 1304A was not displayed prior to detecting the error condition). Electronic device 900 displays location indication 1304A adjacent to lock icon 1302. Location indication 1304A includes an indication of a user action that can be performed to correct the detected error condition (e.g., for a subsequent biometric authentication attempt). In some examples, location indication 1304A includes an indication of the location of biometric sensor 903 on the device. In some examples, location indication 1304A includes a visual indication (e.g., text, arrow) describing or indicating the location of biometric sensor 903. For example, location indication 1304A can be an animated arrow, as described below with respect to location indication 1318 in FIGS. 13C-13D.

[0370] At FIG. 13B, the user still wishes to access restricted content on electronic device 900, so the user attempts to unlock the device via a swipe gesture despite not having corrected the error condition. Electronic device 900 displays unlock indication 905 in a predefined region adjacent to the bottom edge of display 902 (e.g., with respect to the user). Unlock indication 905 provides an indication of an approximate location on display 902 from which a user can start an upward swipe gesture to attempt to unlock the electronic device.

[0371] While displaying locked state UI 1300A with location indication 1304A, electronic device 900 detects a request to unlock the electronic device. Detecting a request to

unlock the device includes receiving input 1312A starting at a location of display 902, and determining that input 1312A is an upward swipe gesture that starts within a predefined region adjacent to the bottom edge of display 902.

[0372] At FIG. 13C, in response to detecting the request to unlock the device, electronic device 900 displays (e.g., replaces display of locked state UI 1300A with) interstitial interface 1314A. Interstitial interface 1314A indicates to the user that electronic device 900 has not yet completed biometric authentication (e.g., is attempting to biometrically authenticate the user using biometric sensor 903). Displaying interstitial interface 1314A includes ceasing to display unlock indication 905. In some examples, displaying interstitial interface 1314A includes sliding the locked state UI 1300A in an upward direction to display (e.g., reveal) interstitial interface 1314A.

[0373] Further in response to detecting the request to unlock the device, electronic device 900 determines whether the error condition is still occurring. Upon a determination that the error condition is still occurring at a time immediately after the request to unlock the device, electronic device 900 maintains display of location indication 1304A and initially displays location indication 1318. Electronic device 900 displays location indication 1318 at a location on display 902 that is adjacent to biometric sensor 903 such that location indication 1318 is pointing at biometric sensor 903. As depicted in FIGS. 13C-13D, location indication 1318 includes a visual arrow that is animated in a manner where it appears to bounce near biometric sensor 903. Similar to location indication 1304A, location indication 1318 is a prompt to the user to take an action that corrects the error condition. For example, upon seeing location indication 1318, a user turns their head toward biometric sensor 903 such that their face is substantially directed to (or facing) biometric sensor 903.

[0374] At FIG. 13E, upon a determination that the error condition is still occurring after a predetermined amount of time has elapsed (e.g., 1, 3, or 5 seconds since receiving the request and/or since displaying the interstitial interface 1314A) and/or a determination that biometric authentication has not successfully completed, electronic device 900 displays (e.g., replaces display of interstitial interface 1314 with) passcode entry UI 1320A. Passcode entry UI 1320A includes a plurality of entry affordances for entering a passcode (or password). Displaying passcode entry UI 1320A includes again initially displaying unlock indication 905 and maintaining display of lock icon 1302. Further upon a determination that the error condition is still occurring after a predetermined amount of time has elapsed, electronic

device 900 ceases displaying location indication 1304A. In some examples, upon a determination that the error condition is still occurring (e.g., immediately after detecting the request to unlock the device, after a predetermined amount of time has elapsed (e.g., 1, 3, or 5 seconds since receiving the request and/or since displaying the interstitial interface 1314A)) and/or a determination that biometric authentication has not successfully completed, electronic device 900 forgoes attempting to unlock the device and/or attempting to biometrically authenticate the user.

[0375] At FIG. 13F, electronic device 900 continues to determine whether the error condition is still occurring while displaying passcode entry UI 1320A. The user turns their head to a new orientation in which the user's face is substantially facing biometric sensor 903 (e.g., the user looks down to begin entering their passcode). Due to the turning of the user's head, electronic device 900 determines that the error condition is no longer occurring. In particular, electronic device 900 determines that a potentially valid biometric feature is substantially facing biometric sensor 903. In some examples, the user can correct the detected error condition by turning the user's face toward biometric sensor 903, or re-orienting the device to a new orientation in which the user's face is substantially facing biometric sensor 903 (e.g., rotating the device so that a face detection sensor is on a right edge, left edge, or top edge of the device as opposed to being on a bottom edge of the device).

[0376] Upon a determination that the error condition is no longer occurring, electronic device 900 attempts to unlock the device using biometric sensor 903. Upon a determination that the captured information about the user's face corresponds to stored authorized credentials, electronic device 900 transitions from a locked state to an unlocked state. Transitioning to an unlocked state includes displaying (e.g., replacing display of lock icon 1302 with) unlock icon 1322, which provides an indication that electronic device 900 has successfully been unlocked. Transitioning to an unlocked state further includes displaying (e.g., replacing display of passcode entry UI 1320A with) home screen 1324A of FIG. 13G or a most recently used application, or an application selected based on other criteria (such as an application corresponding to a selected or recently received notification or an application that the user was using on another related device). In some examples, attempting to unlock the device includes attempting to biometrically authenticate a user. Attempting to biometrically authenticate the user using biometric sensor 903 includes attempting to capture information about a potentially valid biometric feature (e.g., a biometric feature that can be used for

biometric authentication) using biometric sensor 903 and/or determining whether the captured information about the potentially valid biometric feature corresponds to, or matches, stored authorized credentials (e.g., a biometric template). In some examples, attempting to capture information about a potentially valid biometric feature includes powering on biometric sensor 903. In some examples, electronic device 900 determines whether captured information about a potentially valid biometric feature matches stored authorized credentials if, or when, electronic device 900 successfully captures information about a potentially valid biometric feature. In some examples, if electronic device 900 does not, or fails to, capture information about a potentially valid biometric feature, electronic device 900 forgoes determining whether captured information about a potentially valid biometric feature matches stored authorized credentials.

[0377] Upon a determination that the captured information about the user's face does not correspond to stored authorized credentials, electronic device 900 maintains the locked state. For example, electronic device 900 maintains display of passcode entry UI 1320A with lock icon 1302, as depicted in FIG. 13E.

[0378] As described above with respect to FIGS. 13A-13D, the user does not correct the error condition while electronic device 900 displays locked state UI 1300A and/or interstitial UI 1314A. In some examples, instead of failing to correct the error condition in FIGS. 13A-13D, the user corrects the error condition by turning their head to a new orientation in which the user's face is substantially facing biometric sensor 903, as depicted in FIG. 13H. While location indication 1304A of FIGS. 13A-13D is displayed (e.g., after detecting a request to perform an operation that requires authentication, after detecting a request to unlock the device, and/or before passcode entry UI 1320A is displayed), electronic device 900 determines whether the error condition is still occurring. In some examples, electronic device 900 determines that the error condition is no longer occurring. In particular, electronic device 900 determines that a potentially valid biometric feature is substantially facing biometric sensor 903. Upon a determination that the error condition is no longer occurring, electronic device 900 attempts to unlock the device using biometric sensor 903.

[0379] In some examples, upon a determination that the captured information about the user's face does not correspond to stored authorized credentials, electronic device 900 maintains the locked state. For example, electronic device 900 displays (e.g., replaces display of interstitial interface 1314 with) passcode entry UI 1320A of FIG. 13E.

[0380] In some examples, the user does not correct the error condition and/or otherwise fails to successfully complete biometric authentication. Instead, while displaying passcode entry 1320A of FIG. 13E, electronic device 900 receives, via display 902, a sequence of one or more characters that corresponds to a password or passcode, as depicted in FIG. 13I. As an example, electronic device 900 receives character input 1326, which is a portion of the sequence of one or more characters.

[0381] At FIG. 13J, in some examples, upon a determination that the sequence of one or more characters corresponds to stored authorized credentials, electronic device 900 transitions from a locked state to an unlocked state. Transitioning to an unlocked state can include displaying (e.g., replacing display of lock icon 1302 with) unlock icon 1322, which provides an indication that electronic device 900 has successfully been unlocked. Transitioning to an unlocked state can include displaying (e.g., replacing display of passcode entry UI 1320A with) home screen 1324A of FIG. 13G or the most recently used application.

[0382] In some examples, upon a determination that the sequence of one or more characters does not correspond to stored authorized credentials, electronic device 900 maintains the locked state. For example, electronic device 900 maintains display of passcode entry UI 1320A of FIG. 13E.

[0383] FIGS. 13K-13P illustrate another scenario where electronic device 900 detects an error condition while attempting to unlock the device using biometric sensor 903. FIGS. 13K depicts processes that are analogous to the processes described above with respect to FIGS. 13A. To initiate the process of accessing restricted content on electronic device 900, the user lifts (or raises) electronic device 900 (e.g., from a substantially horizontal orientation to the orientation of the device as depicted in the user's hand in FIG. 13K). In some examples, due to the change in orientation of the device, electronic device 900 detects (e.g., via accelerometer 168) a request to perform an operation that requires authentication (e.g., a request to unlock the device). In response to detecting the request to unlock the device, electronic device 900 attempts to biometrically authenticate the user using biometric sensor 903.

[0384] In some examples, while attempting to biometrically authenticate the user using biometric sensor 903, electronic device 900 detects that an error condition has occurred. In some examples, detecting that an error condition has occurred requires determining that

biometric sensor 903 is occluded (e.g., by the user's hand). Because biometric sensor 903 is occluded at FIG. 13K, electronic device 900 is unable to capture information about the user's face. Accordingly, electronic device 900 has no captured information for biometrically authenticating the user. The user can correct the detected error condition by moving their hand away from biometric sensor 903 such that biometric sensor 903 is no longer occluded.

[0385] In some examples, in response to detecting that an error condition has occurred, electronic device 900 maintains a locked state. In some examples, further in response to detecting that an error condition has occurred, electronic device 900 initially displays location indication 1304B (e.g., location indication 1304B were not displayed prior to detecting the error condition). In some examples, location indication 1304B includes an indication of the location of biometric sensor 903 on the device. In some examples, electronic device 900 displays location indication 1304B at a location on display 902 that is adjacent to biometric sensor 903. In some examples, location indication 1304B includes a visual indication (e.g., text, arrow) describing or indicating the location of biometric sensor 903. For example, location indication 1304B can be an animated arrow, as described above with respect to location indication 1318 in FIGS. 13C-13D. In some examples, electronic device 900 displays location indication 1304C of FIG. 13Y in addition to or instead of location indication 1304B. In some examples, location indication 1304C includes some or all of the features of error indication 928 of FIGS. 9E-9I. In some examples, electronic device 900 displays location indication 1304D of FIG. 13Z in addition to or instead of location indication 1304B. In some examples, location indication 1304D includes a text description of the location of biometric sensor 903 (e.g., with respect to the user and/or with respect to location indication 1304D).

[0386] In some examples, further in response to detecting that an error condition has occurred, electronic device 900 initially displays error indication 1328. In some examples, electronic device 900 displays error indication 1328 adjacent to lock icon 1302. In some examples, error indication 1328 includes an indication of the cause of the error condition. In some examples, error indication 1328 includes an indication of a user action that can be performed to correct the detected error condition (e.g., for a subsequent biometric authentication attempt).

[0387] FIG. 13L depicts processes that are analogous to the processes described above with respect to FIG. 13B. At FIG. 13L, the user still wishes to access restricted content on

electronic device 900, so the user attempts to unlock the device via a swipe gesture despite not having corrected the error condition. In some examples, while displaying locked state UI 1300B with location indication 1304B, electronic device 900 detects a request to unlock the electronic device using biometric sensor 903. Detecting a request to unlock the device includes receiving input 1312B starting at a location of display 902, and determining that input 1312B is an upward swipe gesture that starts within a predefined region adjacent to the bottom edge of display 902. Locked state UI 1300B is a landscape version of locked state UI 1300A, and includes some or all of the feature of locked state UI 1300A.

[0388] FIG. 13M depicts processes that are analogous to the processes described above with respect to FIG. 13C. At FIG. 13M, in some examples, in response to detecting the request to unlock the device, electronic device 900 displays (e.g., replaces display of locked state UI 1300B with) interstitial interface 1314B. Interstitial interface 1314B is a landscape version of interstitial interface 1314A, and includes some or all of the features of interstitial interface 1314A.

[0389] Further in response to receiving the request to unlock the device, electronic device 900 determines whether the error condition is still occurring. Upon a determination that the error condition is still occurring at a time immediately after the request to unlock the device, electronic device 900 maintains display of location indication 1304B.

[0390] FIG. 13N depicts processes that are analogous to the processes described above with respect to FIG. 13I. At FIG. 13N, in some examples, upon a determination that the error condition is still occurring after a predetermined amount of time has elapsed (e.g., 1, 3, or 5 seconds), electronic device 900 displays (e.g., replaces display of interstitial interface 1314B with) passcode entry UI 1320B. Passcode entry UI 1320B is a landscape version of passcode entry UI 1320A, and includes some or all of the features of passcode entry UI 1320A.

[0391] In some examples, the user does not correct the error condition. Instead, while displaying passcode entry 1320B of FIG. 13N, electronic device 900 receives, via display 902, a sequence of one or more characters that corresponds to a password or passcode. As an example, electronic device 900 receives character input 1330, which is a portion of the sequence of one or more characters.

[0392] FIG. 13O depicts processes that are analogous to the processes described above with respect to FIG. 13J. At FIG. 13J, in some examples, upon a determination that the sequence of one or more characters corresponds to stored authorized credentials, electronic device 900 transitions from a locked state to an unlocked state. Transitioning to an unlocked state can include displaying (e.g., replacing display of lock icon 1302 with) unlock icon 1322, which provides an indication that electronic device 900 has successfully been unlocked. Transitioning to an unlocked state can include displaying (e.g., replacing display of passcode entry UI 1320B with) home screen 1324B of FIG. 13P or the most recently used application.

[0393] In some examples, upon a determination that the sequence of one or more characters does not correspond to stored authorized credentials, electronic device 900 maintains the locked state. For example, electronic device 900 maintains display of passcode entry UI 1320B of FIG. 13N.

[0394] At FIG. 13Q, in some examples, while in a locked state, electronic device 900 detects the occurrence of a type of error condition that is different from the type of error conditions detected in FIGS. 13A and 13K, as described above. The error conditions detected in FIGS. 13A and 13K are of the type where the location of biometric sensor 903 would be especially useful for the user to know in order to correct the error condition. In some examples, while attempting to biometrically authenticate the user using biometric sensor 903, electronic device 900 detects an error condition of a different type (e.g., a type where knowledge of the location of biometric sensor 903 is not especially useful). At FIG. 13Q, electronic device 900 detects that the biometric feature is outside acceptable distance range 1303 (e.g., too far from biometric sensor 903). In response to detecting an error condition of a different type, electronic device 900 displays error indication 1332, which includes some or all of the features of error indication 714A in FIG. 7G. Further in response to detecting an error condition of a different type, electronic device 900 forgoes displaying an indication of the location of biometric sensor 903.

[0395] FIGS. 13R-13T illustrate a scenario where electronic device 900 detects an error condition while attempting to make a payment using biometric sensor 903. Similar to unlocking a device, as described above with respect to FIG. 13A, making a payment requires successful authentication of the user.

[0396] At FIG. 13R, a user wishes to purchase some items from an online retail store. In some examples, while displaying webpage 1334 of a browsing application, electronic device 900 detects a request to perform an operation that requires authentication (e.g., a request to make a payment to purchase an item). Specifically, electronic device 900 detects activation of a purchase affordance via input 1336.

[0397] In some examples, upon detecting the request to make a payment, electronic device 900 attempts to biometrically authenticate the user using biometric sensor 903. In some examples, while attempting to biometrically authenticate the user using biometric sensor 903, electronic device 900 detects that an error condition has occurred. Similar to the error condition detected with respect to FIG. 13A, electronic device 900 determines that a potentially valid biometric feature is not substantially facing biometric sensor 903. In some examples, further upon detecting the request to make a payment, electronic device 900 displays pay sheet interface 1338, which overlaps (e.g., partially overlaps) webpage 1334.

[0398] At FIG. 13S, upon detecting that an error condition has occurred, electronic device 900 initially displays location indication 1304E. In some examples, electronic device 900 displays location indication 1304E at a location on display 902 that is adjacent to biometric sensor 903 such that location indication 1304E is pointing at biometric sensor 903. In some examples, location indication 1304E is an animated arrow, as described above with respect to location indication 1318 in FIGS. 13C-13D.

[0399] Electronic device 900 continues to determine whether the error condition is still occurring while displaying location indication 1304E. Prompted by location indication 1304E, the user turns their head downward to a new orientation in which the user's face is substantially facing biometric sensor 903, as shown in FIG. 13T. Due to the turning of the user's head, electronic device 900 determines that the error condition is no longer occurring. In particular, electronic device 900 determines that a potentially valid biometric feature is substantially facing biometric sensor 903.

[0400] In some examples, upon a determination that the error condition is no longer occurring, electronic device 900 attempts to make a payment using biometric sensor 903. In some examples, upon a determination that the captured information about the user's face corresponds to stored authorized credentials, electronic device 900 makes the payment, as shown in FIG. 13T. In some examples, upon a determination that the captured information

about the user's face does not correspond to stored authorized credentials, electronic device 900 forgoes making the payment.

[0401] FIGS. 13U-13X illustrate a scenario where electronic device 900 detects an error condition while attempting to biometrically authenticate using biometric sensor 903, as a precursor to autofilling fillable fields (e.g., username field, password field) using stored information. Similar to unlocking a device, as described above with respect to FIG. 13A, autofilling fillable fields requires successful authentication of the user.

[0402] At FIG. 13U, a user wishes to autofill the username field and password field using stored log-in information. In some examples, while displaying log-in UI 1340 of a mobile application, electronic device 900 detects a request to perform an operation that requires authentication (e.g., a request to autofill). Specifically, electronic device 900 detects activation of an autofill affordance via input 1342.

[0403] In some examples, upon detecting the request to autofill fillable fields, electronic device 900 attempts to biometrically authenticate the user using biometric sensor 903. In some examples, while attempting to biometrically authenticate the user using biometric sensor 903, electronic device 900 detects that an error condition has occurred. Similar to the error condition detected with respect to FIG. 13A, electronic device 900 determines that a potentially valid biometric feature is not substantially facing biometric sensor 903.

[0404] At FIG. 13V, upon detecting that an error condition has occurred, electronic device 900 initially displays location indication 1304E. In some examples, electronic device 900 displays location indication 1304E at a location on display 902 that is adjacent to biometric sensor 903 such that location indication 1304E is pointing at biometric sensor 903. In some examples, location indication 1304E is an animated arrow, as described above with respect to location indication 1318 in FIGS. 13C-13D.

[0405] Electronic device 900 continues to determine whether the error condition is still occurring while displaying location indication 1304E. Prompted by location indication 1304E, the user turns their head downward to a new orientation in which the user's face is substantially facing biometric sensor 903. Due to the turning of the user's head, electronic device 900 determines that the error condition is no longer occurring. In particular, electronic

device 900 determines that a potentially valid biometric feature is substantially facing biometric sensor 903.

[0406] In some examples, upon a determination that the error condition is no longer occurring, electronic device 900 attempts to autofill the fillable fields using biometric sensor 903. At FIG. 13W, electronic device 900 determines that the captured information about the user's face corresponds to stored authorized credentials. In some examples, upon a determination that the captured information about the user's face corresponds to stored authorized credentials, electronic device 900 autofills the fillable fields, as shown in FIG. 13X. In some examples, autofilling the fillable fields includes automatically logging in the user. In some examples, the user must manually log-in by activating a displayed affordance for signing in the user (e.g., the device detects a request to log-in the user after the fillable fields are autofilled). In some examples, upon a determination that the captured information about the user's face does not correspond to stored authorized credentials, electronic device 900 forgoes autofilling the fillable fields.

[0407] FIGS. 14A-14B are flow diagrams illustrating a method for prompting a user to correct an error condition that is detected while attempting to biometrically authenticate the user, in accordance with some examples. Method 1400 is performed at an electronic device (e.g., 900) with a display (e.g., 902) and one or more biometric sensors (e.g., 903) (e.g., a first biometric sensor of a device with a plurality of biometric sensors) (e.g., a fingerprint sensor, a contactless biometric sensor (e.g., a biometric sensor that does not require physical contact, such as a thermal or optical facial recognition sensor), an iris scanner). In some examples, the one or more biometric sensors include one or more cameras. Some operations in method 1400 are, optionally, combined, the orders of some operations are, optionally, changed, and some operations are, optionally, omitted.

[0408] As described below, method 1400 provides an intuitive way for prompting a user to correct an error condition that is detected while attempting to biometrically authenticate the user. The method reduces the cognitive burden on a user performing biometric authentication, thereby creating a more efficient human-machine interface. For battery-operated computing devices, enabling a user to perform biometric authentication faster and more efficiently conserves power and increases the time between battery charges.

[0409] The electronic device (e.g., 900) with a biometric sensor (e.g., 903) and a touch-sensitive display (e.g., 902) detects (1402) occurrence of an error condition (e.g., biometric sensor is partially occluded or covered, fully occluded, occluded to a degree sufficient to inhibit operation of the sensor, biometric sensor is occluded by a portion of the user (e.g., a hand) while interacting with the electronic device, the biometric sensor is not directed to a portion of a biometric feature (e.g., face) that can be used for biometric authentication, the biometric feature is turned away from the biometric sensor, the biometric feature is not oriented such that it is substantially facing the biometric sensor) for detecting biometric information (e.g., information about, or corresponding to, a biometric feature) at the biometric sensor. In some examples, the user can correct the error condition by moving the user's hand away from the biometric sensor. In some examples, the user can correct the error condition by turning the user's face toward the biometric sensor and/or tilting/rotating the device (e.g., 900) so that the biometric sensor is in a position and/or orientation in which the biometric feature is substantially facing the biometric sensor. In some examples, the device detects occurrence of an error condition while the device is in a locked state. In some examples, detecting occurrence of an error condition is, or includes, determining that a set of one or more error condition criteria has been met. In some examples, detecting occurrence of an error condition is, or includes, determining that an error condition has occurred.

[0410] In some examples, the occurrence of the error condition (e.g., error condition criteria) includes a requirement (1404) that the biometric sensor (e.g., 903) is covered in order for the error condition to occur. In some examples, the occurrence of the error condition (e.g., error condition criteria) includes a requirement that the display (e.g., 902) is on for the error condition to occur. In some examples, the occurrence of the error condition (e.g., error condition criteria) includes a requirement that an input (e.g., 1312A-B, 1336, 1342) corresponding to a request to attempt biometric authentication (e.g., a request to perform an operation that requires authentication) has been met in order for the error condition to occur (e.g., an upward swipe, tilting device upward, waking device by pressing a button (e.g., 904) or tapping on the screen (e.g., display 902), tapping on screen when the display is on, activating an affordance, etc.).

[0411] In some examples, the occurrence of the error condition (e.g., error condition criteria) includes a requirement that a maximum number (e.g., a predetermined number) of failed authentication attempts has not yet been reached in order for the error condition to

occur (e.g., the device allows only a respective number of failed authentication attempts before non-biometric authentication (e.g., password, passcode, or pattern) is required to unlock the device). In some examples, the occurrence of the error condition (e.g., error condition criteria) includes a requirement (1406) that the electronic device (e.g., 900) is oriented so that the biometric sensor (e.g., 903) is not directed to a portion of the biometric feature that can be used for biometric authentication in order for the error condition to occur. In some examples, in this orientation, the biometric sensor is located at (or adjacent or near) the bottom edge of the device. Requiring that a maximum number of failed authentication attempts has not yet been reached in order to detect the error condition reduces the instances of multiple resource-intensive re-attempts of biometric authentication that is likely to fail due to the error condition. This, in turn, reduces power usage and improves battery life of the device by limiting the performance of operations that are likely to fail.

[0412] In some examples, the occurrence of the error condition is detected when the error condition is of a first type (e.g., biometric sensor is partially occluded (or covered), fully occluded, occluded to a degree sufficient to inhibit operation of the sensor, biometric sensor is occluded by a portion of the user (e.g., a hand), while interacting with the electronic device, the biometric sensor is not directed to a portion of a biometric feature (e.g., face) that can be used for biometric authentication, the biometric feature is turned away from the biometric sensor, the biometric feature is not oriented such that it is substantially facing the biometric sensor). In some examples, the user can correct the error condition by moving the user's hand away from the biometric sensor. In some examples, the user can correct the error condition by turning the user's face toward the biometric sensor and/or tilting/rotating the device so that the biometric sensor is in a position (or orientation) in which the biometric feature is substantially facing the biometric sensor. In some examples, in response to detecting occurrence of a second type of error condition (e.g., error conditions different from the first type), the electronic device displays an indication (e.g., 1332) of the occurrence of the second type of error condition (e.g., information about the cause of the error condition (e.g., device too far away, device too close)) without displaying an indication (e.g., 1304A-E), of the location of the biometric sensor.

[0413] In response to (e.g., subsequent to) detecting the occurrence of the error condition, the electronic device (e.g., 900) displays (1408), on the touch-sensitive display (e.g., 902), an indication (e.g., 1304A-E) of a location of the biometric sensor (e.g., 903) on the electronic

device (e.g., a textual indication (e.g., 1304A, 1304D) (e.g., text stating "look down"), a graphical, visual, or pictorial indication (e.g., 1304B-C, 1304E) (e.g., a visual object (e.g., arrow or other shape) that is static or animated (e.g., moves back and forth between two positions of the user interface, a bouncing object))). In some examples, in response to (e.g., subsequent to) detecting the occurrence of the error condition, the electronic device forgoes determining whether captured biometric information about a biometric feature corresponds to (or matches) stored authorized credentials (e.g., a biometric template).

[0414] In some examples, the indication of the location of the biometric sensor includes an indication (e.g., 1304A-1304E) of a user action that can be performed to correct the error condition (e.g., for a subsequent authentication attempt). In some examples, the indication of the user action indicates how to correct the error condition for a subsequent authentication attempt. Displaying an indication of a user action that can be performed to correct the error condition provides feedback to the user as to what course of action to take so that the user can be biometrically authenticated in a subsequent authentication attempt. Providing improved visual feedback to the user enhances the operability of the device and makes the user-device interface more efficient (e.g., by helping the user to provide proper inputs and reducing user mistakes when operating/interacting with the device) which, additionally, reduces power usage and improves battery life of the device by enabling the user to use the device more quickly and efficiently.

[0415] In some examples, the indication (e.g., 1304A-E) is located near (e.g., adjacent to) the biometric sensor. In some examples, the indication includes an instruction (1410) (e.g., 1304A) to change a pose (e.g., orientation) of the biometric feature toward the biometric sensor (e.g., textual indication (e.g., "look down")). In some examples, the indication includes a text description (1412) (e.g., 1304D) of where the biometric sensor is located (e.g., face sensor to right, face sensor to left, face sensor down)). In some examples, the indication includes a graphical indication (e.g., 1304B-C, 1304E) located near (e.g., adjacent to) the biometric sensor. In some examples, the indication includes a pictorial illustration (e.g., 1304B, 1304E) of a location of the biometric sensor (e.g., an object (e.g., arrow or other shape) pointing toward the sensor). In some examples, the indication (e.g., 1304A-E) includes an animation that illustrates a location of the biometric sensor (e.g., an object bouncing or sliding toward the sensor, an animation pulsing or glowing near the sensor). Displaying the indication near the biometric sensor provides feedback to the user of the

location of the device that is the source of the error condition. By displaying the indication near the biometric sensor, the user is prompted to remove their hand from the biometric sensor to correct the error condition. Providing improved visual feedback to the user enhances the operability of the device and makes the user-device interface more efficient (e.g., by helping the user to provide proper inputs and reducing user mistakes when operating/interacting with the device) which, additionally, reduces power usage and improves battery life of the device by enabling the user to use the device more quickly and efficiently. In some examples, no indicator is displayed during biometric authentication. Displaying a pictorial illustration of the location of the biometric sensor provides feedback to the user of the location of the device that is the source of the error condition. By displaying a pictorial illustration of the location of the biometric sensor, the user is prompted to remove their hand from the biometric sensor to correct the error condition. Providing improved visual feedback to the user enhances the operability of the device and makes the user-device interface more efficient (e.g., by helping the user to provide proper inputs and reducing user mistakes when operating/interacting with the device) which, additionally, reduces power usage and improves battery life of the device by enabling the user to use the device more quickly and efficiently. In some examples, no indicator is displayed during biometric authentication.

[0416] While displaying the indication (e.g., 1304A-E) of the location of the biometric sensor (e.g., 903) on the electronic device (e.g., 900), the electronic device detects (1414) a request to unlock the electronic device using the biometric sensor (e.g., the request corresponds to a touch gesture input (e.g., 1312A-B) (e.g., swipe gesture (e.g., a contact that exceeds a threshold distance in a horizontal or vertical direction)), the request corresponds to a contact starting from an edge (e.g., bottom edge) of the display (e.g., 902) or starting from within a predefined region (e.g., lower portion) of the display). In some examples, the request corresponds to a touch gesture input (e.g., 1312A-B) starting at a first region of the display (e.g., a region along a bottom edge of the display) and ends (or progresses through) a second region of the display (e.g., a region above the region along the bottom edge of the display).

[0417] In response to (e.g., subsequent to) detecting the request to unlock the electronic device (e.g., 900) using the biometric sensor (e.g., 903): in accordance with a determination that the error condition is still occurring at a respective time that occurs after detecting the request to unlock the electronic device (e.g., a time immediately after detecting the request to

unlock the electronic device or a respective time that occurs after a delay time period such as 1, 3, or 5 seconds has elapsed): the electronic device ceases (1416) to display the indication (e.g., 1304A-E) of the location of the biometric sensor; and displays (1416) a touch-based user interface (e.g., 1320A-B) for entering touch-based authentication information (e.g., a password, passcode, swipe pattern). In some examples, while displaying the touch-based user-interface, the electronic device determines that the error condition is no longer occurring. In some examples, in accordance with a determination that the error condition is no longer occurring, the electronic device attempts to unlock the electronic device using the biometric sensor. In some examples, a determination that a set of one or more error condition criteria is still being met is (or includes) a determination that the error condition is still occurring.

[0418] Ceasing to display the indication (e.g., text stating "look down") of the location of the biometric sensor after detecting a request to unlock the device improves feedback to the user by removing potential confusion resulting from displaying both the indication of the location of the biometric sensor and the passcode entry user interface. For example, if the electronic device were to continue displaying the indication of the location of the biometric sensor while also displaying, for example, a passcode entry user interface, the user is likely to become confused as to what action to take in order to perform biometric authentication (e.g., look down or enter passcode). Providing improved feedback to the user enhances the operability of the device and makes the user-device interface more efficient (e.g., by helping the user to provide proper inputs and reducing user mistakes when operating/interacting with the device) which, additionally, reduces power usage and improves battery life of the device by enabling the user to use the device more quickly and efficiently.

[0419] Automatically displaying a touch-based user interface in accordance with a determination that the error condition is still occurring provides a user the ability to attempt non-biometric authentication when the conditions are appropriate without requiring the user to explicitly request performing non-biometric authentication. Performing an operation when a set of conditions has been met without requiring further user input enhances the operability of the device (e.g., directs the user to the action needed to authenticate) and makes the user-device interface more efficient (e.g., by helping the user to provide proper inputs and reducing user mistakes when operating/interacting with the device) which, additionally,

reduces power usage and improves battery life of the device by enabling the user to use the device more quickly and efficiently.

[0420] In some examples, while displaying the touch-based user interface (e.g., 1320A-B) for entering touch-based authentication information, the electronic device detects a touch input sequence (e.g., a sequence of one or more inputs (e.g., 1326, 1330) corresponding to one or more characters, a sequence of one or more characters) on the touch-sensitive display (e.g., for inputting a password, passcode, or swipe pattern). In some examples, in response to detecting the touch input sequence: in accordance with a determination that the touch input sequence matches authorized credentials (e.g., stored authorized credentials, password, passcode, swipe pattern), the electronic device transitions the electronic device from a locked state to an unlocked state. In some examples, in response to detecting the touch input sequence: in accordance with a determination that the touch input sequence does not match authorized credentials, the electronic device maintains the electronic device in a locked state.

[0421] In some examples, the respective time is a time that occurs (1418) after a predetermined delay time period from when the request to unlock the electronic device using the biometric sensor was detected.

[0422] In response to (e.g., subsequent to) detecting the request to unlock the electronic device (e.g., 900) using the biometric sensor (e.g., 903): in accordance with a determination that the error condition is no longer occurring (e.g., the error condition has been corrected), the electronic device attempts (1420) to unlock the electronic device using the biometric sensor (e.g., comparing the information captured by the biometric sensor with stored authorized credentials (e.g., a biometric template associated with the user)). In some examples, if the captured information matches, within a threshold time period, the stored authorized credentials, the device transitions from a locked state to an unlocked state. In some examples, if the captured information does not match, within the threshold, the stored authorized credentials, the device maintains the locked state and/or displays the touch-based interface (e.g., 1320A-B) for entering touch-based authentication information. In some examples, attempting to unlock the electronic device via biometric authentication occurs without displaying the touch-based user interface for entering touch-based authentication information. In some examples, a determination that a set of one or more error condition criteria is no longer being met is (or includes) a determination that the error condition is no longer occurring. In some examples, the determination that the error condition is no longer

occurring can be made at any time up to the respective time that occurs after detecting the request to unlock the electronic device. Automatically attempting to unlock the electronic device in accordance with a determination that the error condition is no longer occurring improves the chance of success of the attempt to unlock the device. For example, the device performs the attempt immediately after the device detects that the error condition has been corrected. Performing an optimized operation when a set of conditions has been met without requiring further user input enhances the operability of the device and makes the user-device interface more efficient (e.g., by helping the user to provide proper inputs and reducing user mistakes when operating/interacting with the device) which, additionally, reduces power usage and improves battery life of the device by enabling the user to use the device more quickly and efficiently.

[0423] In some examples, attempting to unlock the electronic device (e.g., 900) includes: in accordance with a determination that biometric authentication is successful (e.g., information captured using the biometric sensor (e.g., 903) matches or corresponds to stored authorized credentials), unlocking the electronic device (e.g., transitioning the device from a locked state to an unlocked state). In some examples, attempting to unlock the electronic device includes: in accordance with a determination that biometric authentication is not successful (e.g., information captured using the biometric sensor (e.g., 903) does not match or correspond to stored authorized credentials), displaying, on the touch-sensitive display (e.g., 902), an alternative authentication user interface (e.g., 1320A-B) (e.g., the touch-based user interface for entering touch-based authentication information (e.g., a password, passcode, swipe pattern). In some examples, further in accordance with a determination that biometric authentication is not successful, the electronic device maintains a locked state. In some examples, attempting to unlock the electronic device includes attempting to biometrically authenticate the user using the biometric sensor.

[0424] In some examples, the determination that the error condition is no longer occurring is made (1422) subsequent to detecting the request to unlock the electronic device (e.g., 900) using the biometric sensor (e.g., 903) (e.g., after detecting the request to unlock but before the predetermined amount of time lapses) and while displaying the indication (e.g., 1304A-E) of the location of the biometric sensor.

[0425] Note that details of the processes described above with respect to method 1400 (e.g., FIGS. 14A-14B) are also applicable in an analogous manner to the methods described

above. For example, method 800, method 1000, and/or method 1200 optionally include one or more of the characteristics of the various methods described above with reference to method 1400. For example, displaying the indication of the location of the biometric sensor, as described in method 1400, can be performed in method 800, method 1000, and method 1200 in response to detecting an error condition. For brevity, these details are not repeated below.

[0426] 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.

[0427] 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.

[0428] One aspect of the present technology is the gathering and use of data available from various sources to improve the delivery to users of invitational content or any other content that may be of interest to them. 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, twitter 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.

[0429] The present disclosure recognizes that the use of such personal information data, in the present technology, can be used to the benefit of users. For example, the personal information data can be used to deliver targeted content that is of greater interest to the user.

Accordingly, use of such personal information data enables users to calculated control of the delivered content. 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.

[0430] 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.

[0431] 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, in the case of advertisement delivery services, 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 during registration for services or anytime thereafter. In another example, users can select not to provide mood-associated data for targeted content delivery services. In yet another example, users can select to limit the length of time mood-associated data is maintained or entirely prohibit the development of a baseline mood profile. 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.

[0432] 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.

[0433] 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, content can be selected and delivered to users by inferring preferences based on 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 available to the content delivery services, or publicly available information.

What is claimed is:

1. A method, comprising:

at an electronic device with a biometric sensor and a touch-sensitive display:

detecting occurrence of an error condition for detecting biometric information at the biometric sensor;

in response to detecting the occurrence of the error condition, displaying, on the touch-sensitive display, an indication of a location of the biometric sensor on the electronic device, wherein the indication is a graphical indicator that is displayed at a respective location on the touch-sensitive display that is a first distance from a first edge of the electronic device, wherein the first edge of the electronic device corresponds to the location of the biometric sensor on the electronic device, and wherein the respective location on the touch-sensitive display is a second distance from a second edge of the electronic device, wherein the second edge is opposite from the first edge, and wherein the second distance is greater than the first distance;

while displaying the indication of the location of the biometric sensor on the electronic device, detecting a request to unlock the electronic device using the biometric sensor; and

in response to detecting the request to unlock the electronic device using the biometric sensor:

in accordance with a determination that the error condition is still occurring at a respective time that occurs after detecting the request to unlock the electronic device:

ceasing to display the indication of the location of the biometric sensor; and

displaying a touch-based user interface for entering touch-based authentication information; and

in accordance with a determination that the error condition is no longer occurring, attempting to unlock the electronic device using the biometric sensor.

2. The method of claim 1, further comprising:

2022279466 18 Dec 2023

while displaying the touch-based user interface for entering touch-based authentication information, detecting a touch input sequence on the touch-sensitive display;

in response to detecting the touch input sequence:

in accordance with a determination that the touch input sequence matches authorized credentials, transitioning the electronic device from a locked state to an unlocked state; and

in accordance with a determination that the touch input sequence does not match authorized credentials, maintaining the electronic device in a locked state.

3. The method of any one of claims 1-2, wherein the respective time is a time that occurs after a predetermined delay time period from when the request to unlock the electronic device using the biometric sensor was detected.

4. The method of any one of claims 1-3, wherein attempting to unlock the electronic device includes:

in accordance with a determination that biometric authentication is successful, unlocking the electronic device; and

in accordance with a determination that biometric authentication is not successful, displaying, on the touch-sensitive display, an alternative authentication user interface.

5. The method of any one of claims 1-4, wherein the occurrence of the error condition includes a requirement that the biometric sensor is covered in order for the error condition to occur.

6. The method of any one of claims 1-5, wherein the occurrence of the error condition includes a requirement that the touch-sensitive display is on for the error condition to occur.

7. The method of any one of claims 1-6, wherein the occurrence of the error condition includes a requirement that an input corresponding to a request to attempt biometric authentication has been met in order for the error condition to occur.

2022279466 18 Dec 2023

8. The method of any one of claims 1-7, wherein the occurrence of the error condition includes a requirement that a maximum number of failed authentication attempts has not yet been reached in order for the error condition to occur.

9. The method of any one of claims 1-8, wherein the occurrence of the error condition includes a requirement that the electronic device is oriented so that the biometric sensor is not directed to a portion of a biometric feature that can be used for biometric authentication in order for the error condition to occur.

10. The method of any one of claims 1-9, wherein the indication includes an instruction to change a pose of a biometric feature toward the biometric sensor.

11. The method of any one of claims 1-10, wherein the indication includes a text description of where the biometric sensor is located.

12. The method of any one of claims 1-11, wherein the indication includes a pictorial illustration of a location of the biometric sensor.

13. The method of any one of claims 1-12, wherein the indication includes an animation that illustrates a location of the biometric sensor.

14. The method of any one of claims 1-13, wherein the occurrence of the error condition is detected when the error condition is of a first type, the method further comprising:

in response to detecting occurrence of a second type of error condition, displaying an indication of the occurrence of the second type of error condition without displaying an indication of the location of the biometric sensor.

2022279466 18 Dec 2023

15. The method of any one of claims 1-14, wherein the request to unlock the electronic device using the biometric sensor is detected via the touch-sensitive display.

16. The method of any one of claims 1-15, wherein using the biometric sensor includes obtaining data that corresponds to facial features.

17. The method of any one of claims 1-16, wherein the determination that the error condition is no longer occurring is made subsequent to detecting the request to unlock the electronic device using the biometric sensor and while displaying the indication of the location of the biometric sensor.

18. A computer-readable storage medium storing one or more programs configured to be executed by one or more processors of an electronic device with a biometric sensor and a touch-sensitive display, the one or more programs including instructions for performing the method of any one of claims 1-17.

19. An electronic device, comprising:

a biometric sensor;

a touch-sensitive display;

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 one of claims 1-17.

2022279466 30 Nov 2022

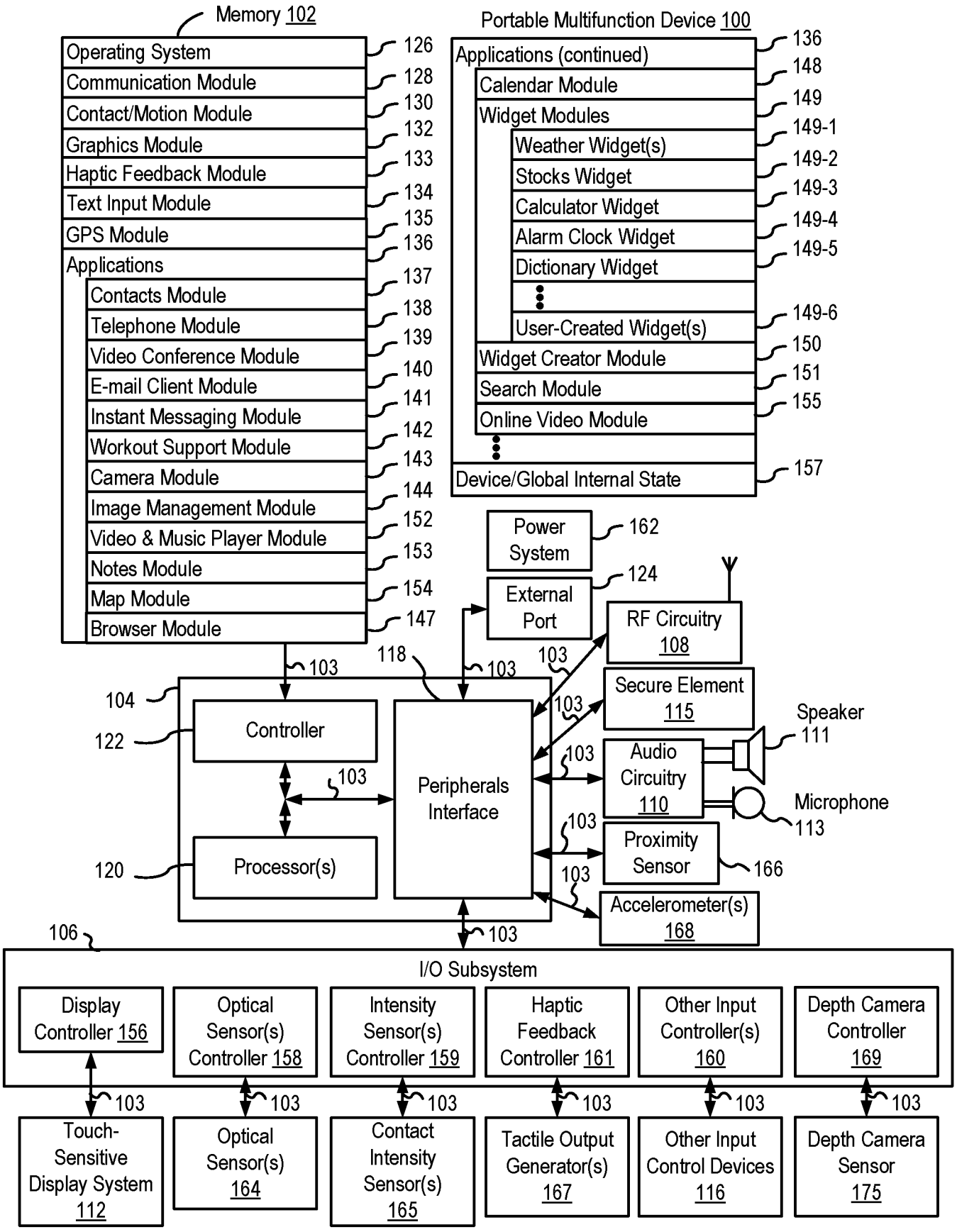


FIG. 1A

2022279466 30 Nov 2022

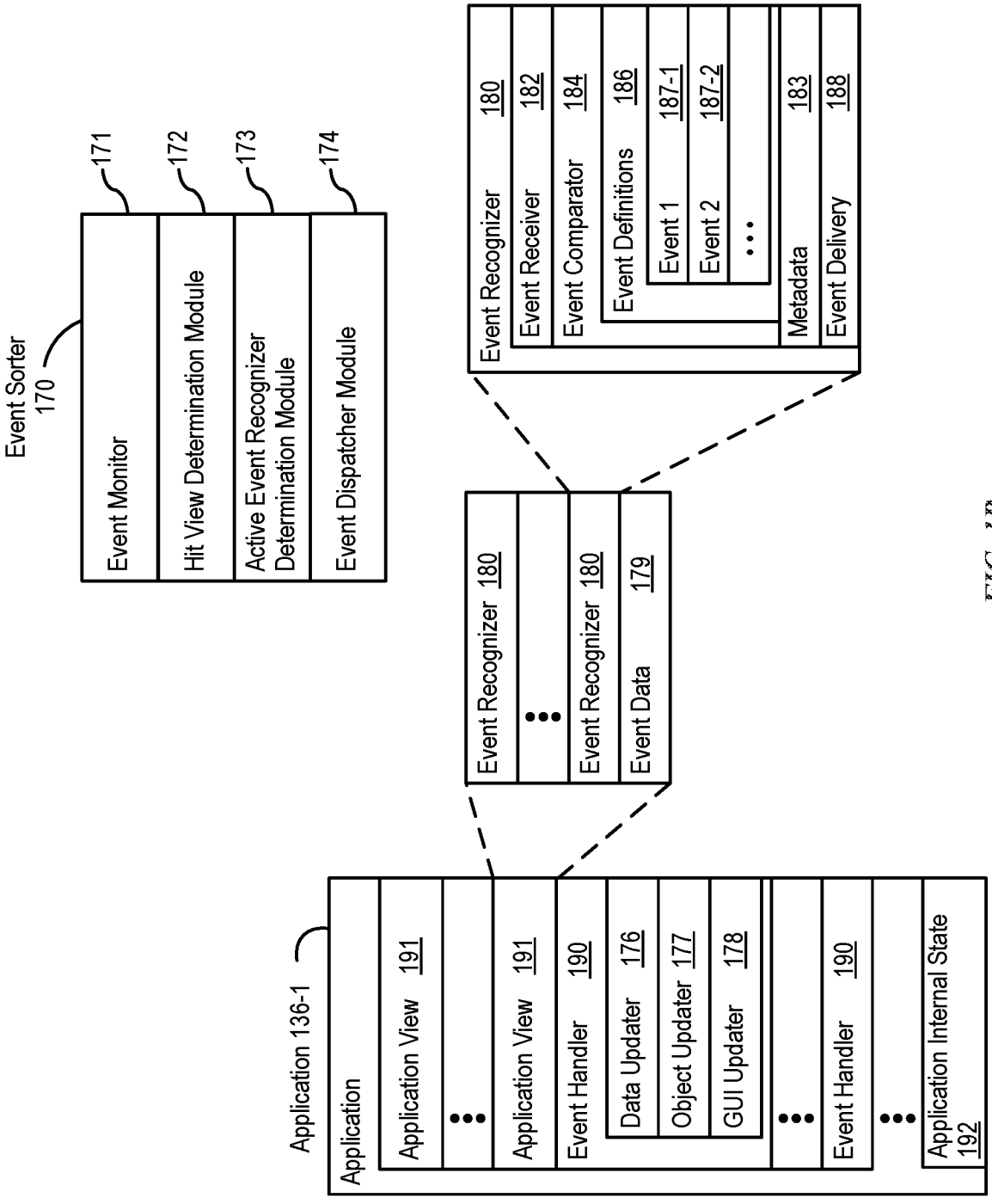


FIG. 1B

2022279466 30 Nov 2022

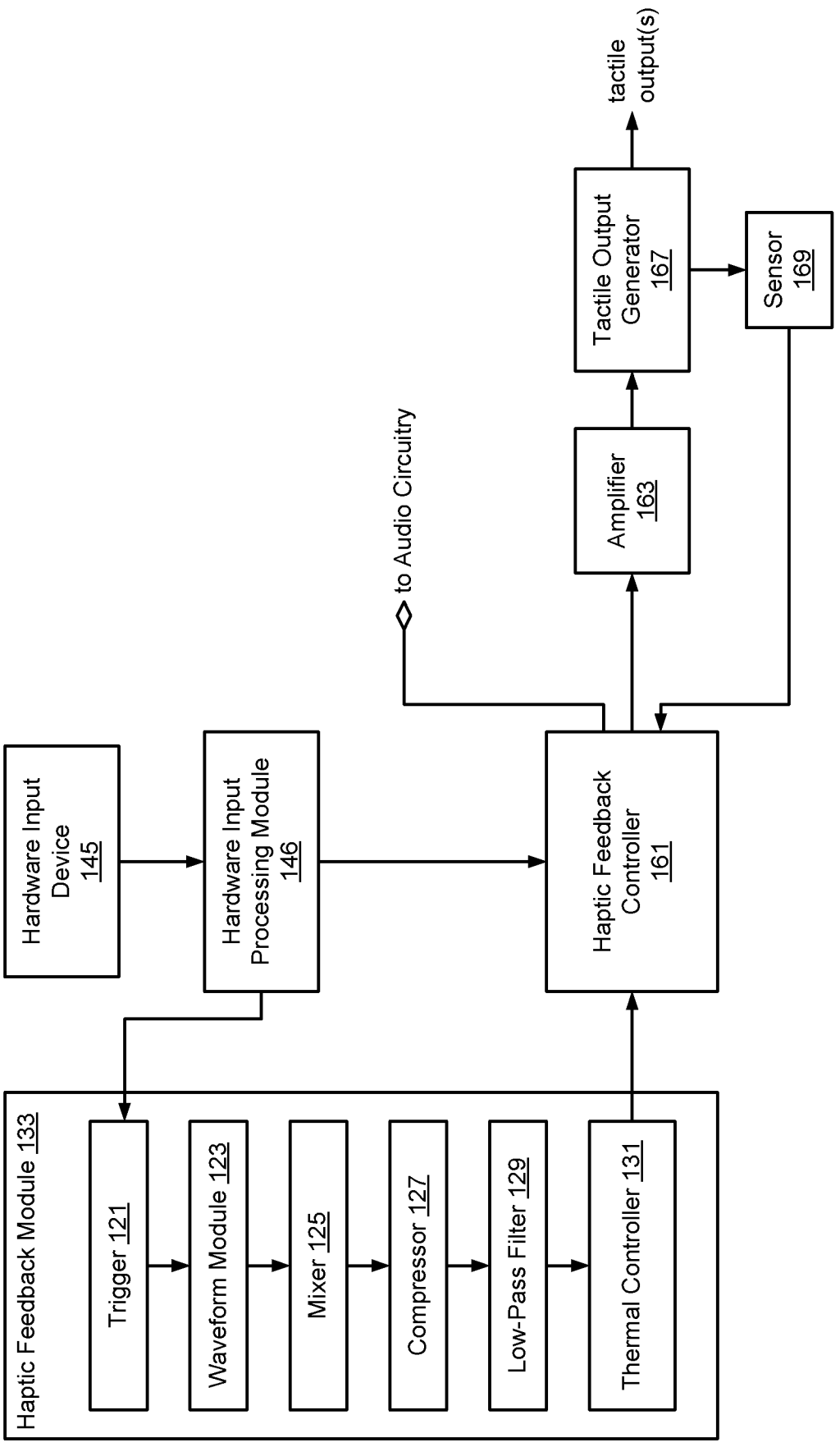


FIG. 1C

2022279466 30 Nov 2022

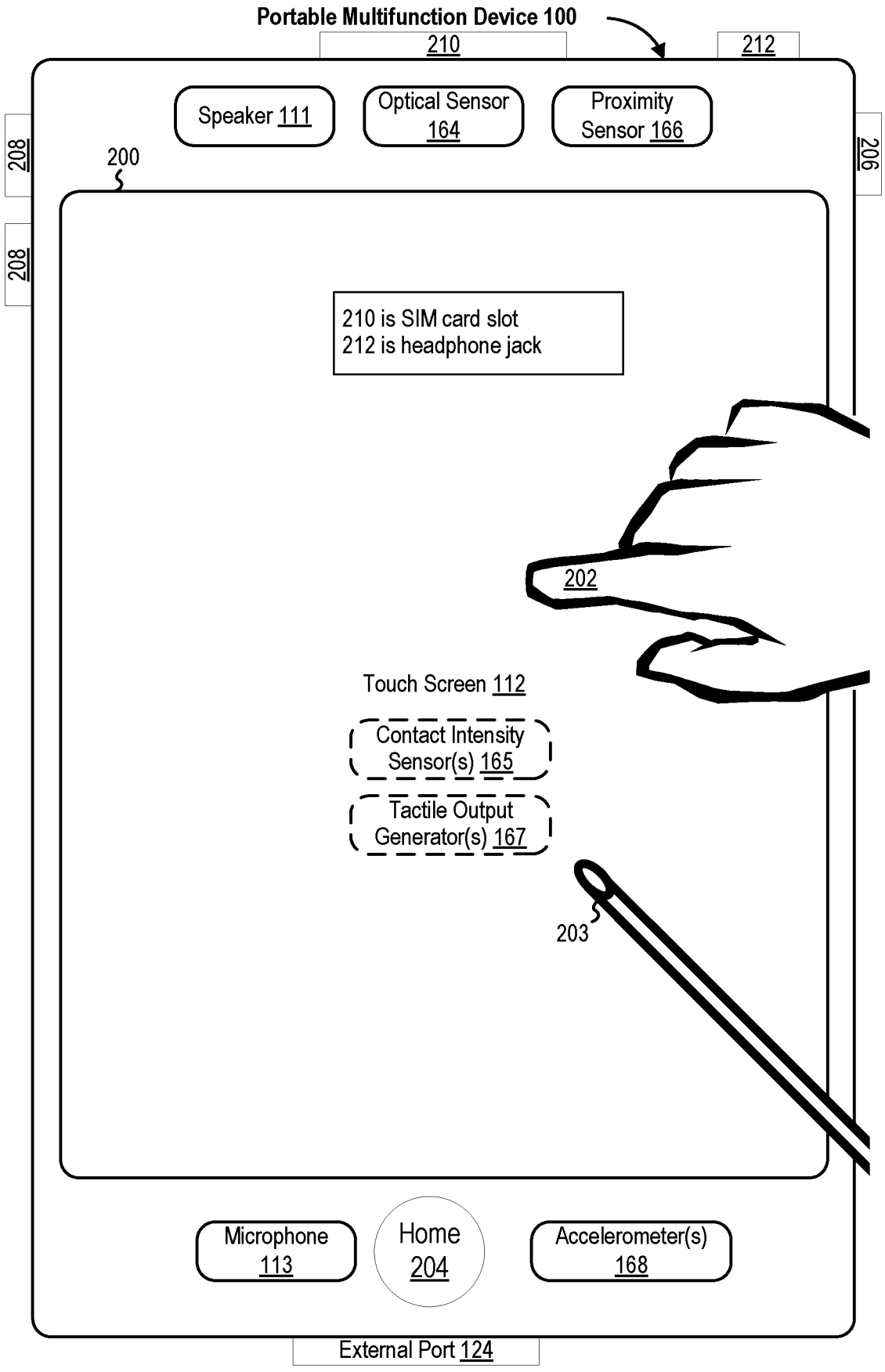


FIG. 2

2022279466 30 Nov 2022

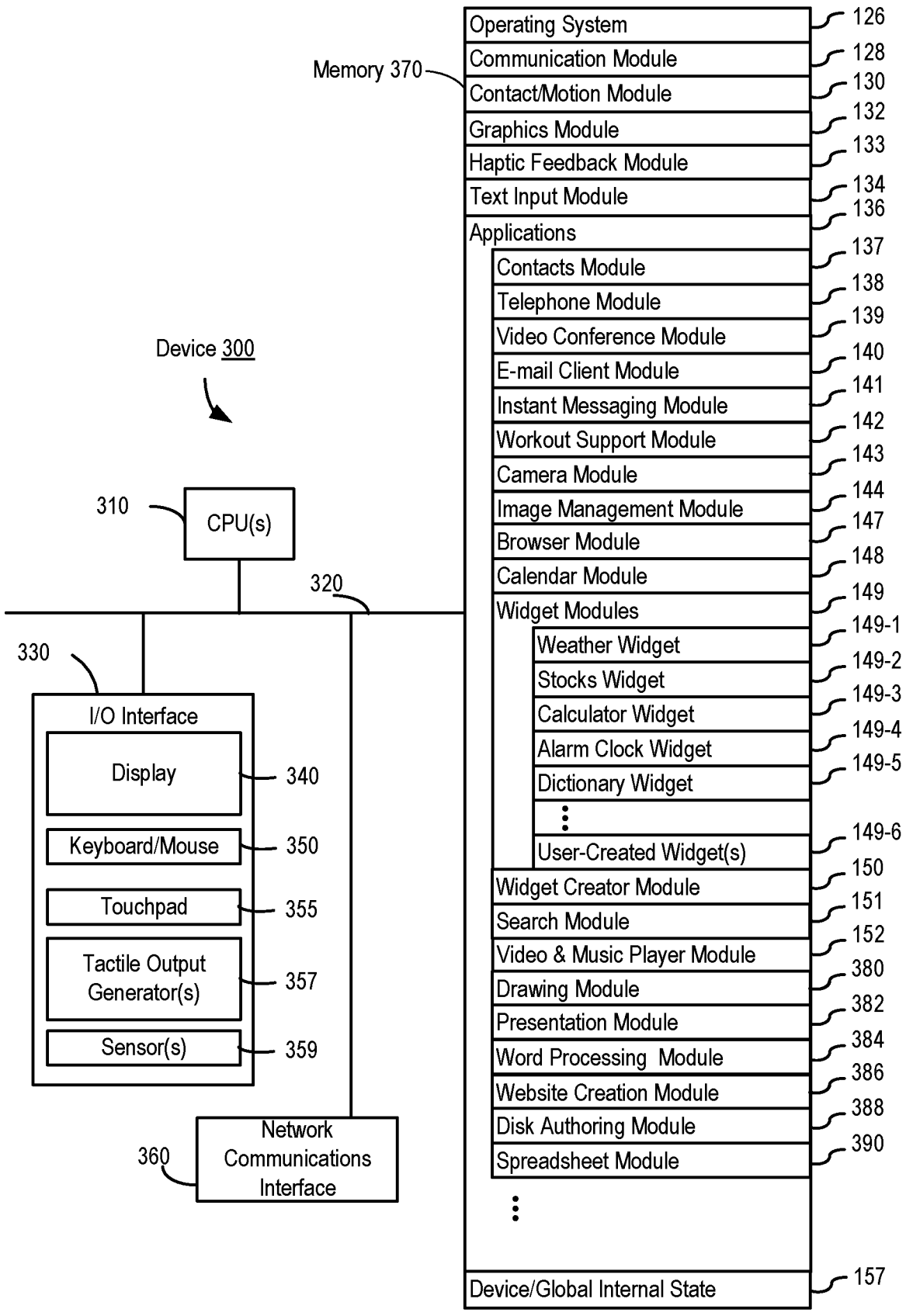


FIG. 3

2022279466 30 Nov 2022

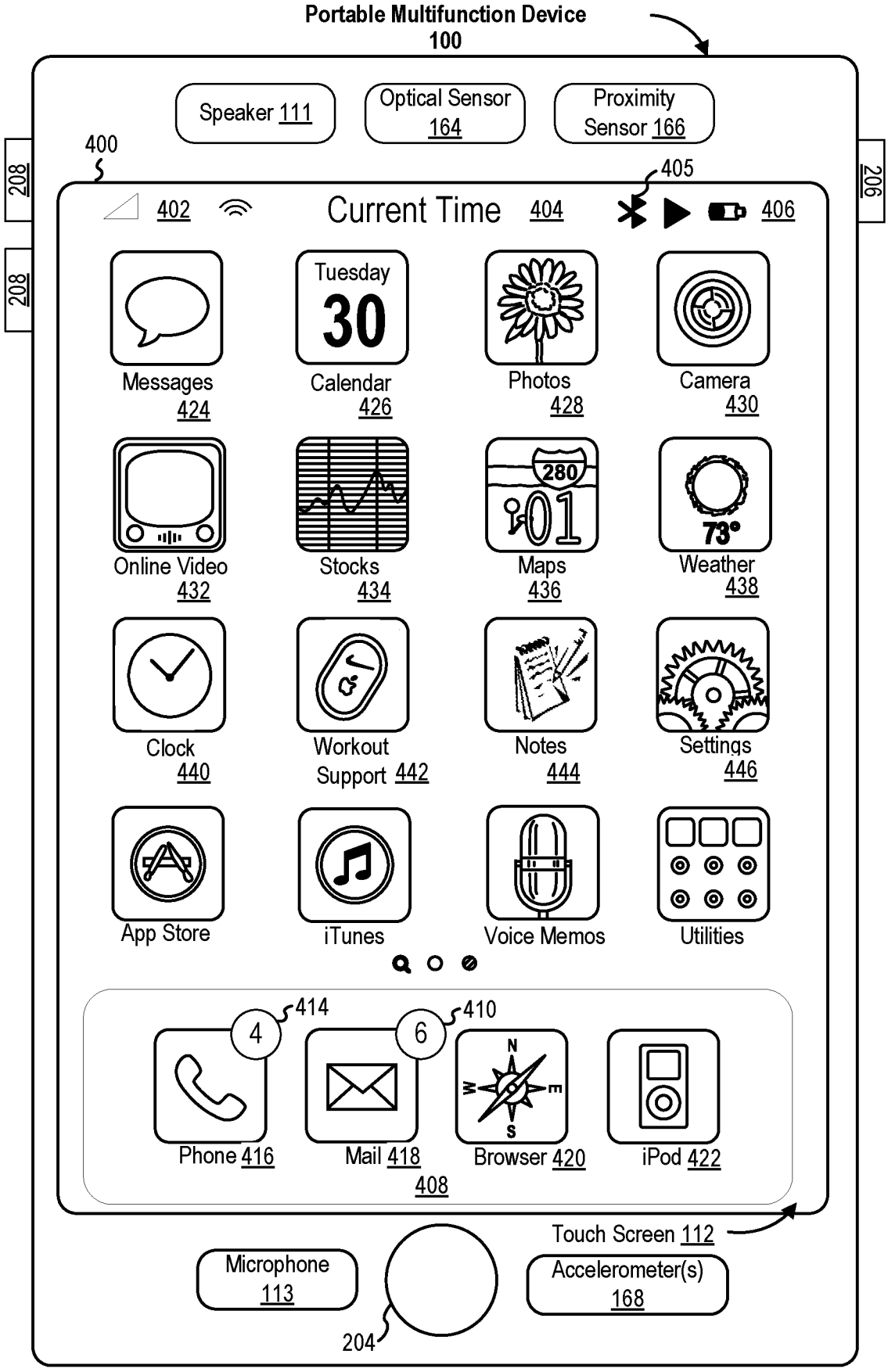
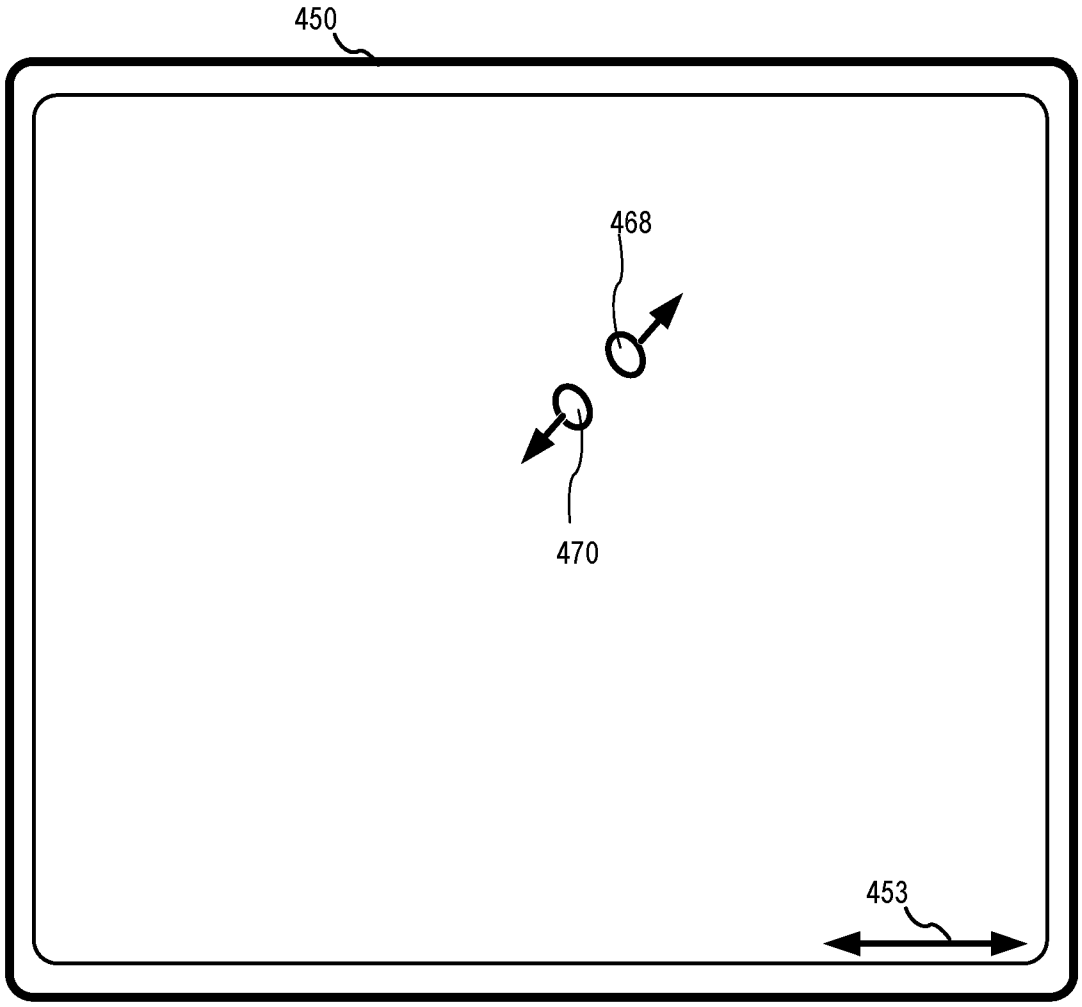


FIG. 4A

2022279466 30 Nov 2022



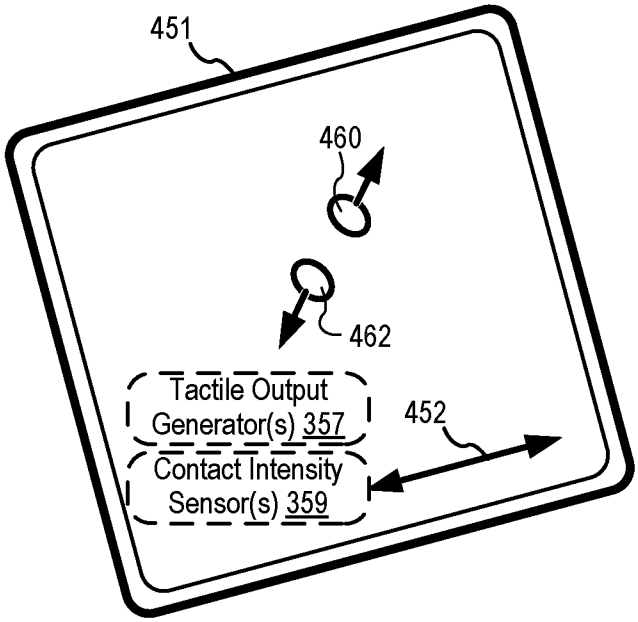


FIG. 4B

30 Nov 2022
2022279466

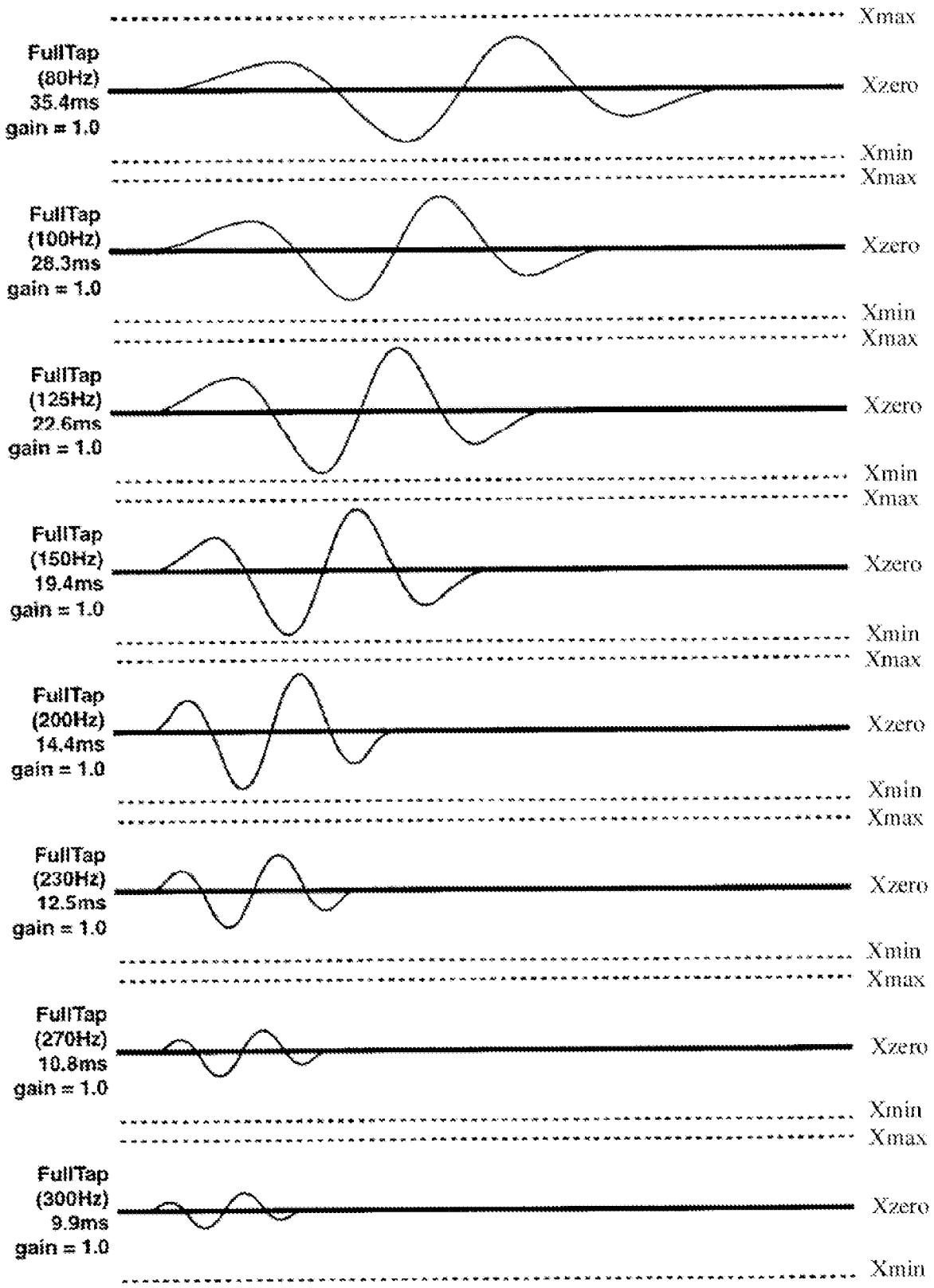


FIG. 4C

2022279466 30 Nov 2022

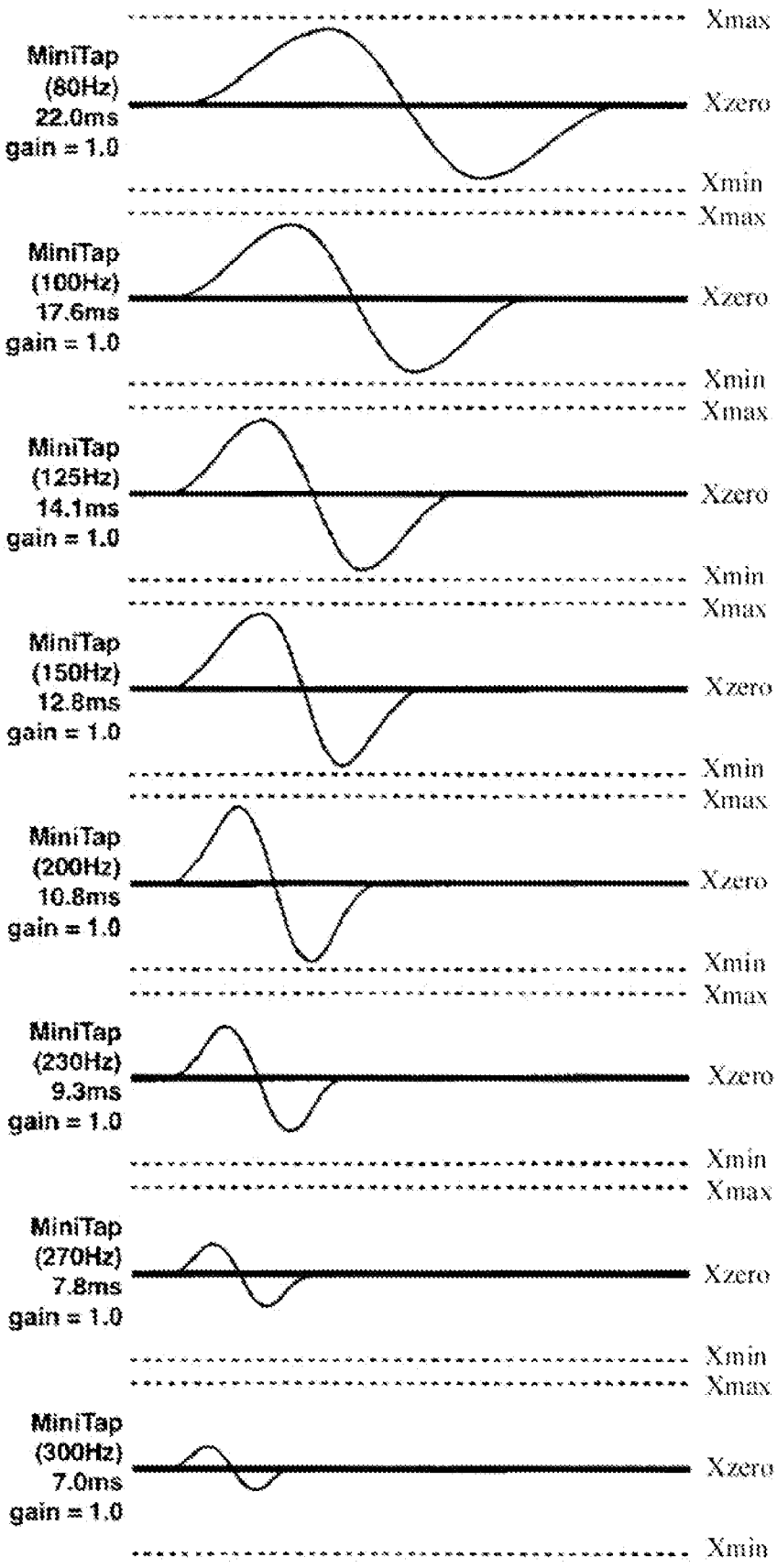


FIG. 4D

2022279466 30 Nov 2022

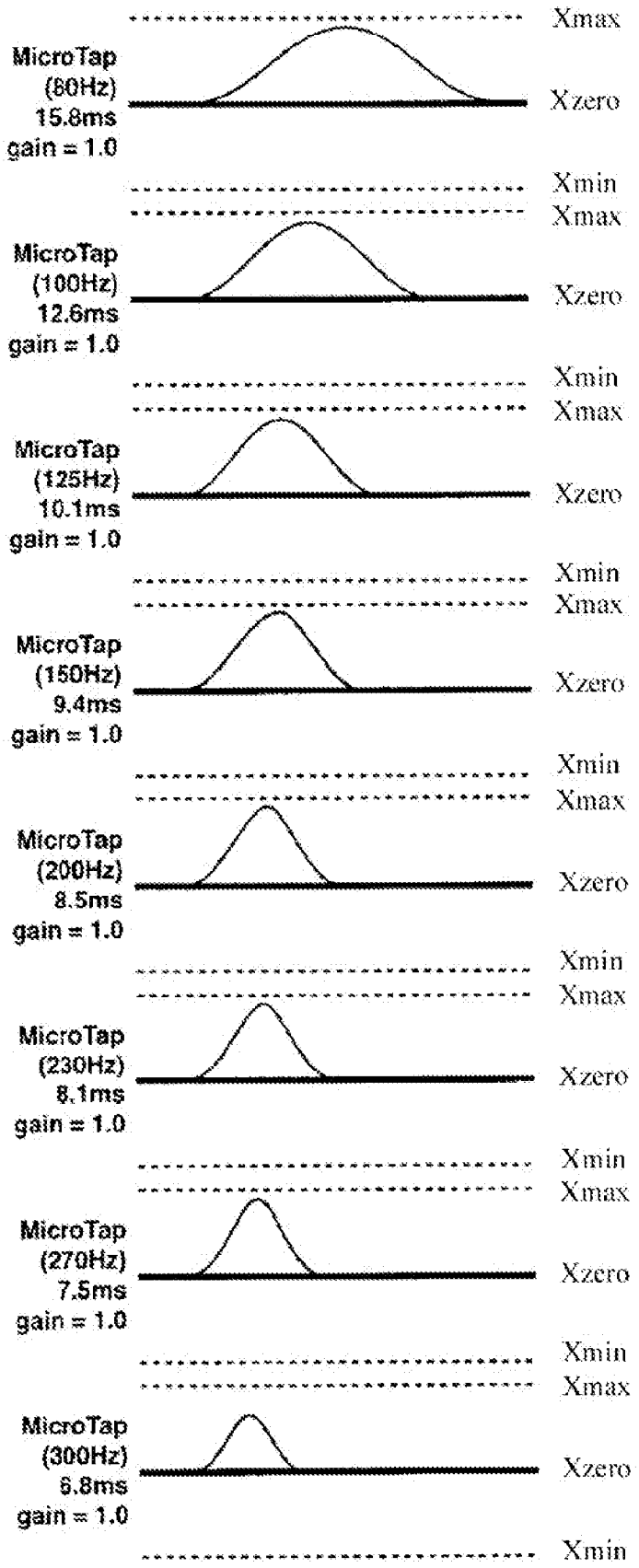


FIG. 4E

2022279466 30 Nov 2022

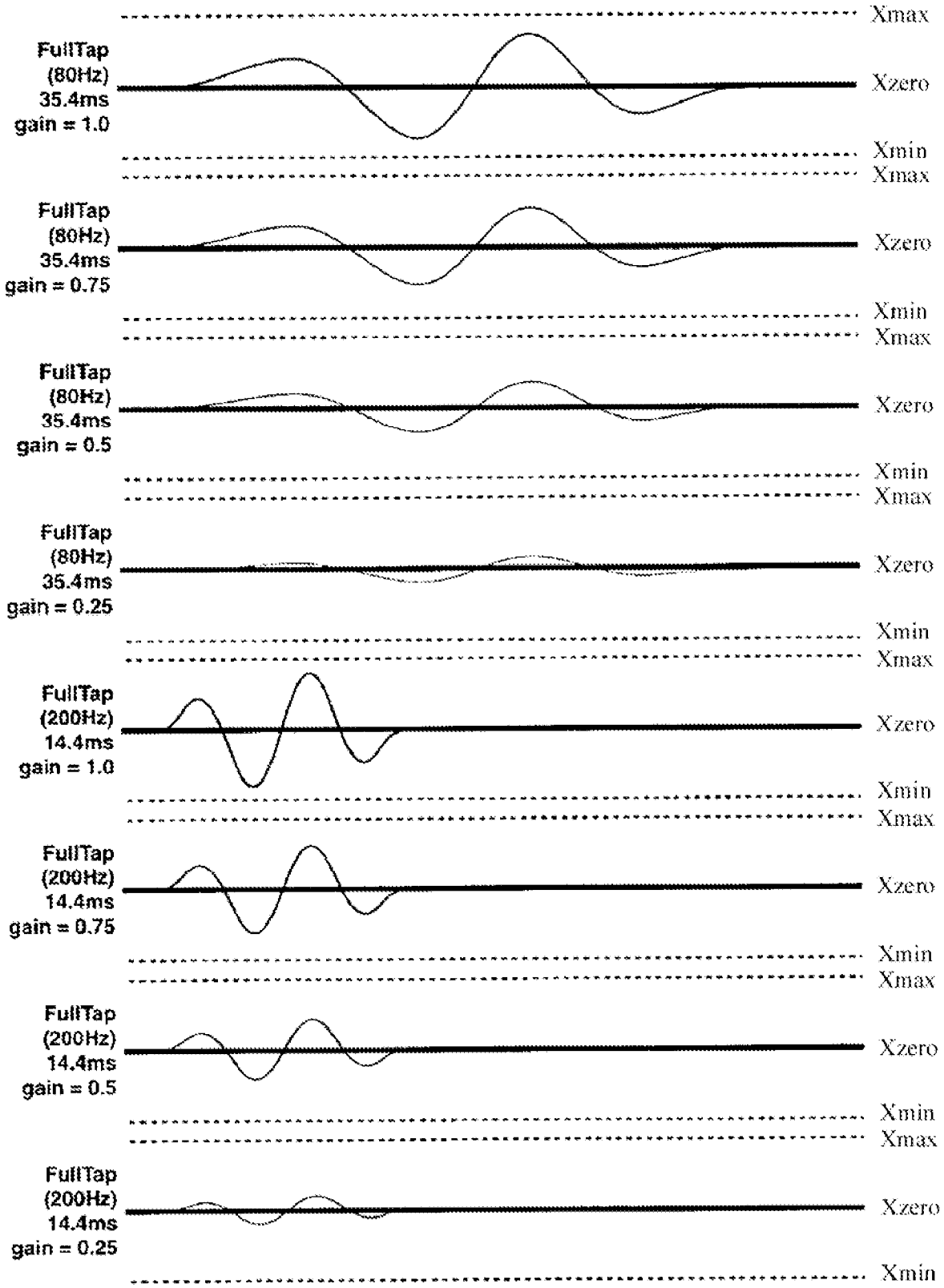


FIG. 4F

2022279466 30 Nov 2022

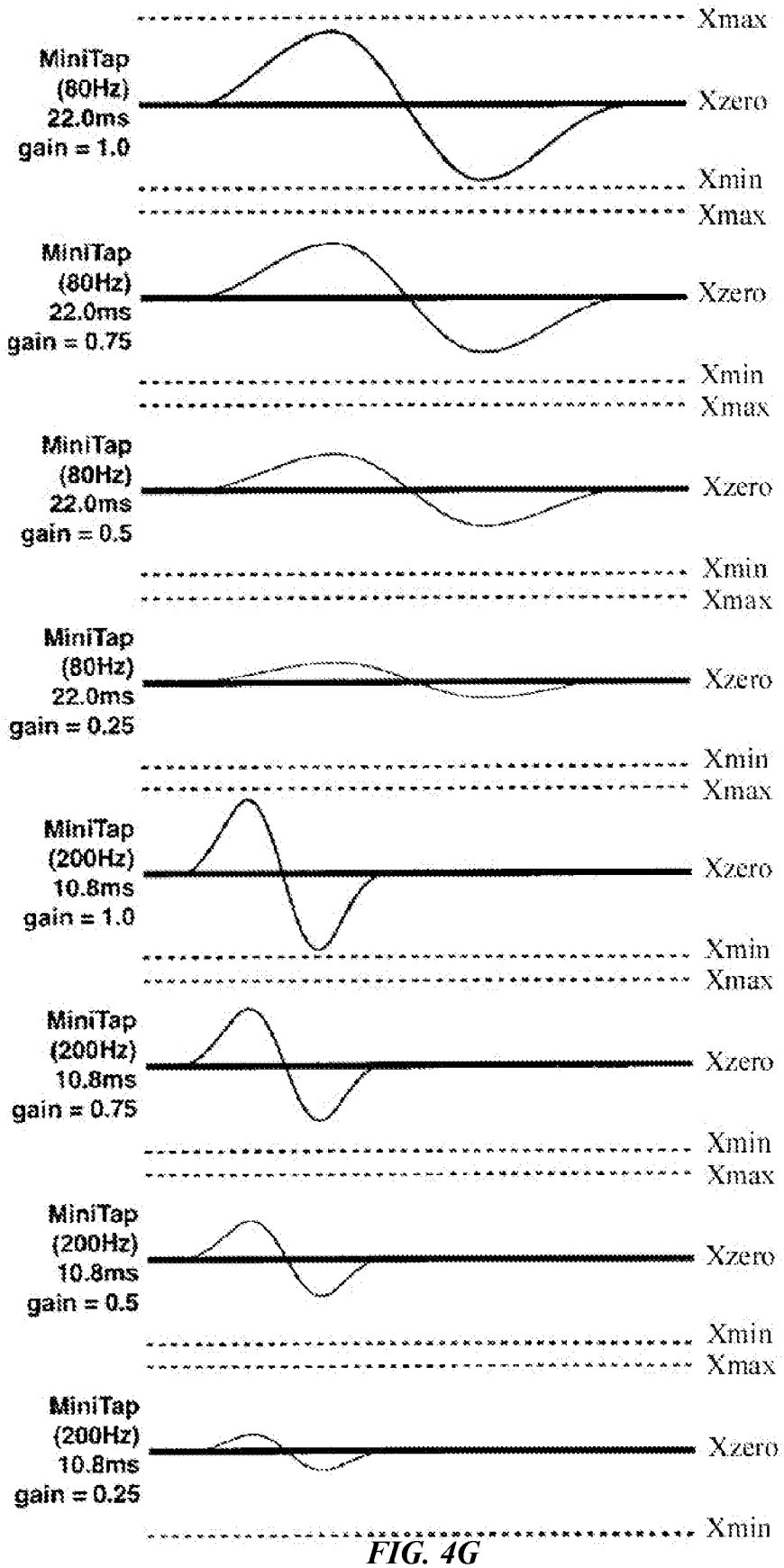


FIG. 4G

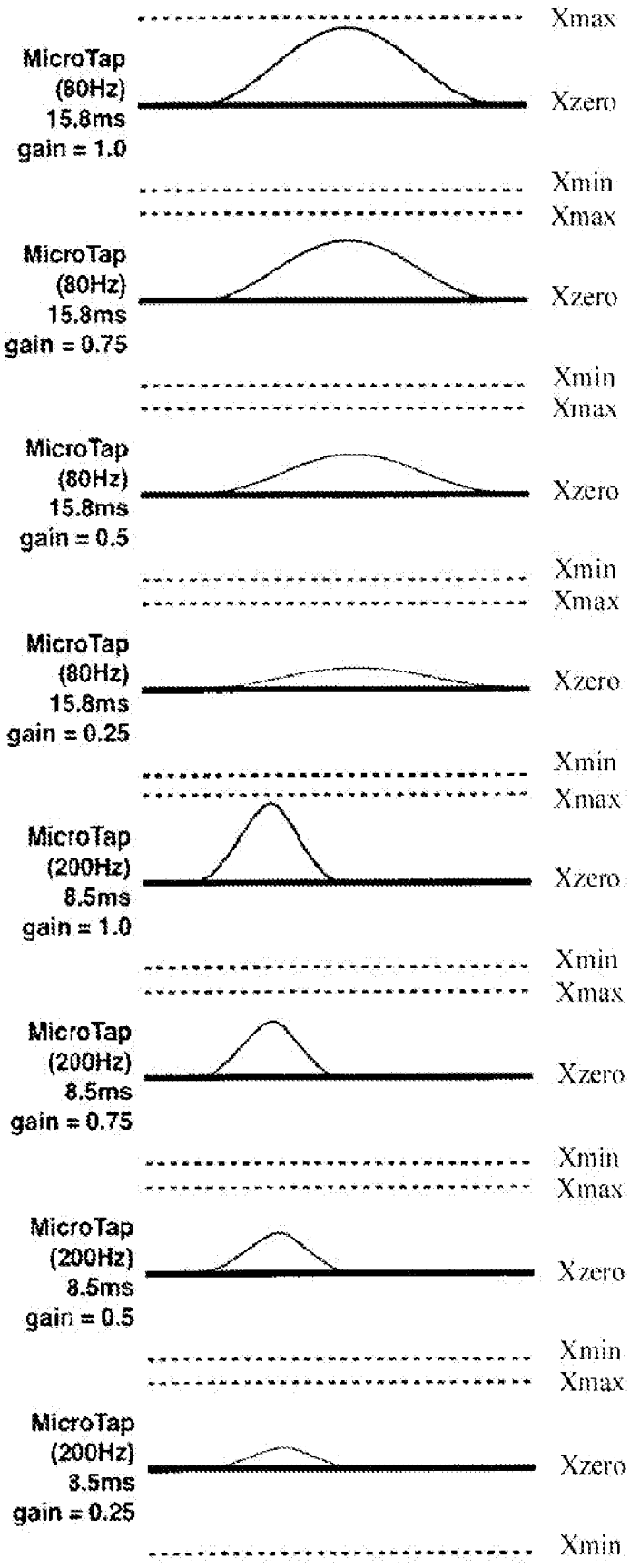


FIG. 4H

2022279466 30 Nov 2022

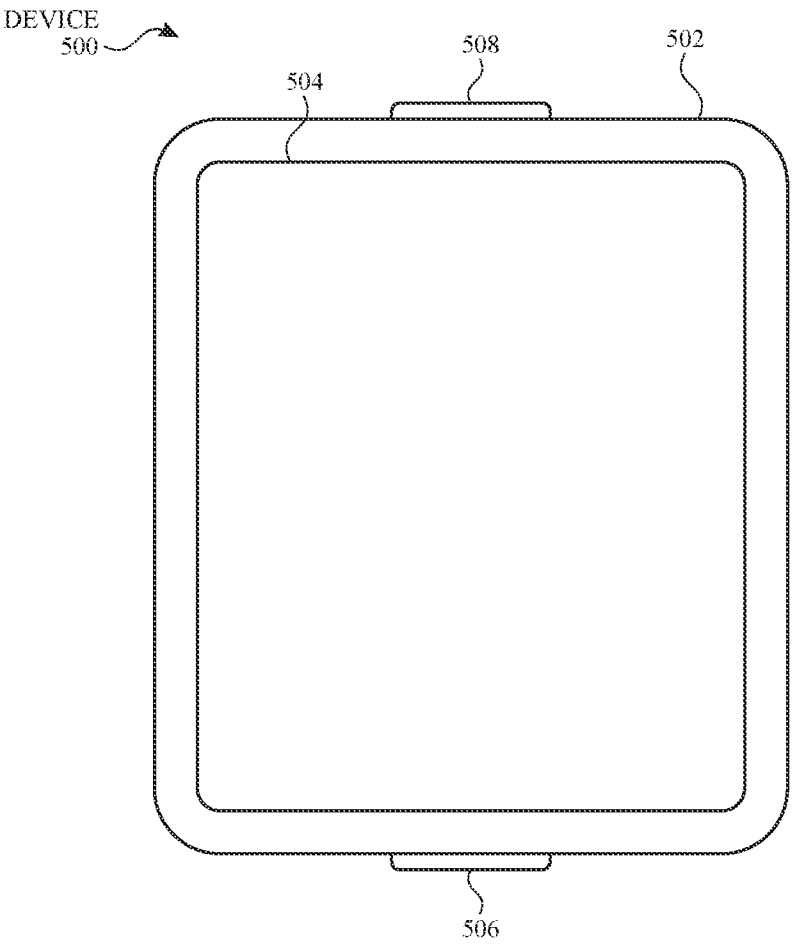


FIG. 5A

2022279466 30 Nov 2022

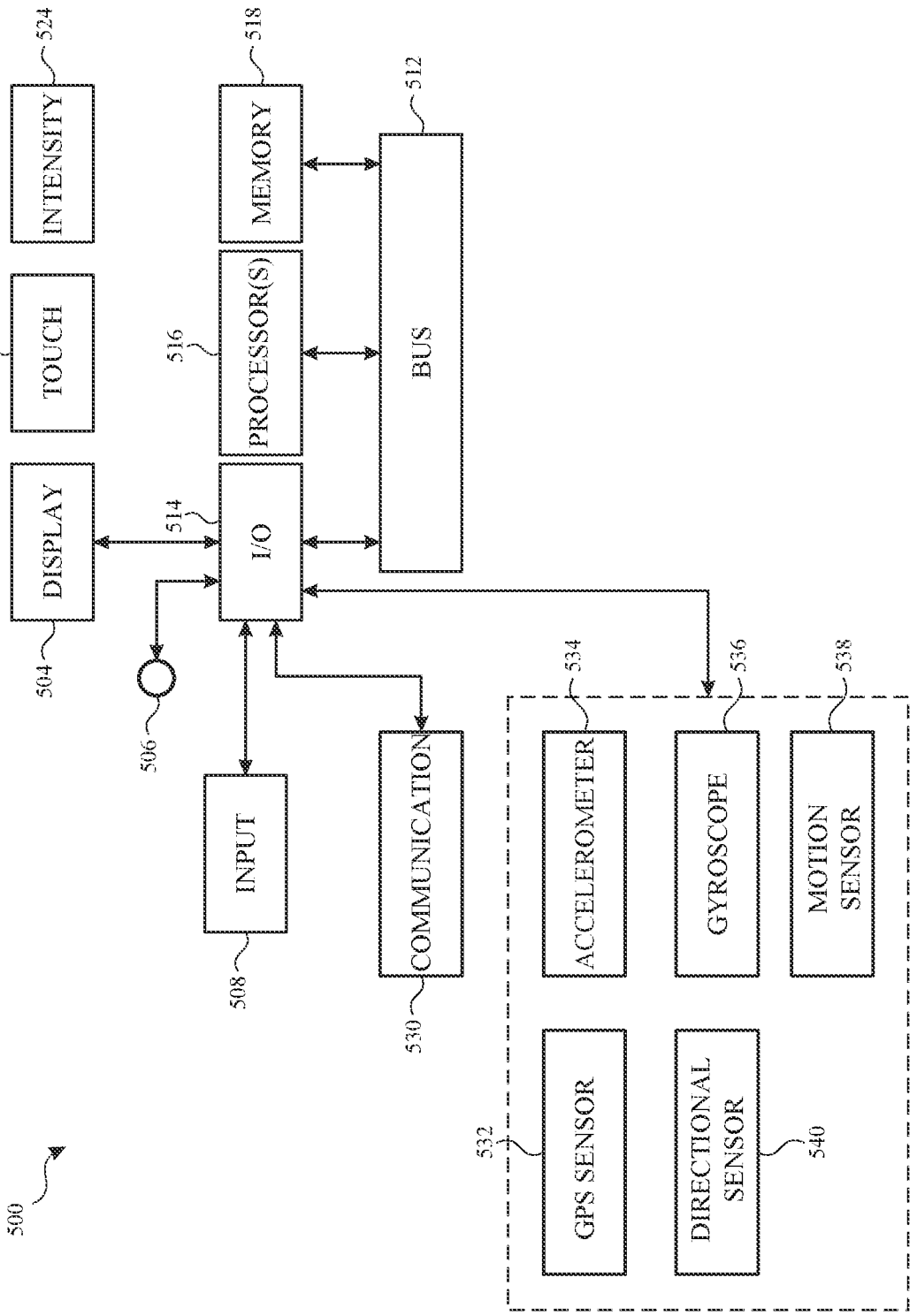


FIG. 5B

2022279466 30 Nov 2022

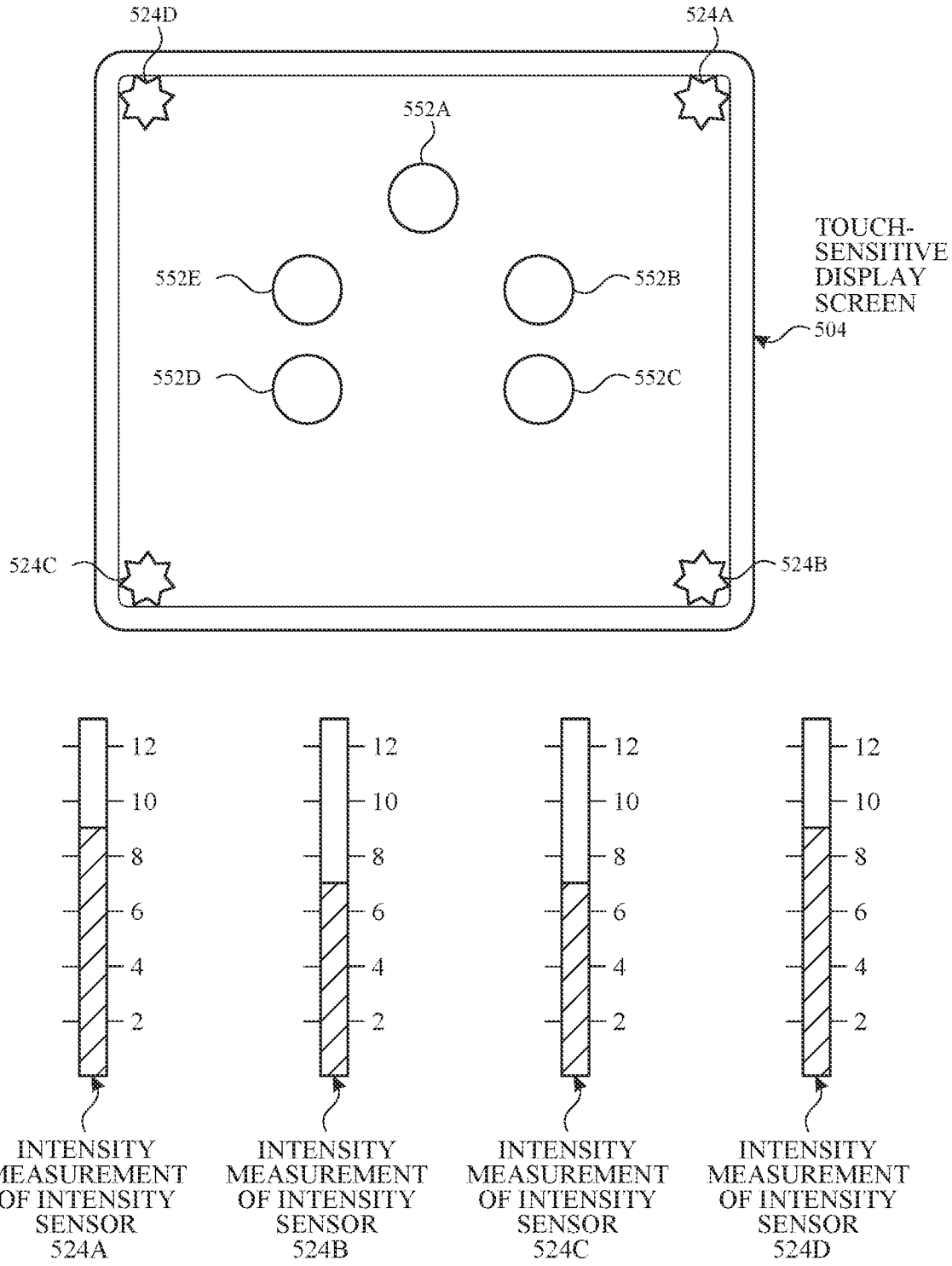


FIG. 5C

2022279466 30 Nov 2022

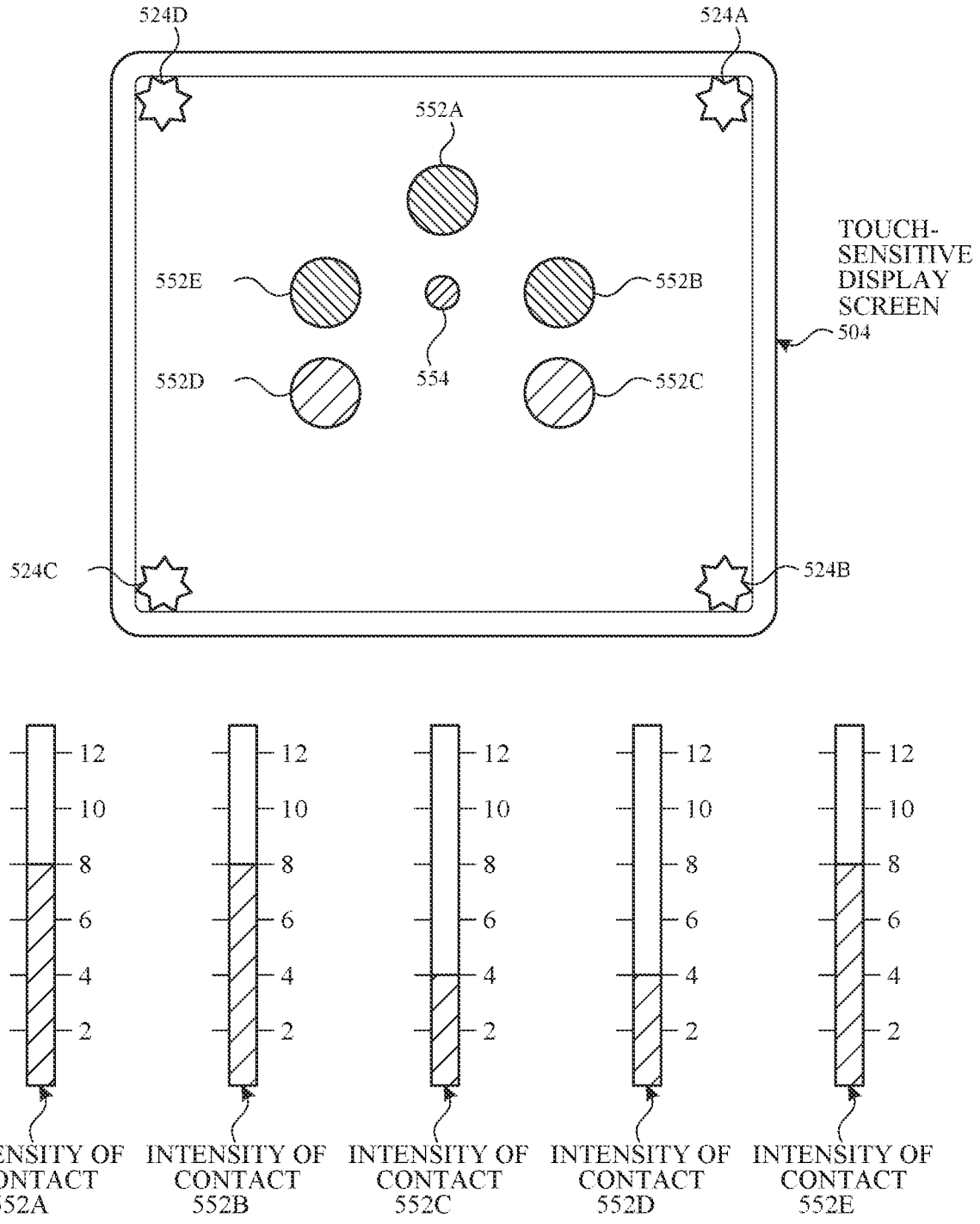


FIG. 5D

2022279466 30 Nov 2022

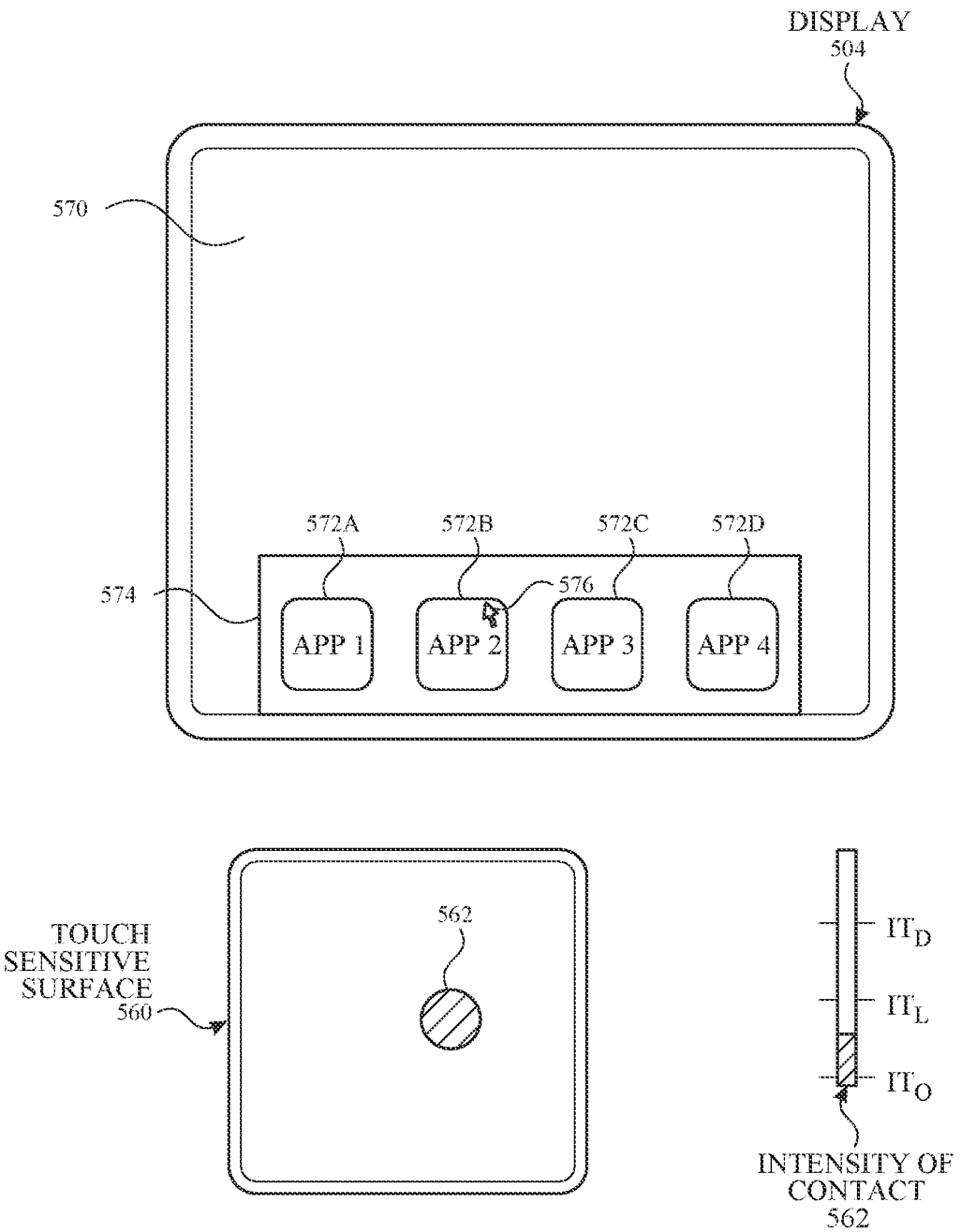


FIG. 5E

2022279466 30 Nov 2022

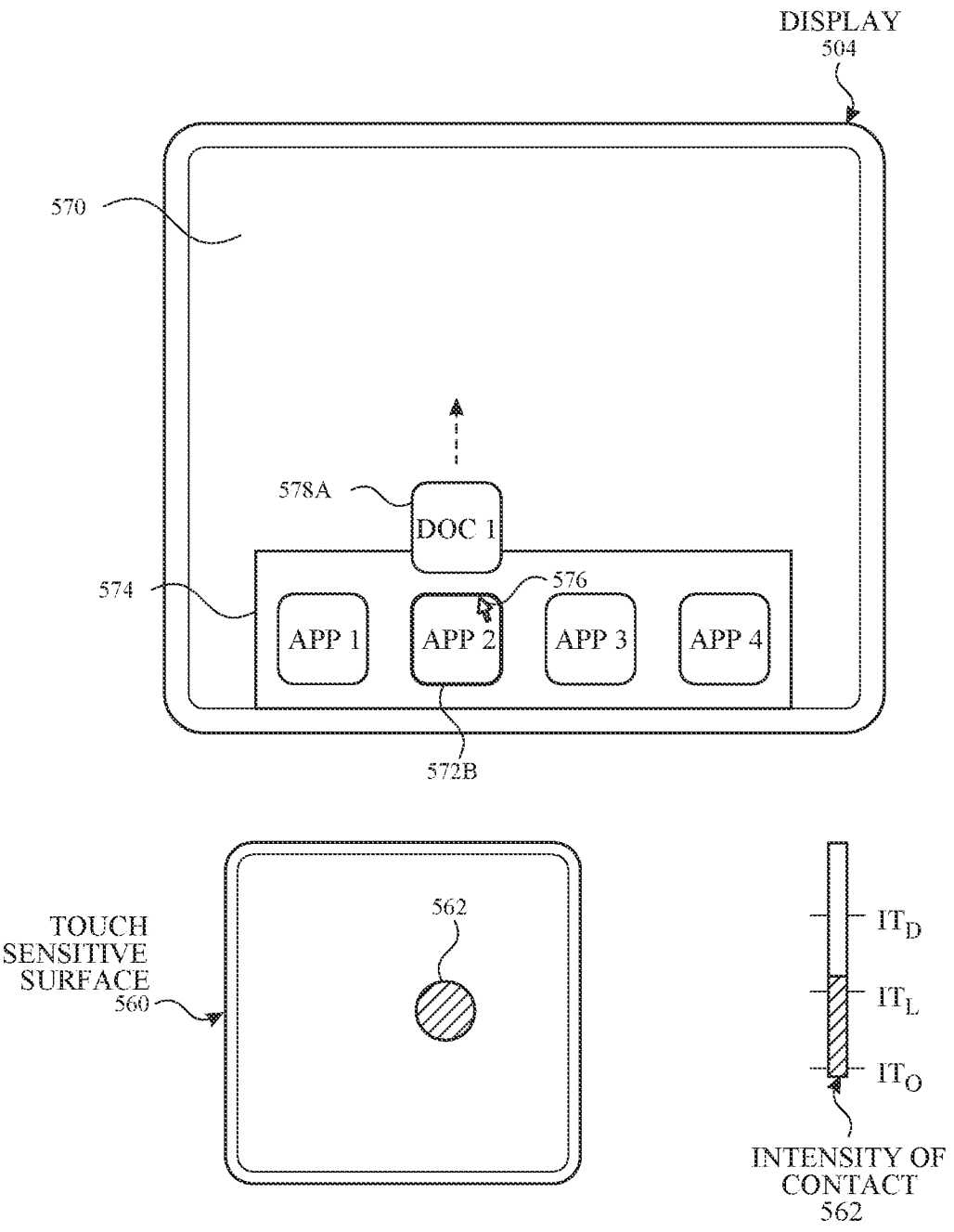


FIG. 5F

2022279466 30 Nov 2022

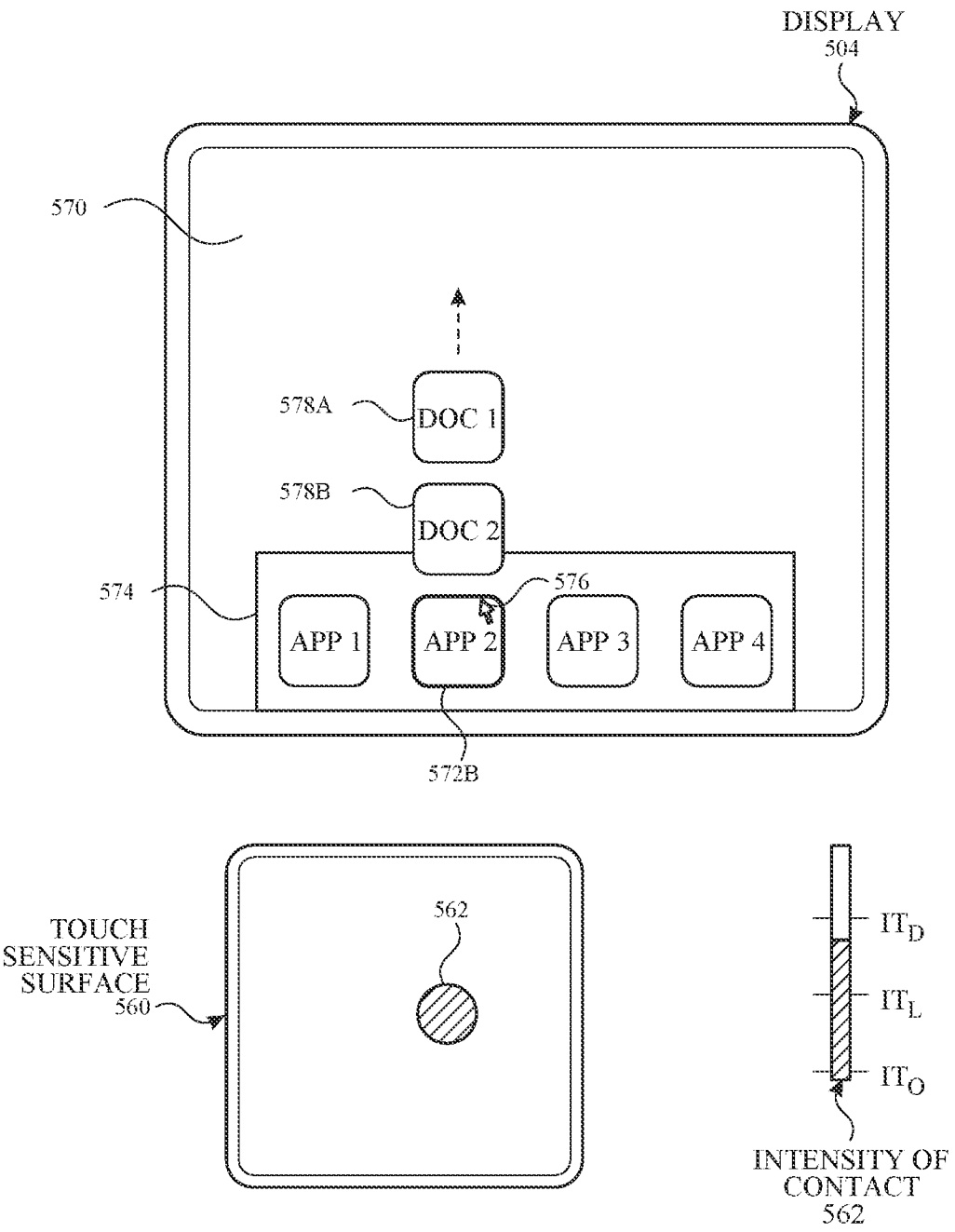


FIG. 5G

2022279466 30 Nov 2022

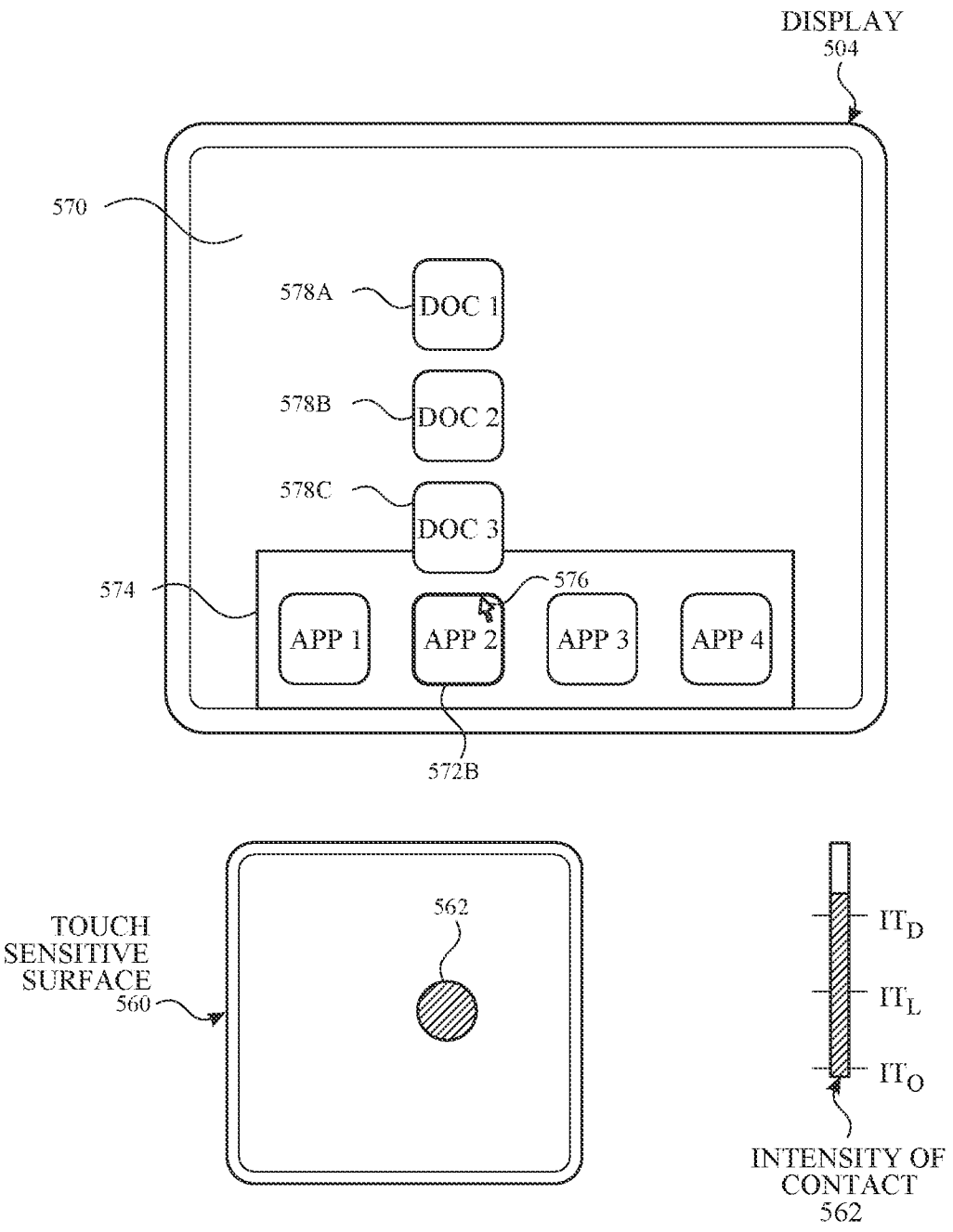


FIG. 5H

2022279466 30 Nov 2022

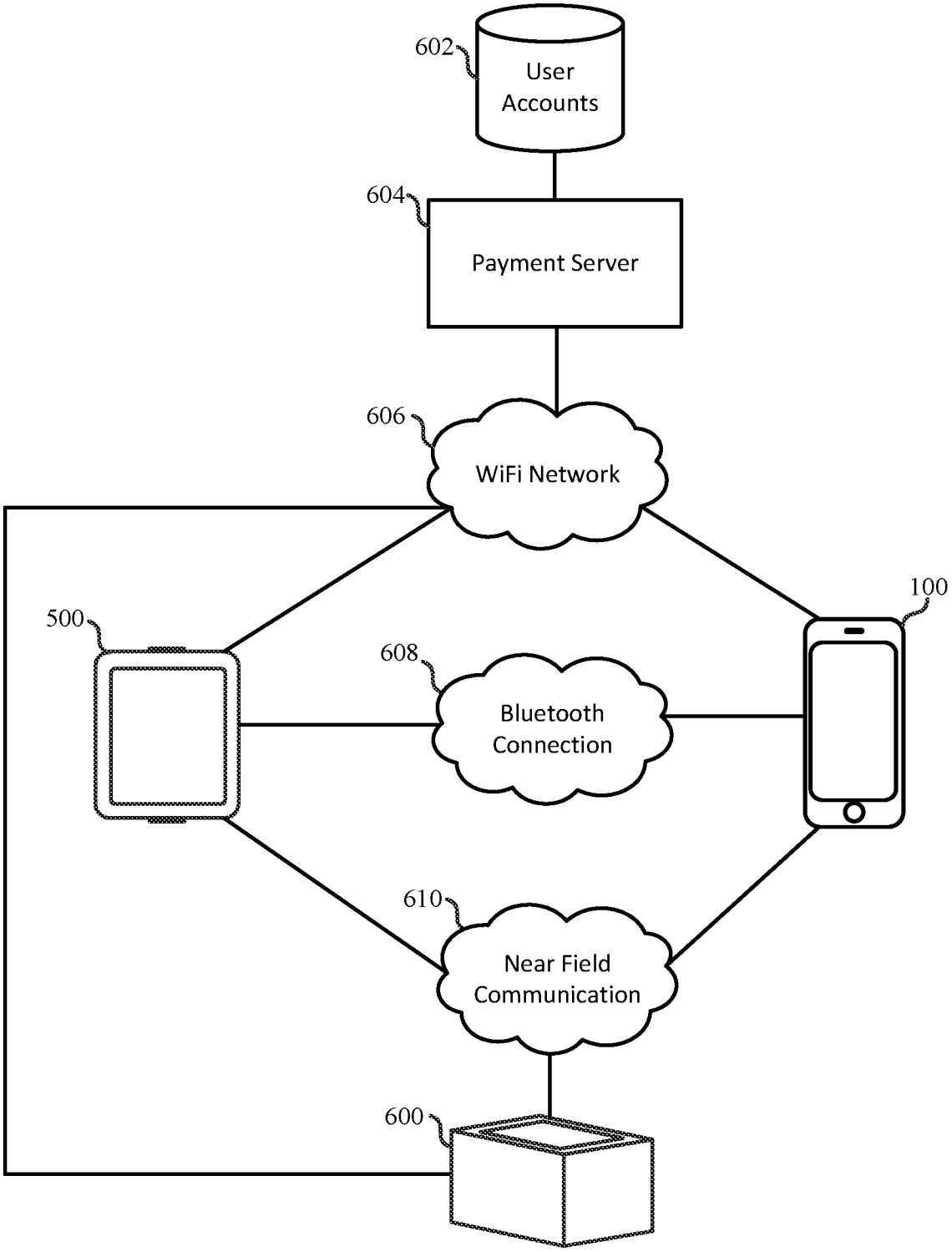


FIG. 6

2022279466 30 Nov 2022

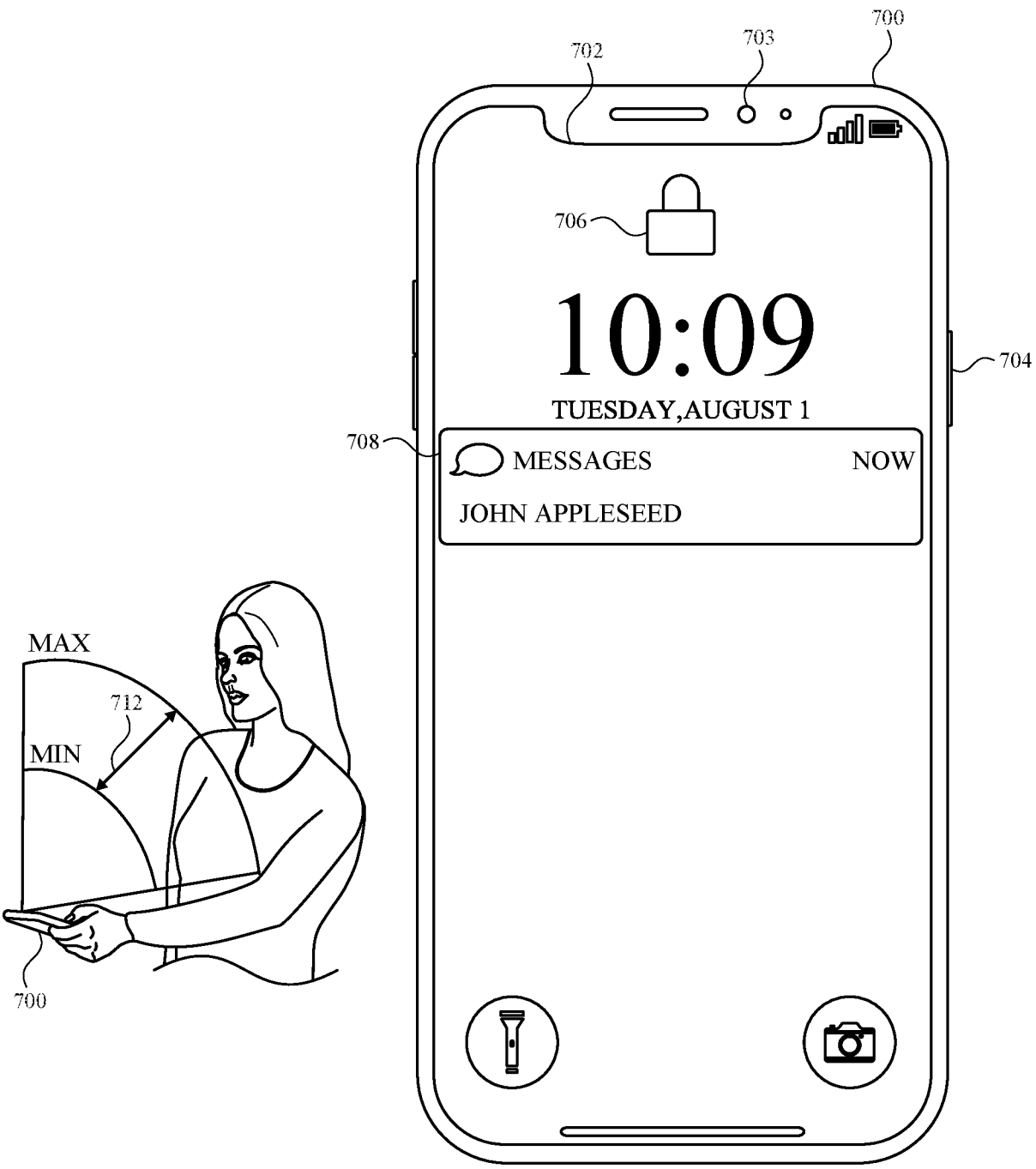


FIG. 7A

2022279466 30 Nov 2022

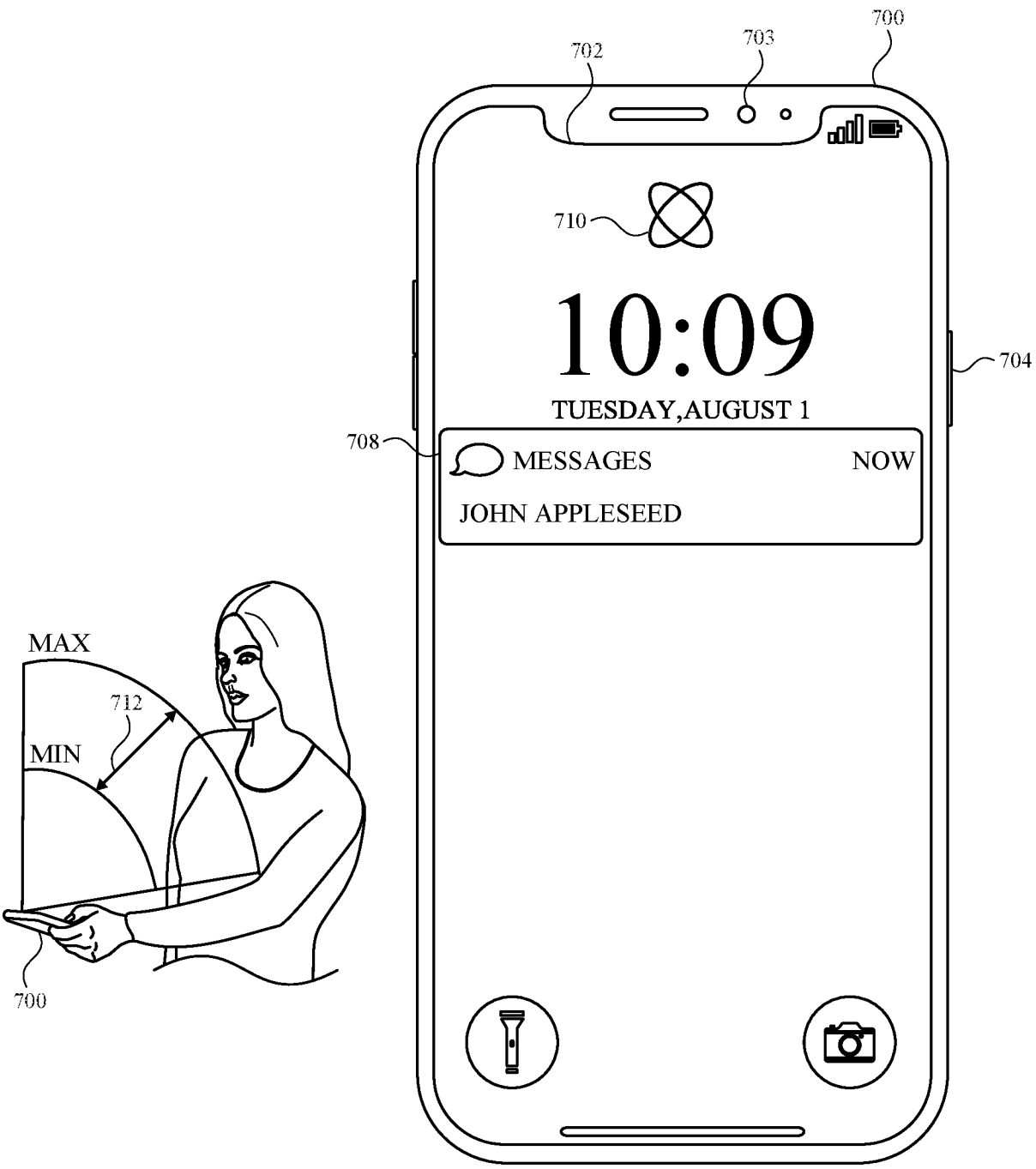


FIG. 7B

2022279466 30 Nov 2022

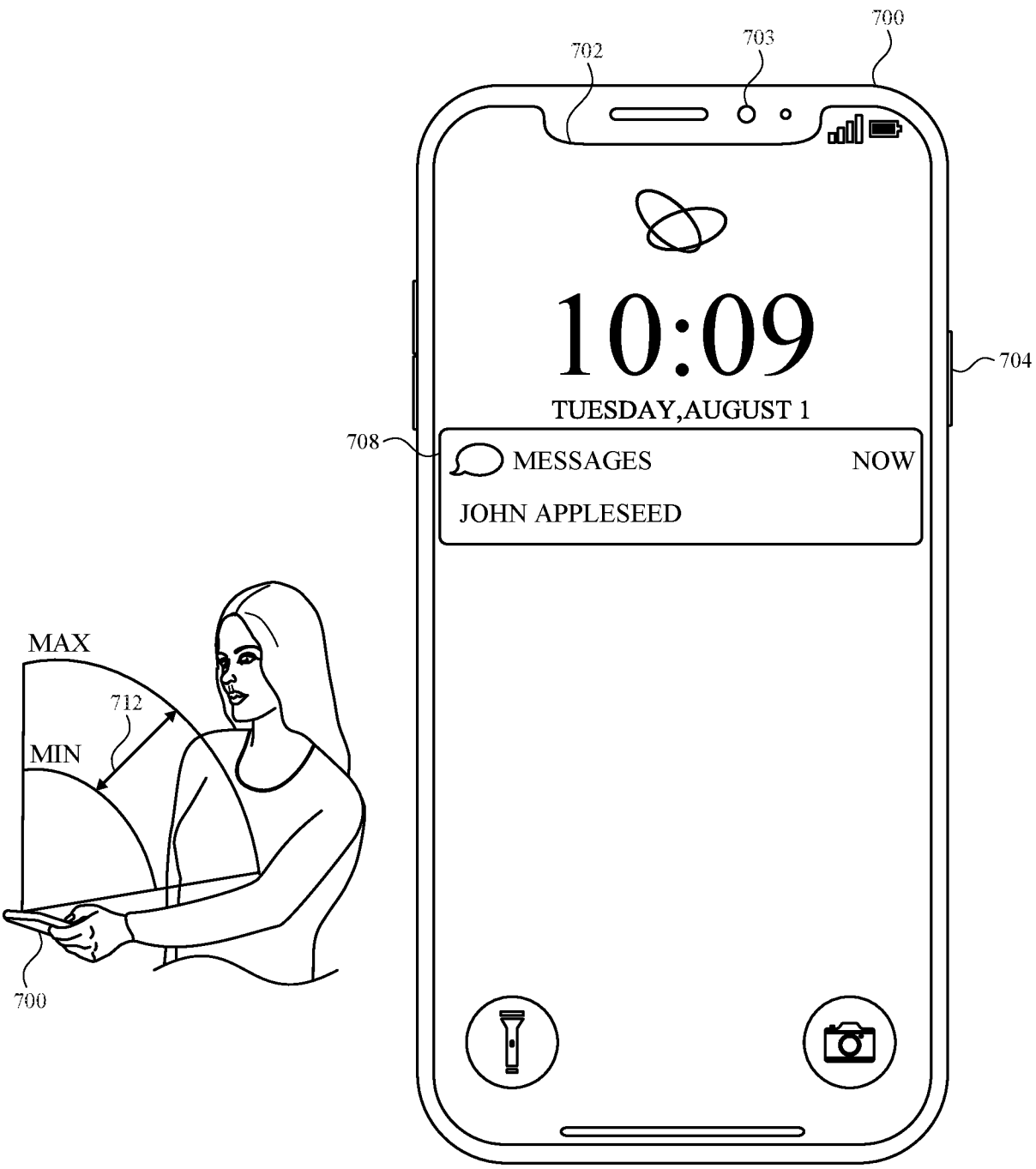


FIG. 7C

2022279466 30 Nov 2022

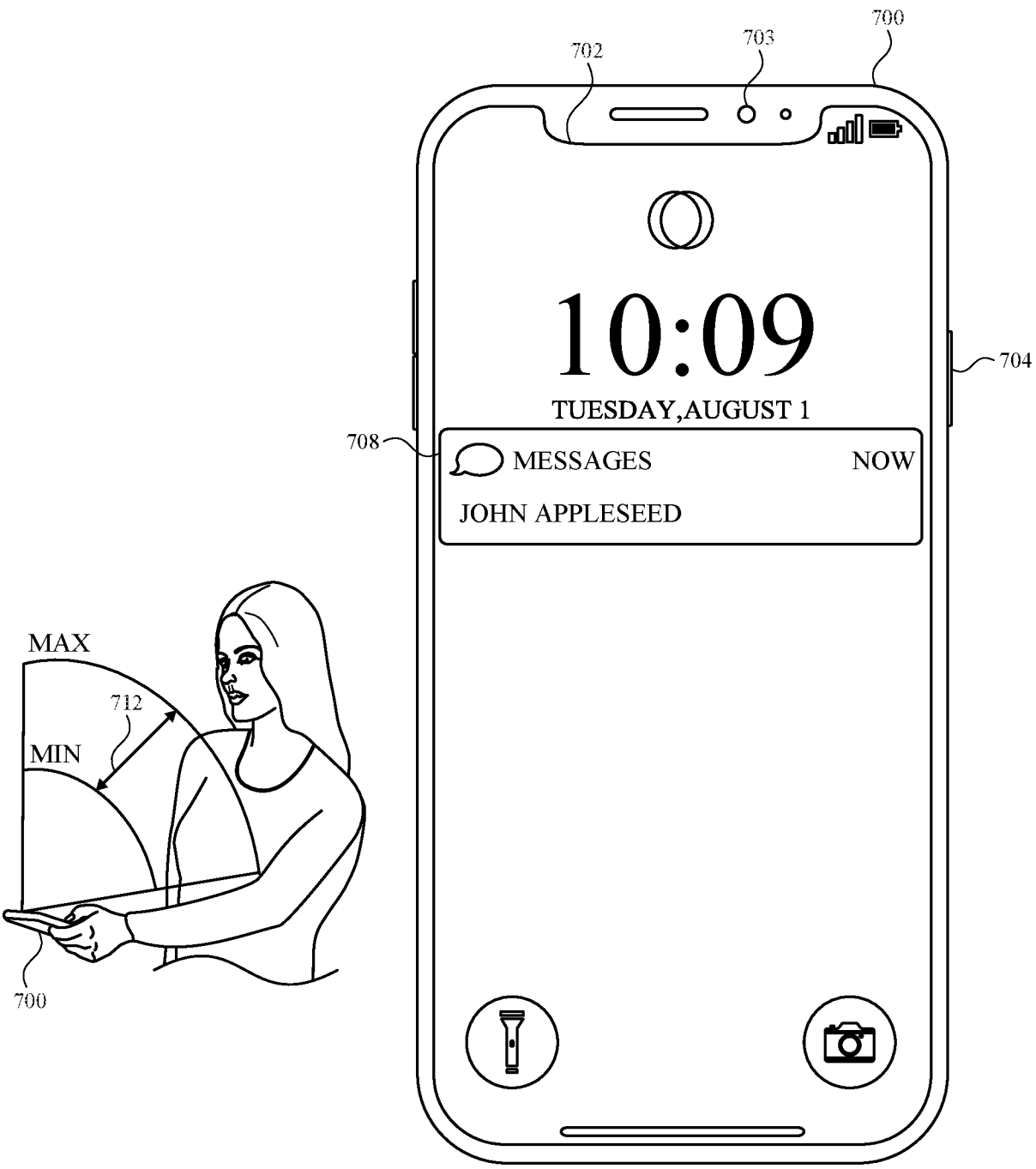


FIG. 7D

2022279466 30 Nov 2022

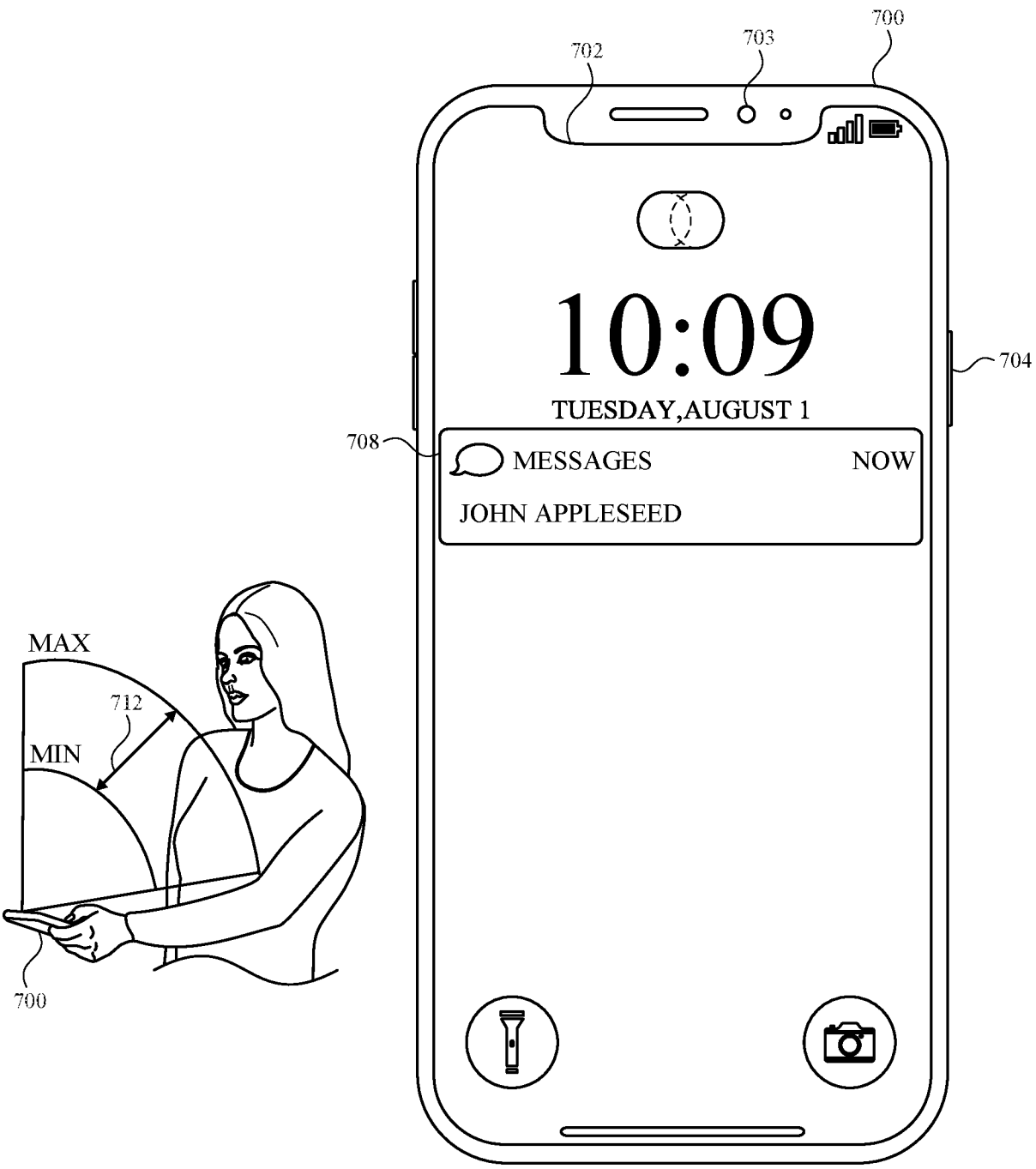


FIG. 7E

2022279466 30 Nov 2022

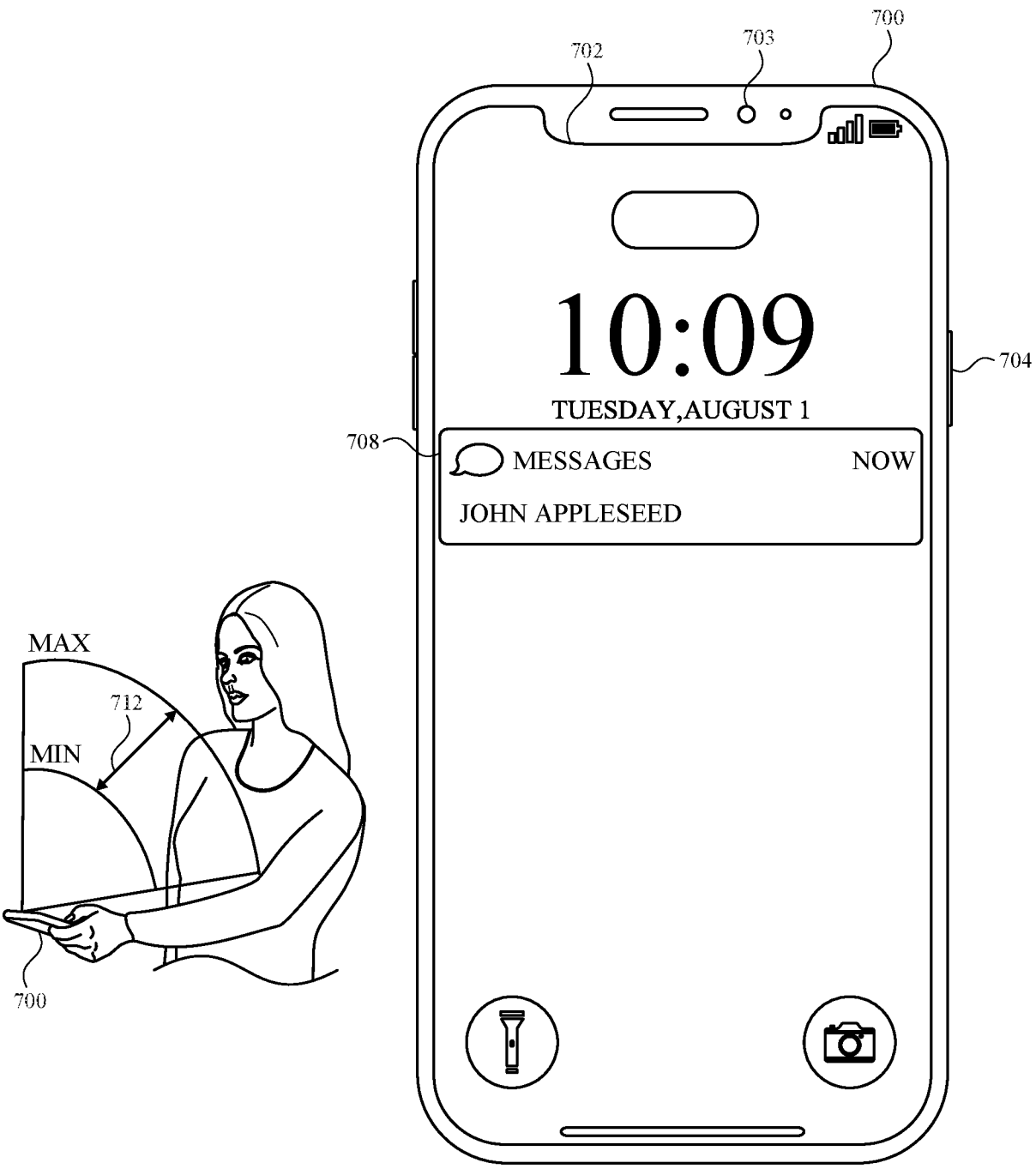


FIG. 7F

2022279466 30 Nov 2022

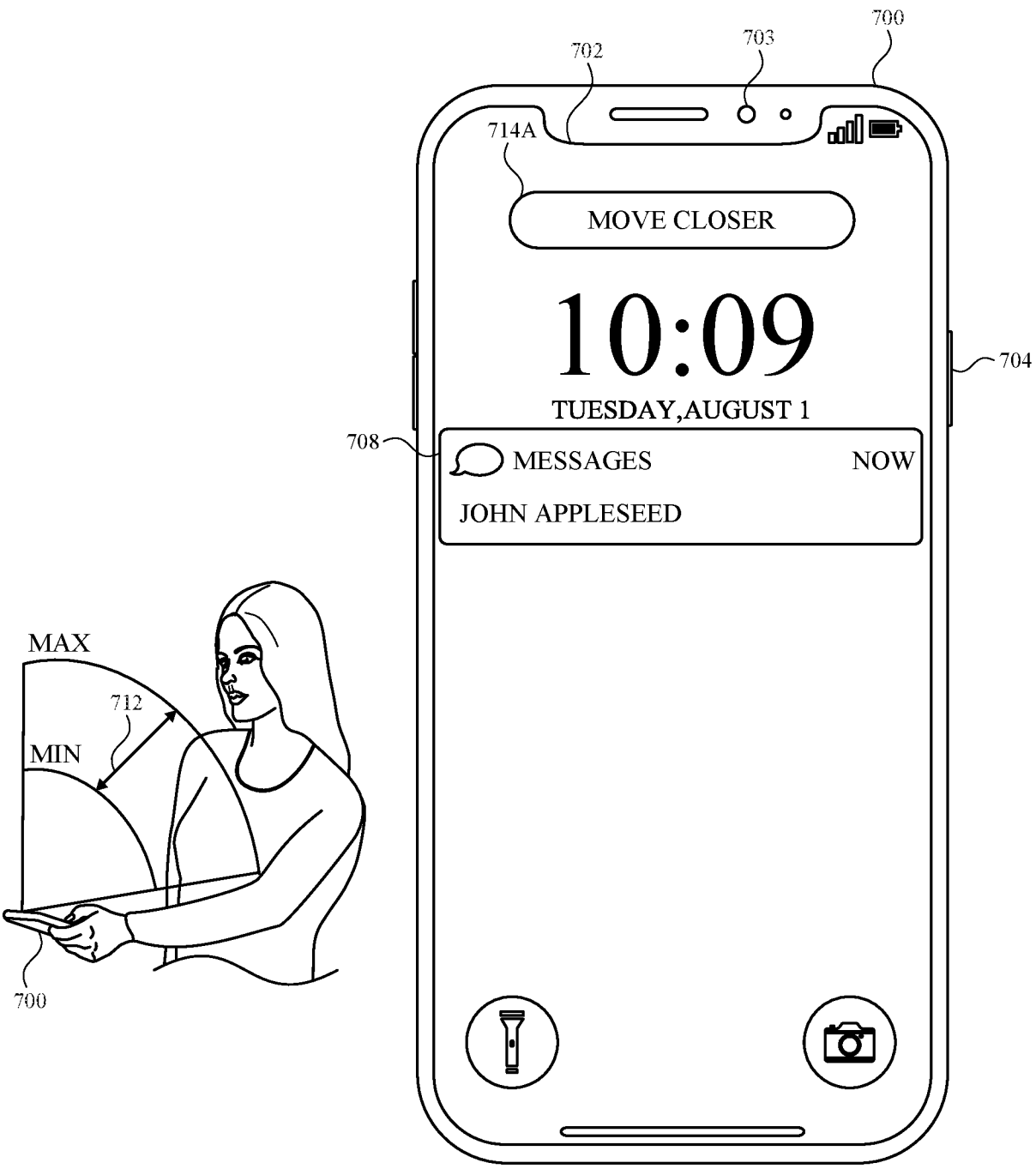


FIG. 7G

2022279466 30 Nov 2022

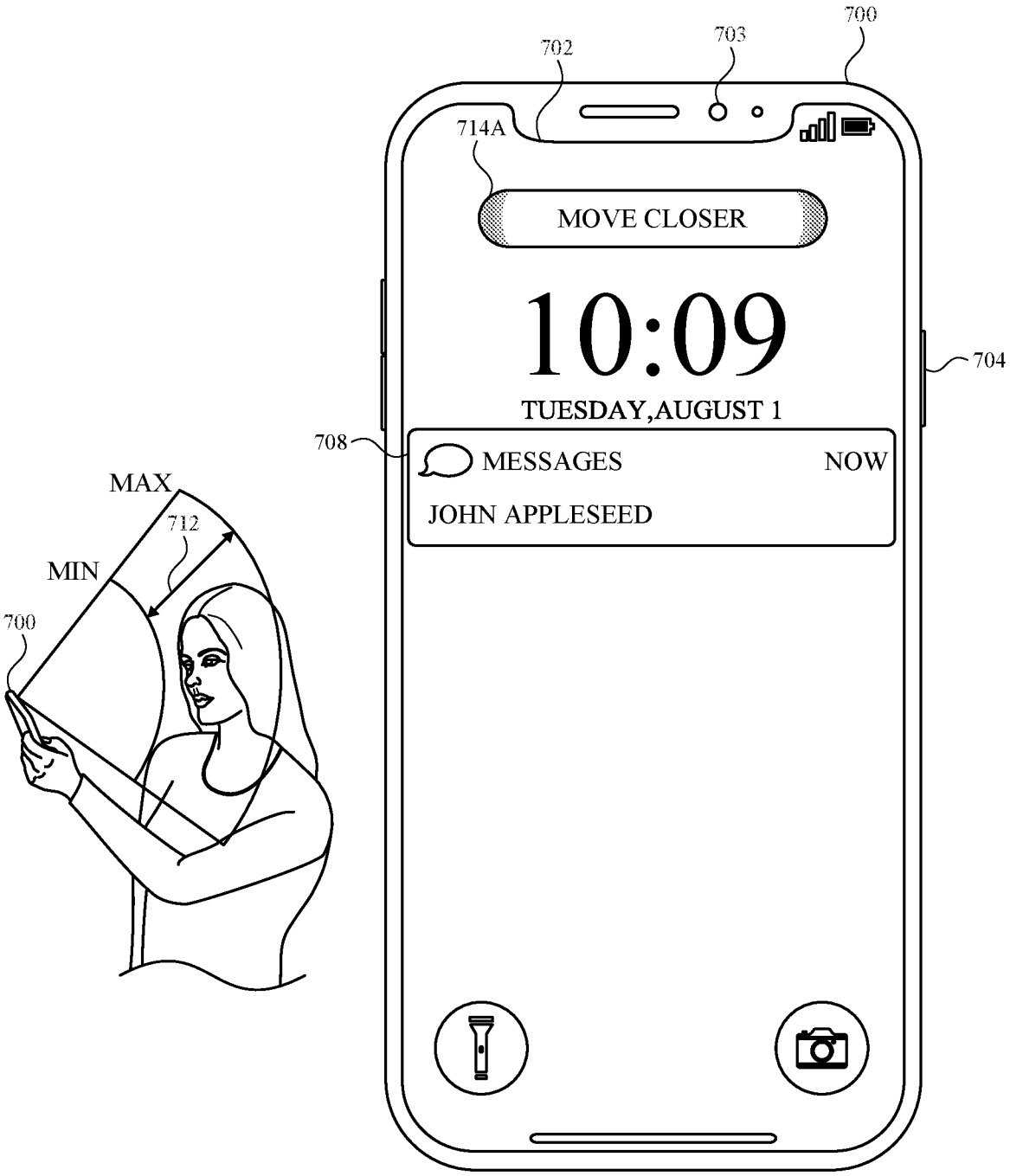


FIG. 7H

2022279466 30 Nov 2022

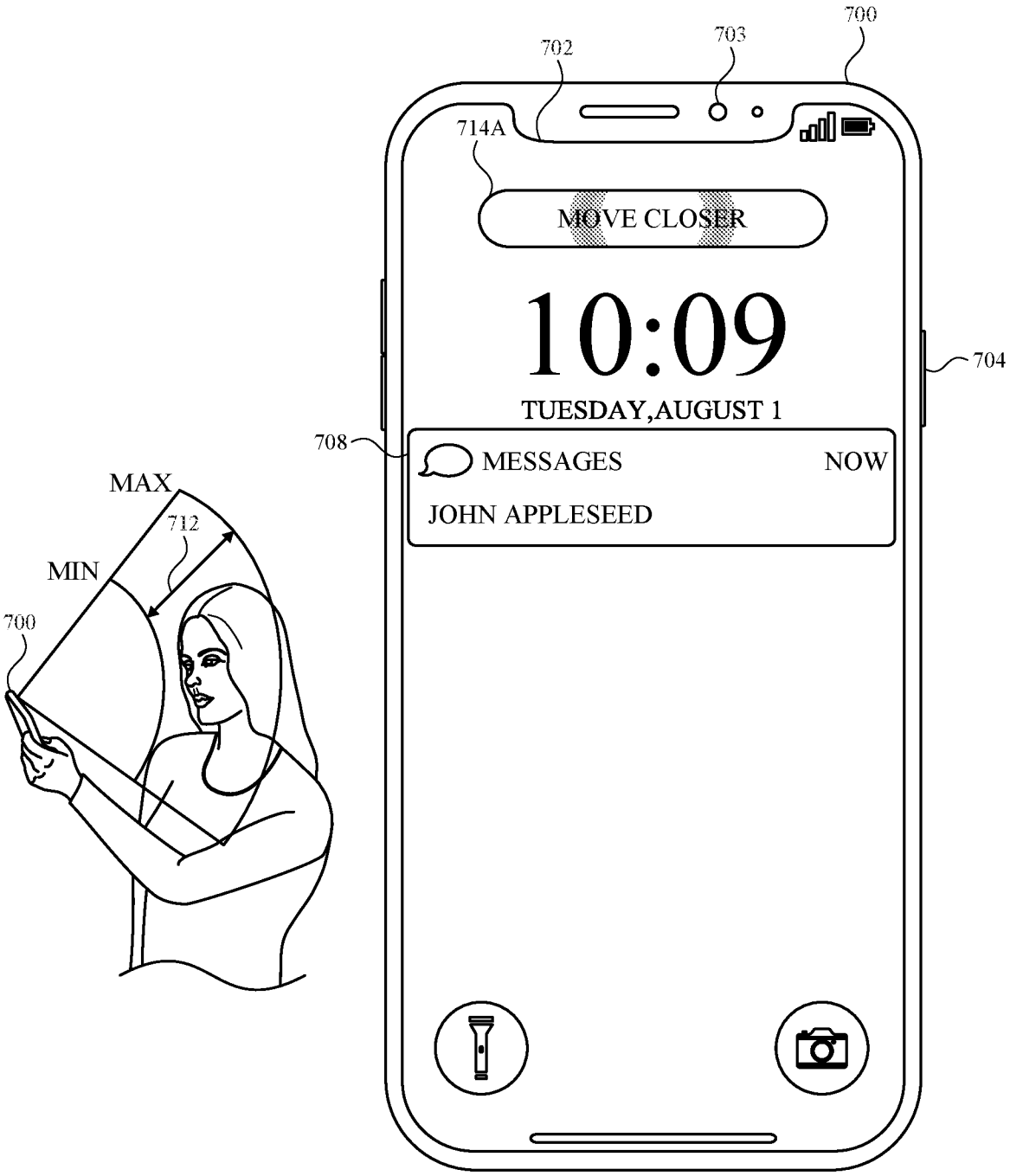


FIG. 7I

2022279466 30 Nov 2022

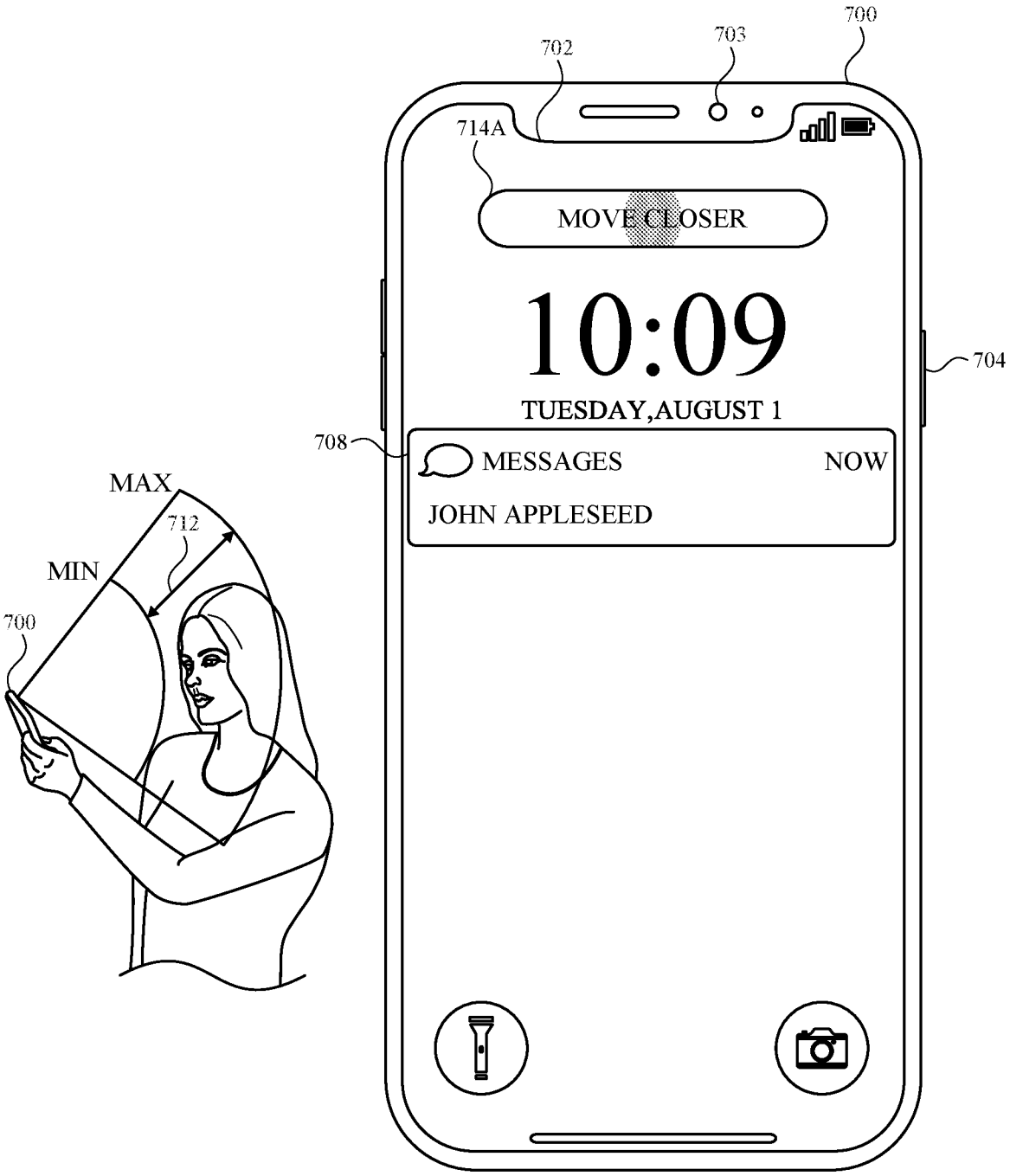


FIG. 7J

2022279466 30 Nov 2022

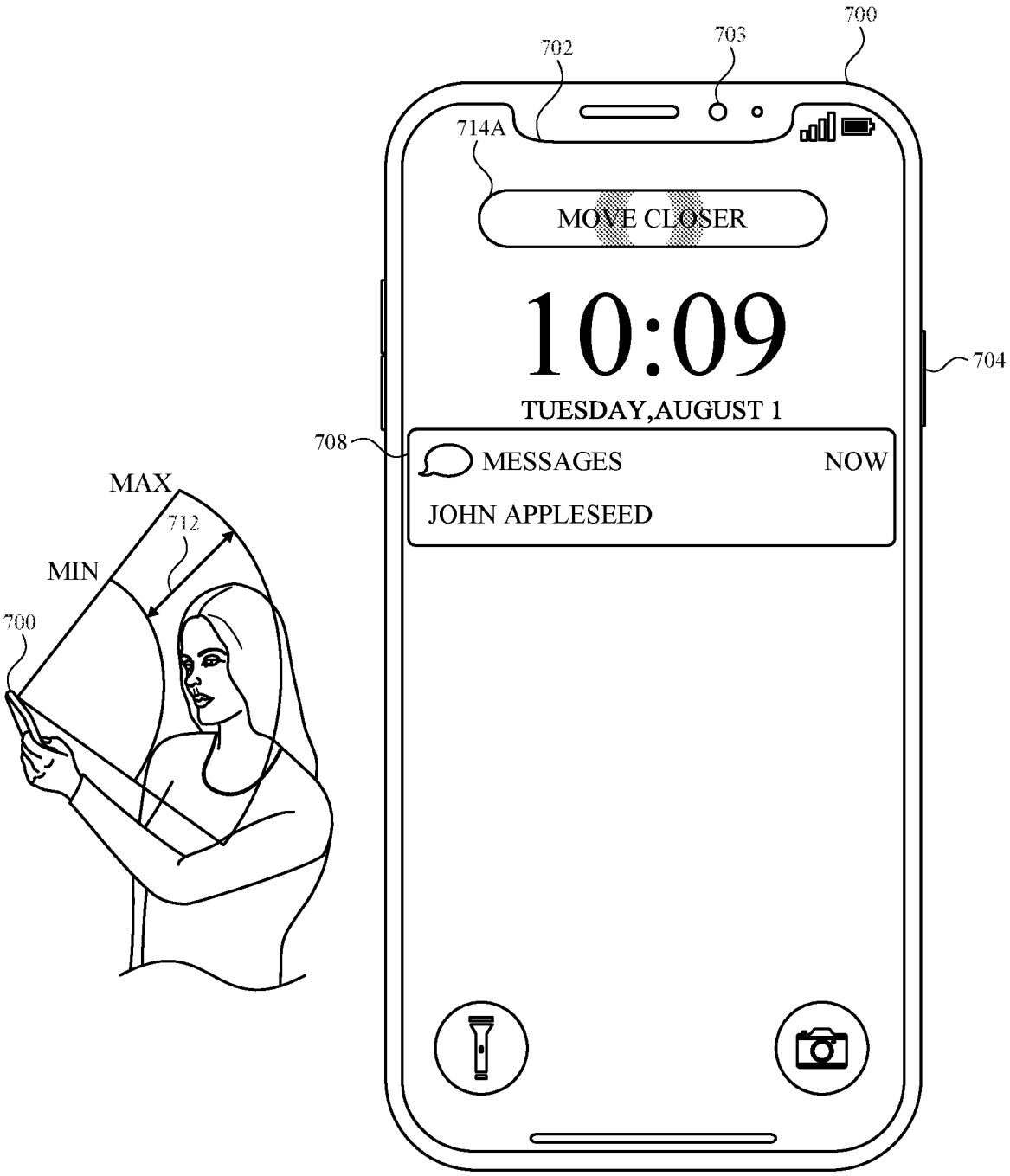


FIG. 7K

2022279466 30 Nov 2022

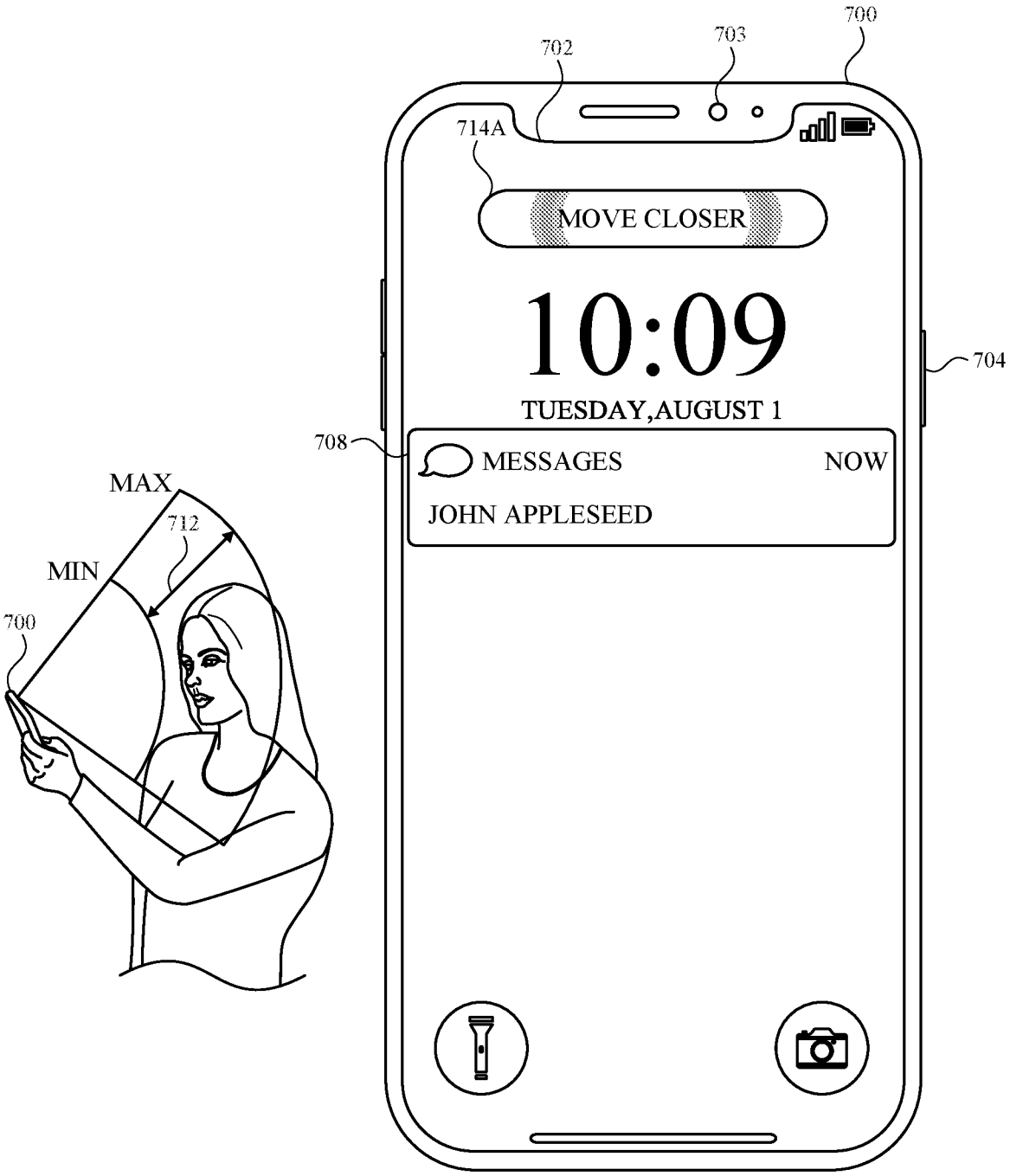


FIG. 7L

2022279466 30 Nov 2022

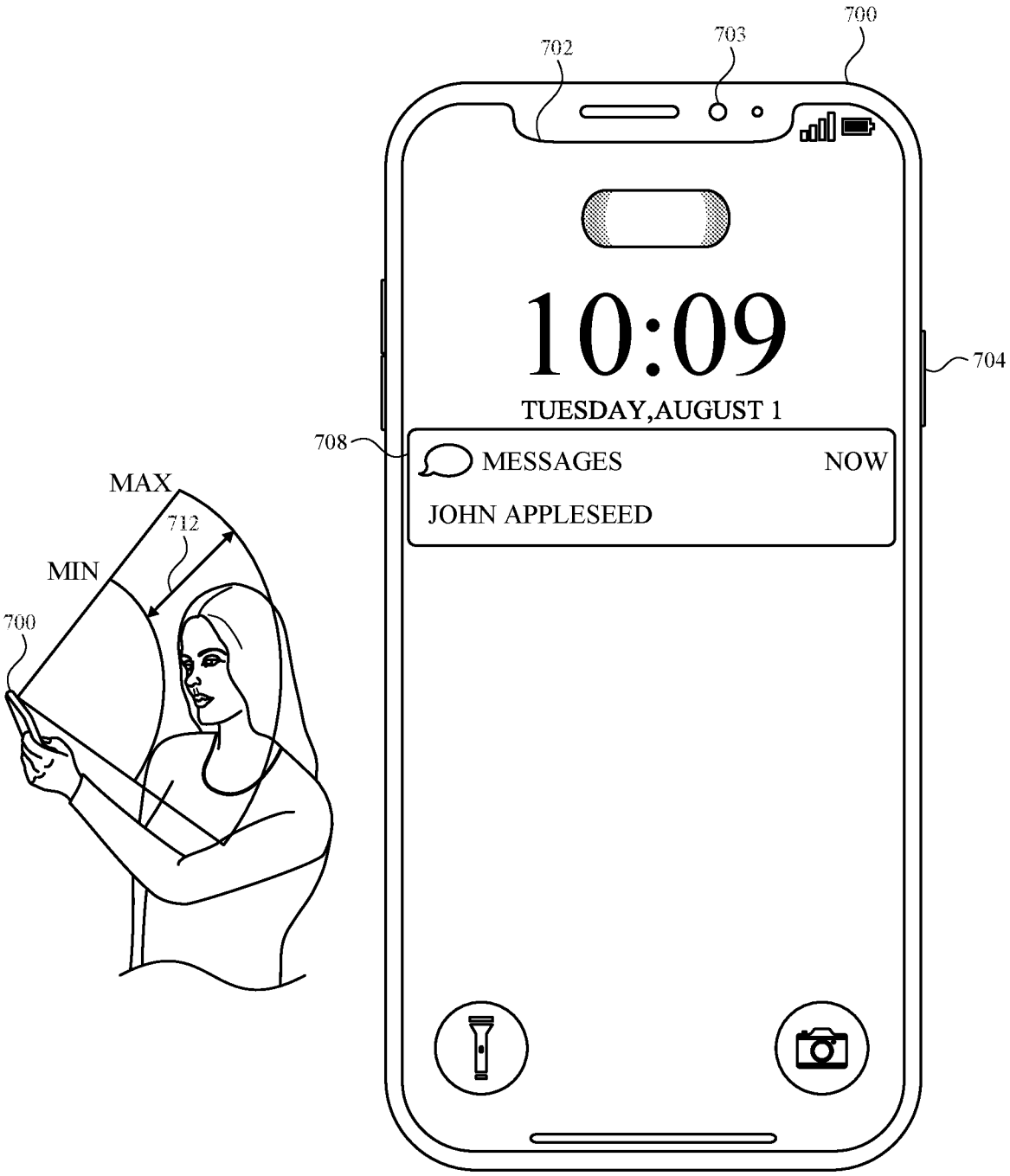


FIG. 7M

2022279466 30 Nov 2022

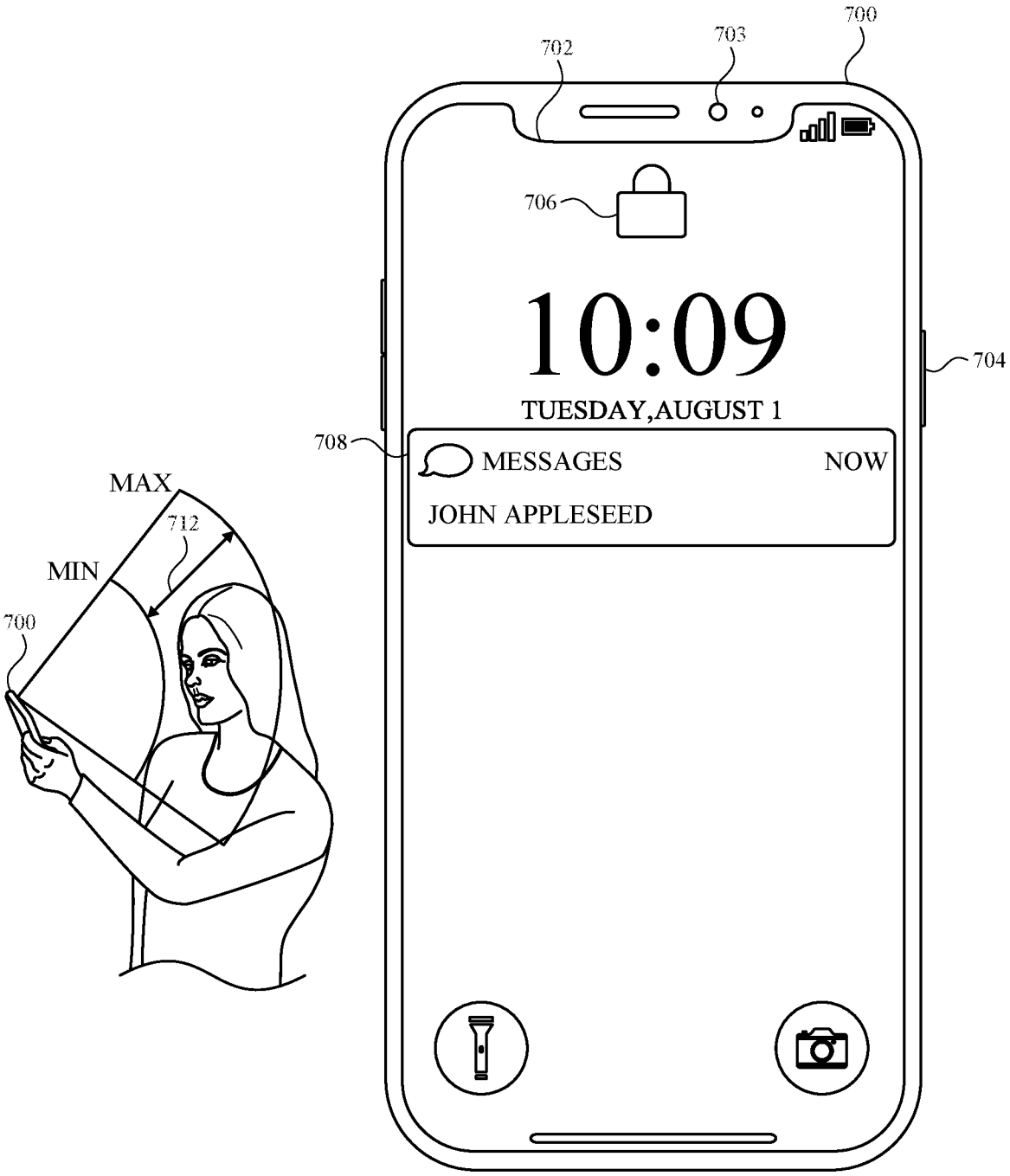


FIG. 7N

2022279466 30 Nov 2022

FIG. 7O

2022279466 30 Nov 2022

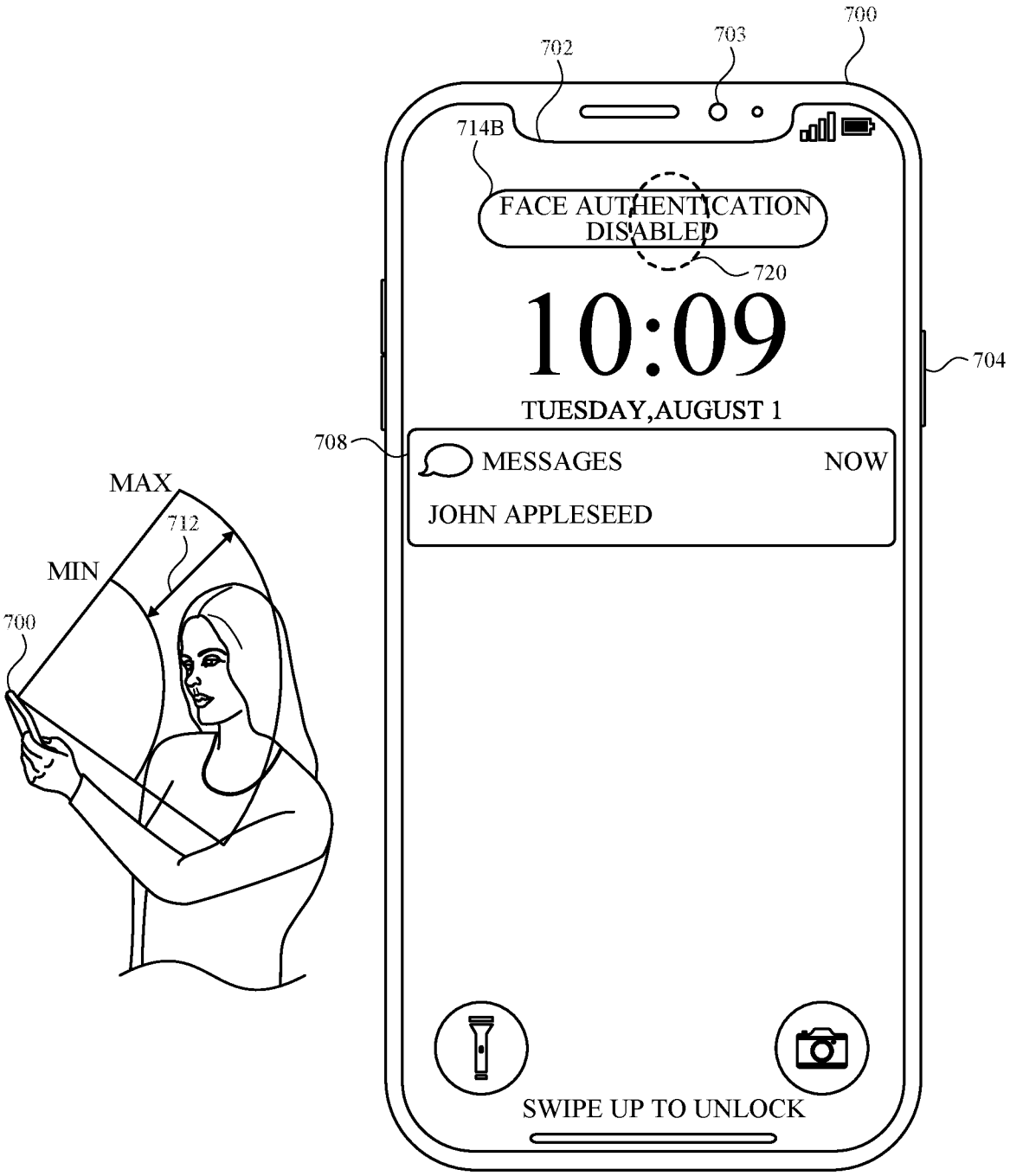


FIG. 7P

2022279466 30 Nov 2022

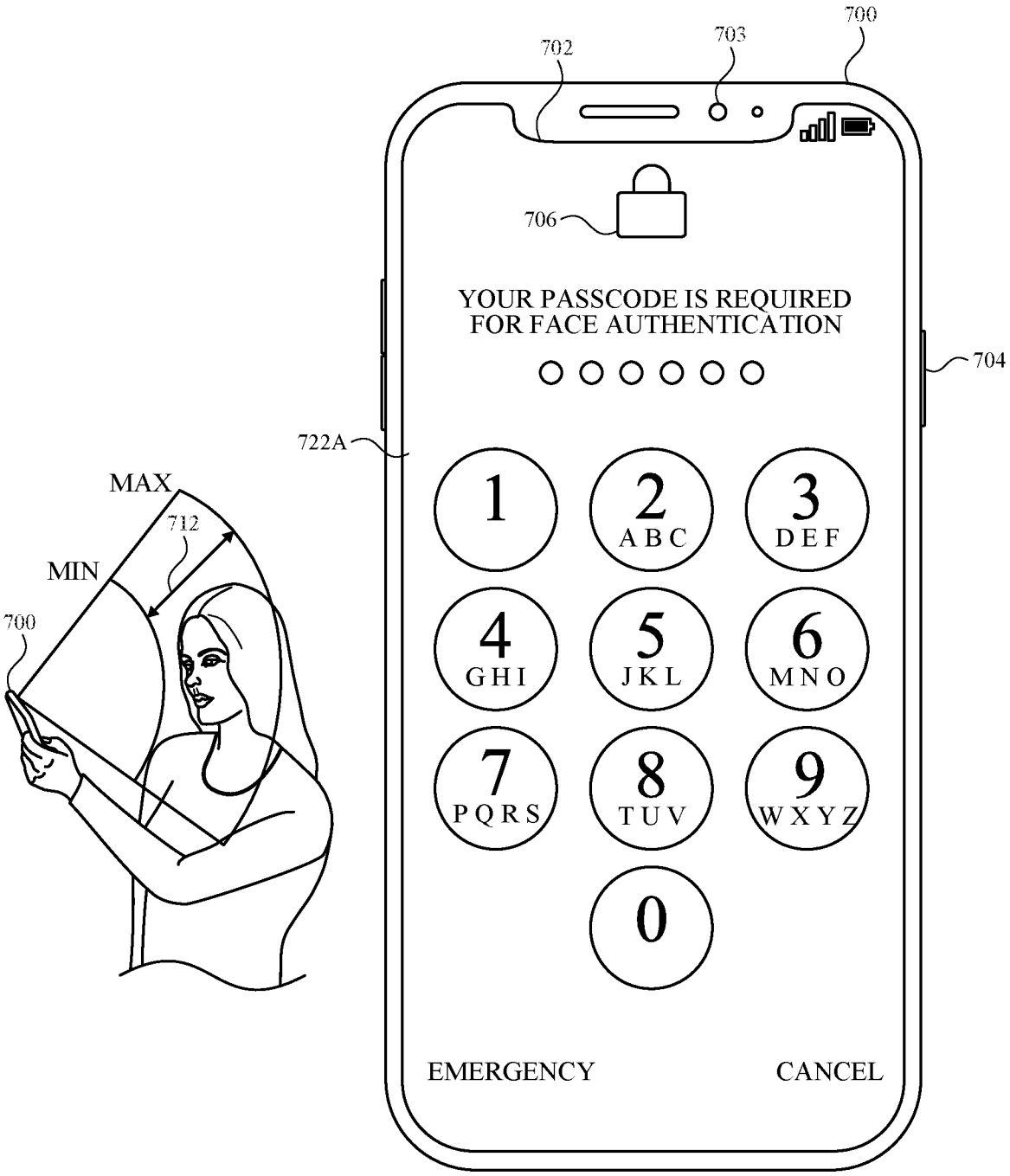


FIG. 7Q

2022279466 30 Nov 2022

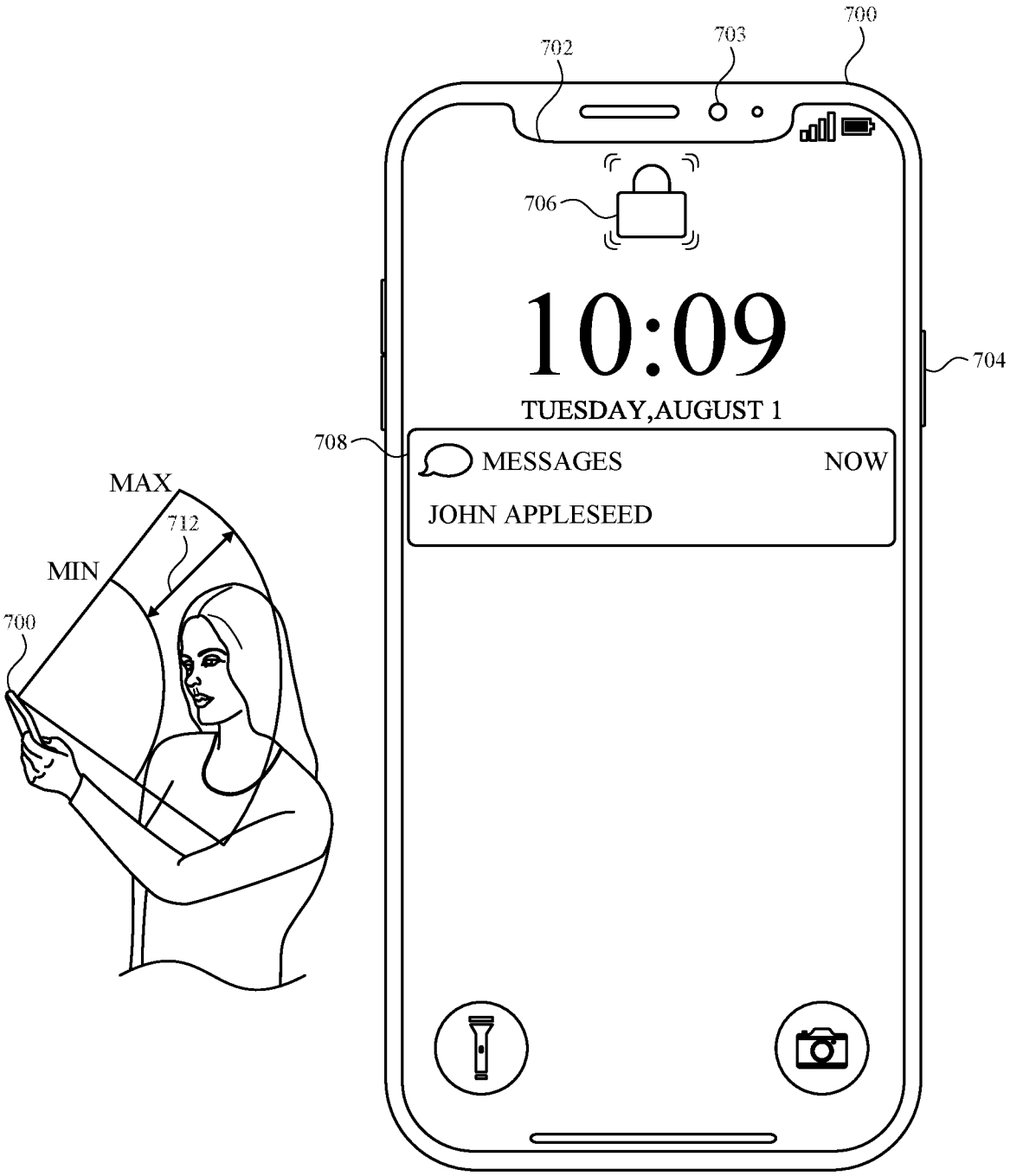


FIG. 7R

2022279466 30 Nov 2022

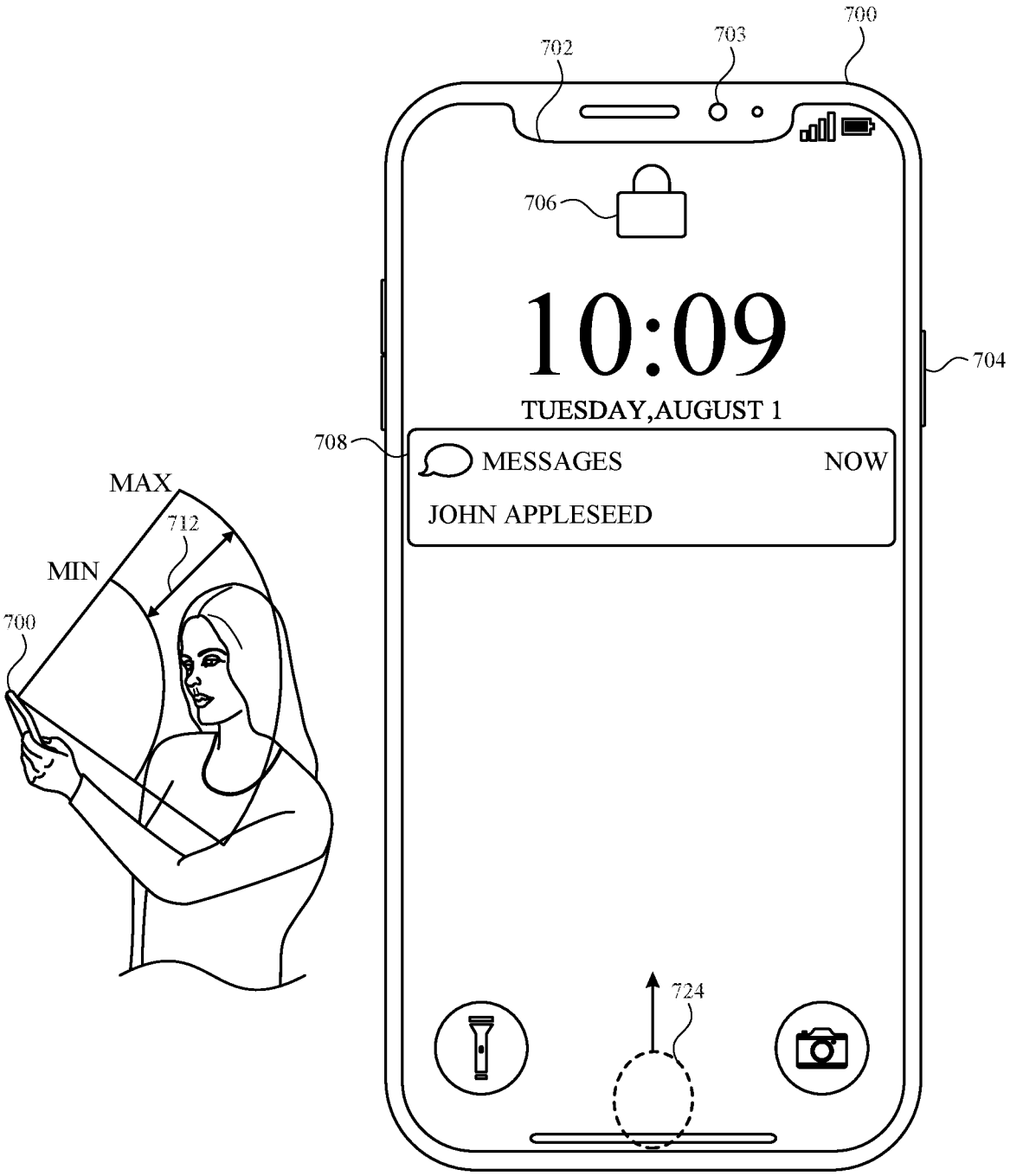


FIG. 7S

2022279466 30 Nov 2022

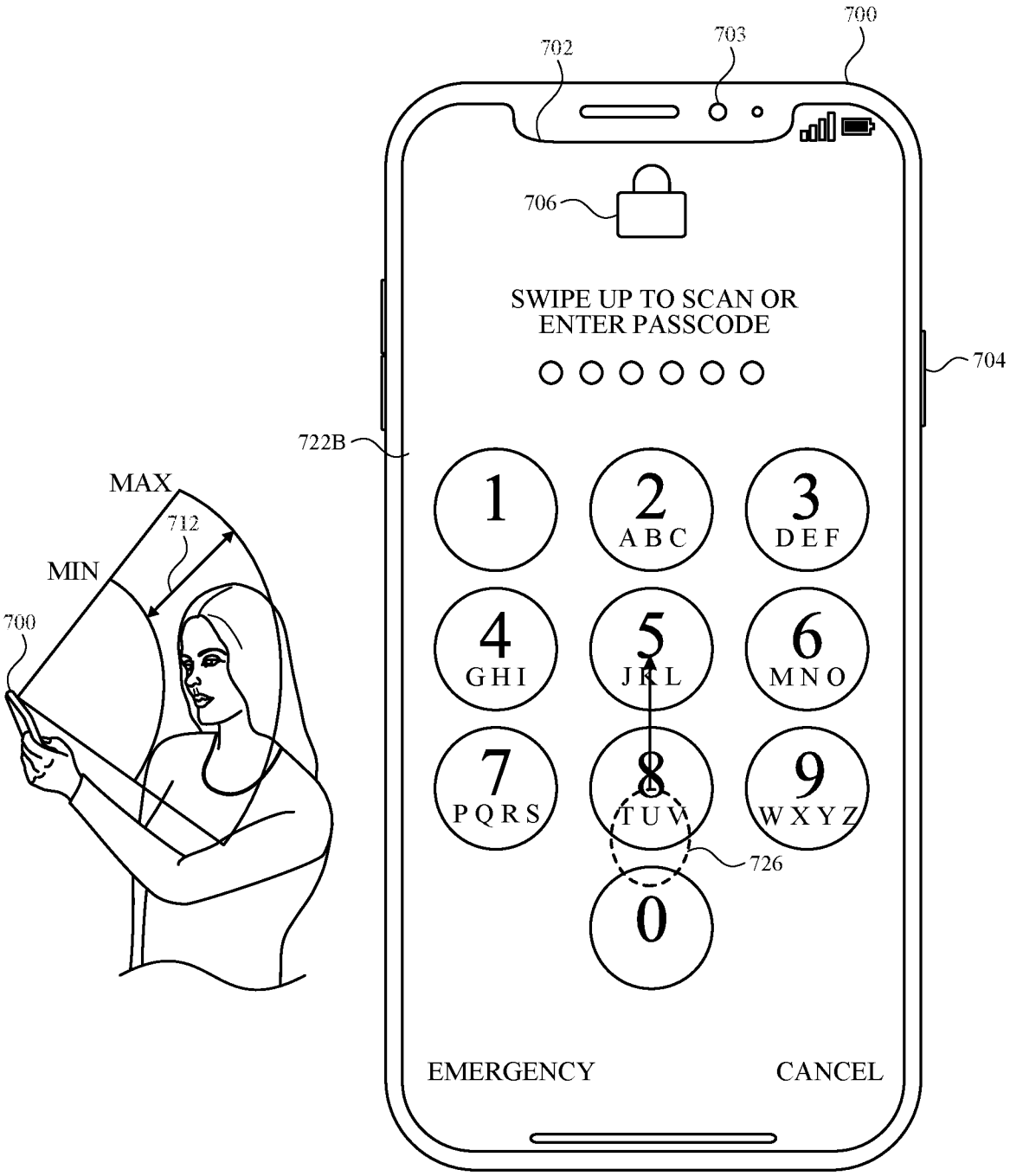


FIG. 7T

2022279466 30 Nov 2022

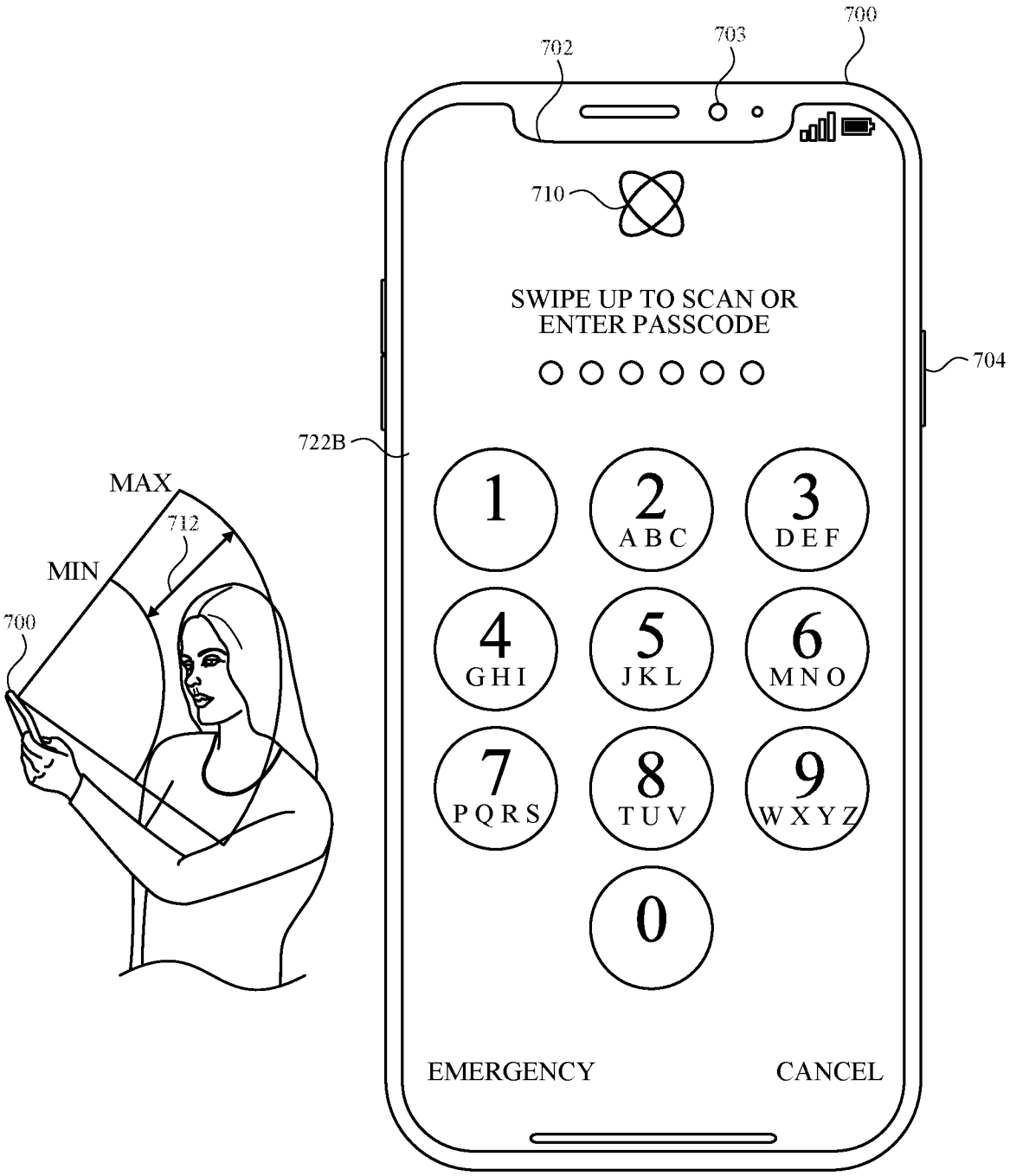


FIG. 7U

2022279466 30 Nov 2022

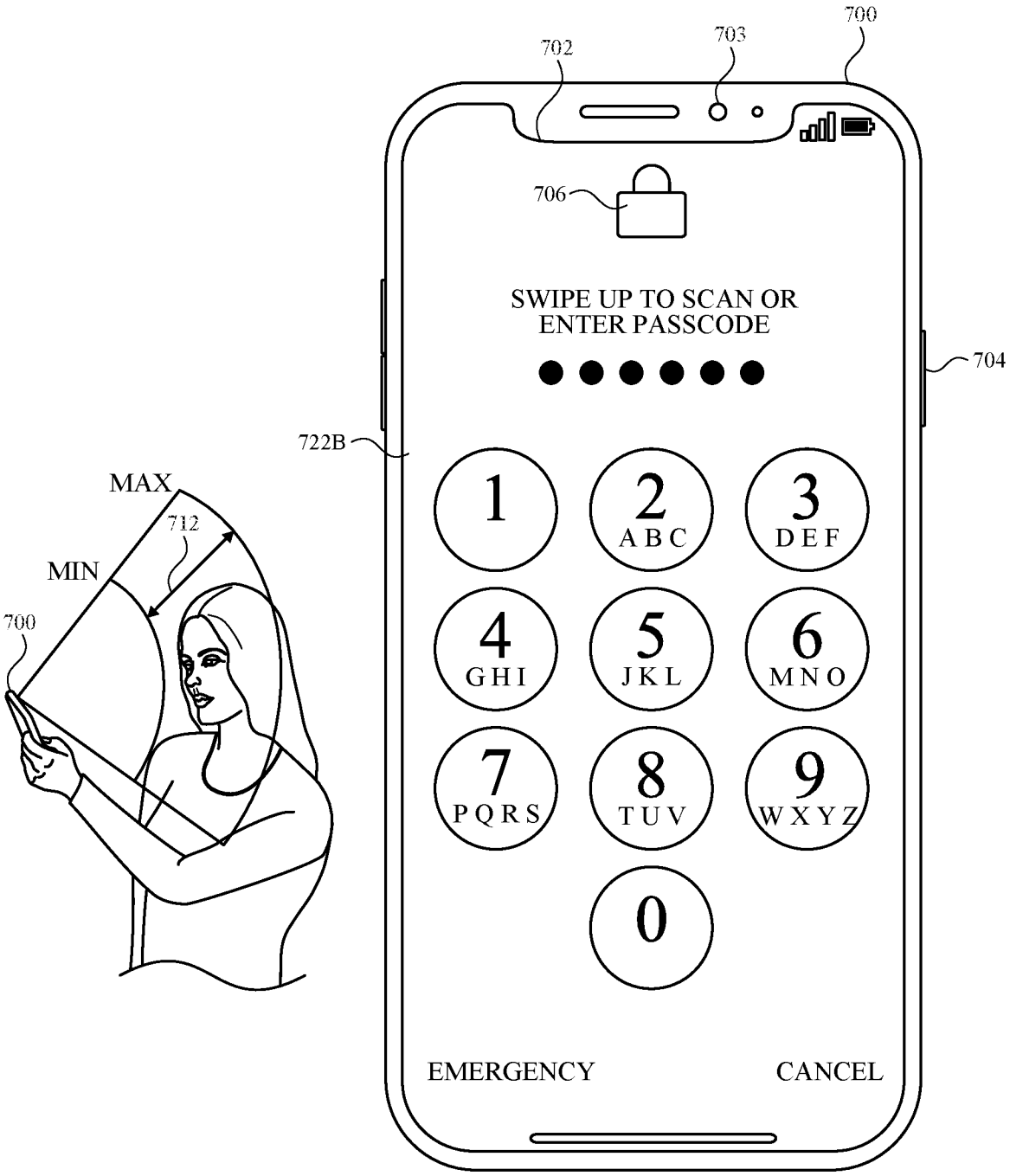


FIG. 7V

2022279466 30 Nov 2022

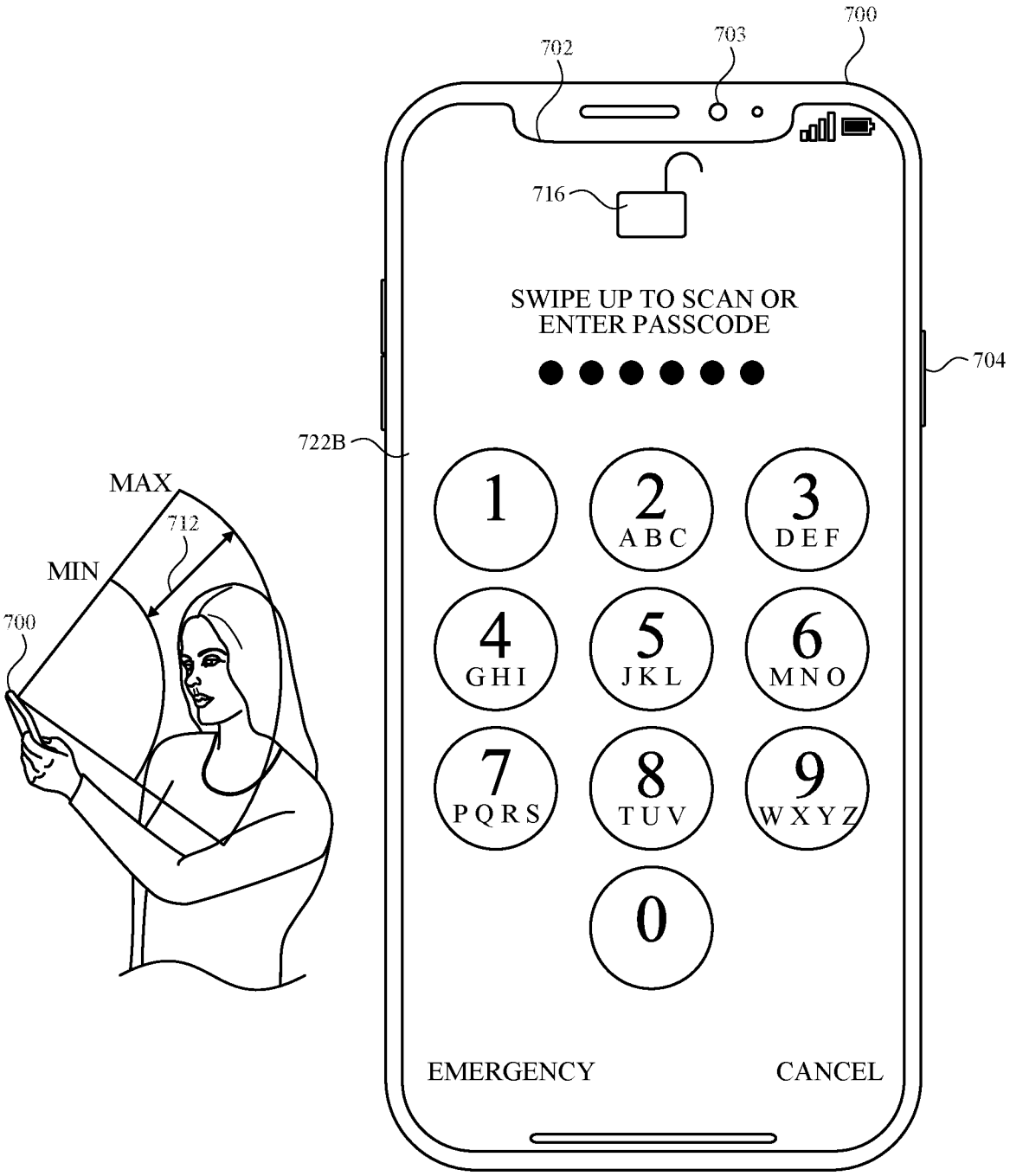


FIG. 7W

2022279466 30 Nov 2022

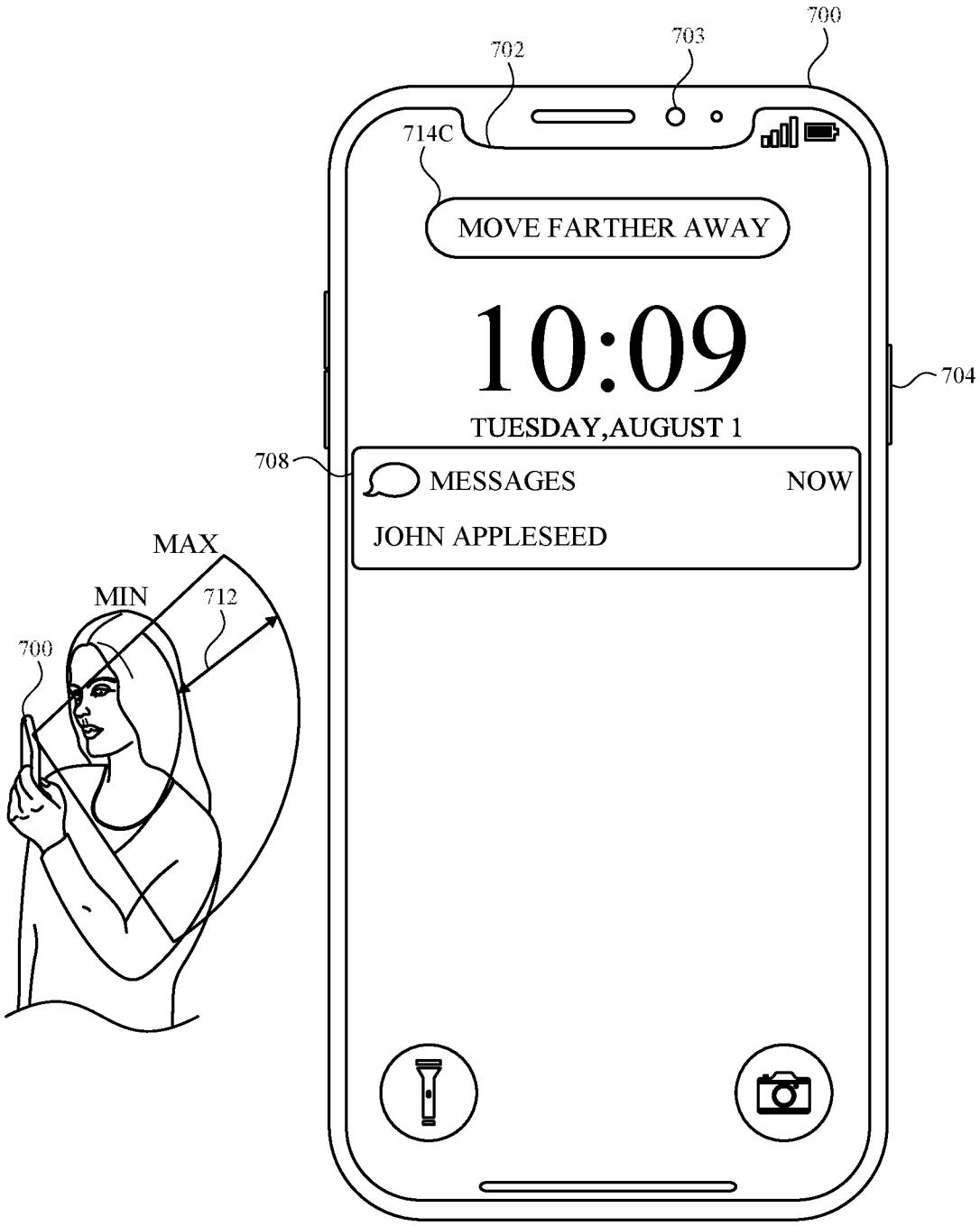


FIG. 7X

2022279466 30 Nov 2022

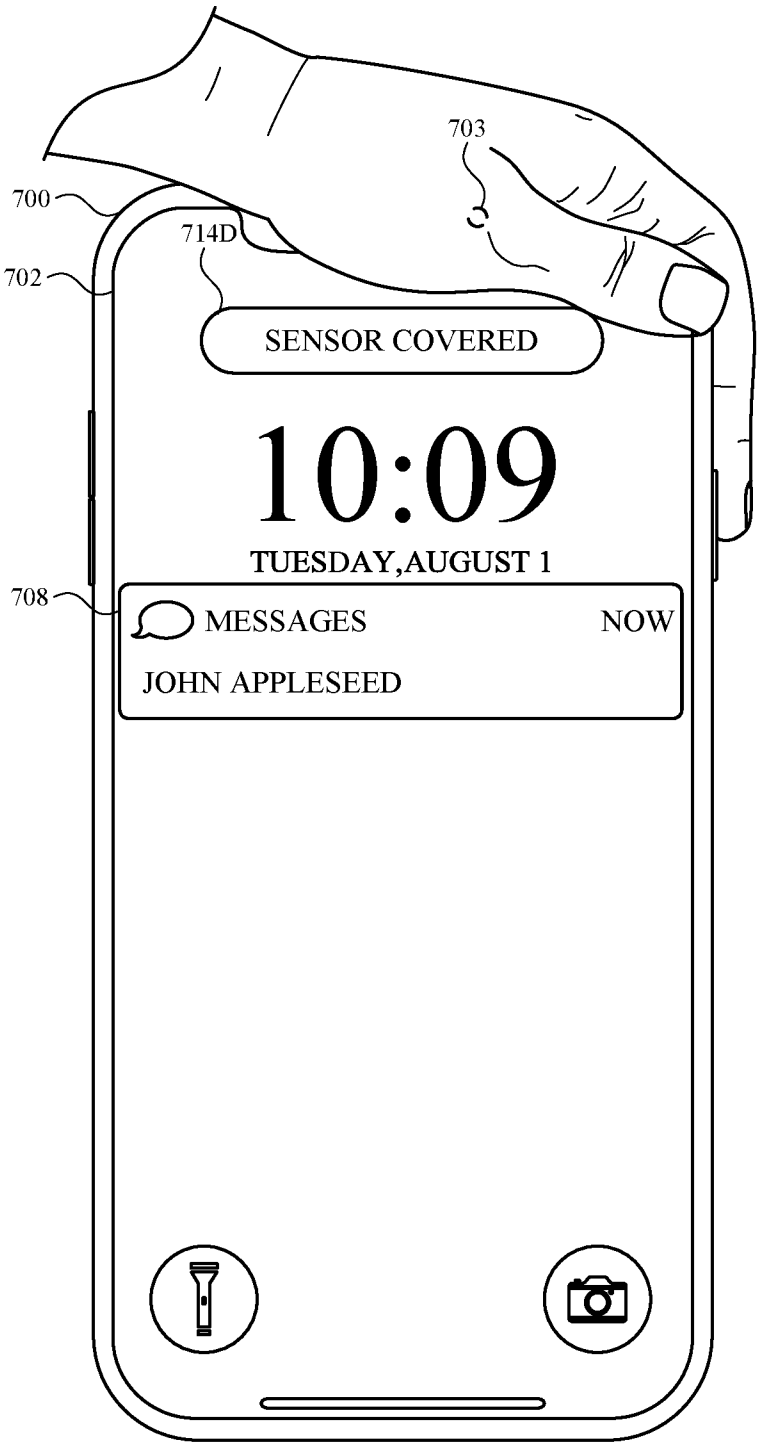


FIG. 7Y

2022279466 30 Nov 2022

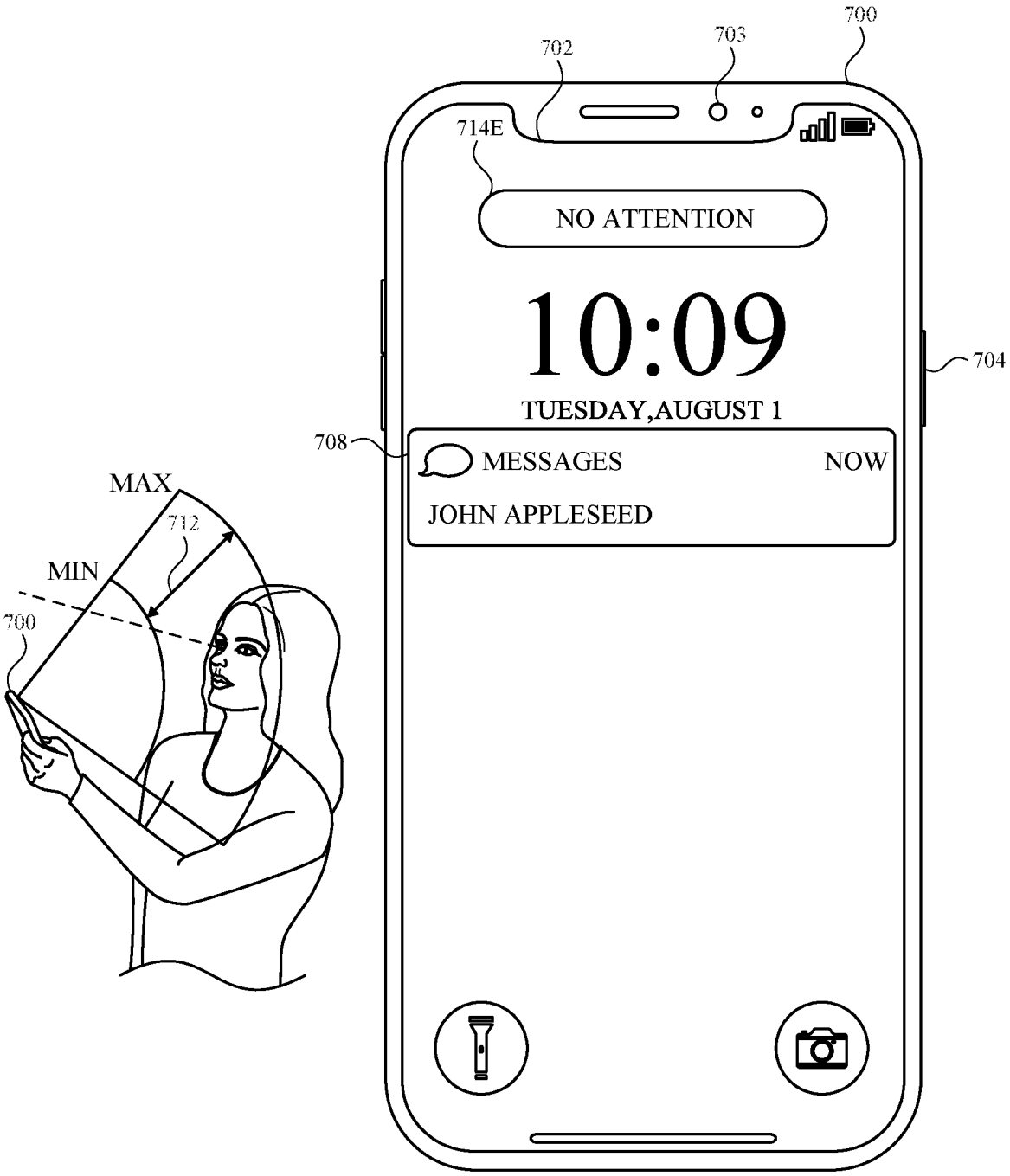


FIG. 7Z

2022279466 30 Nov 2022

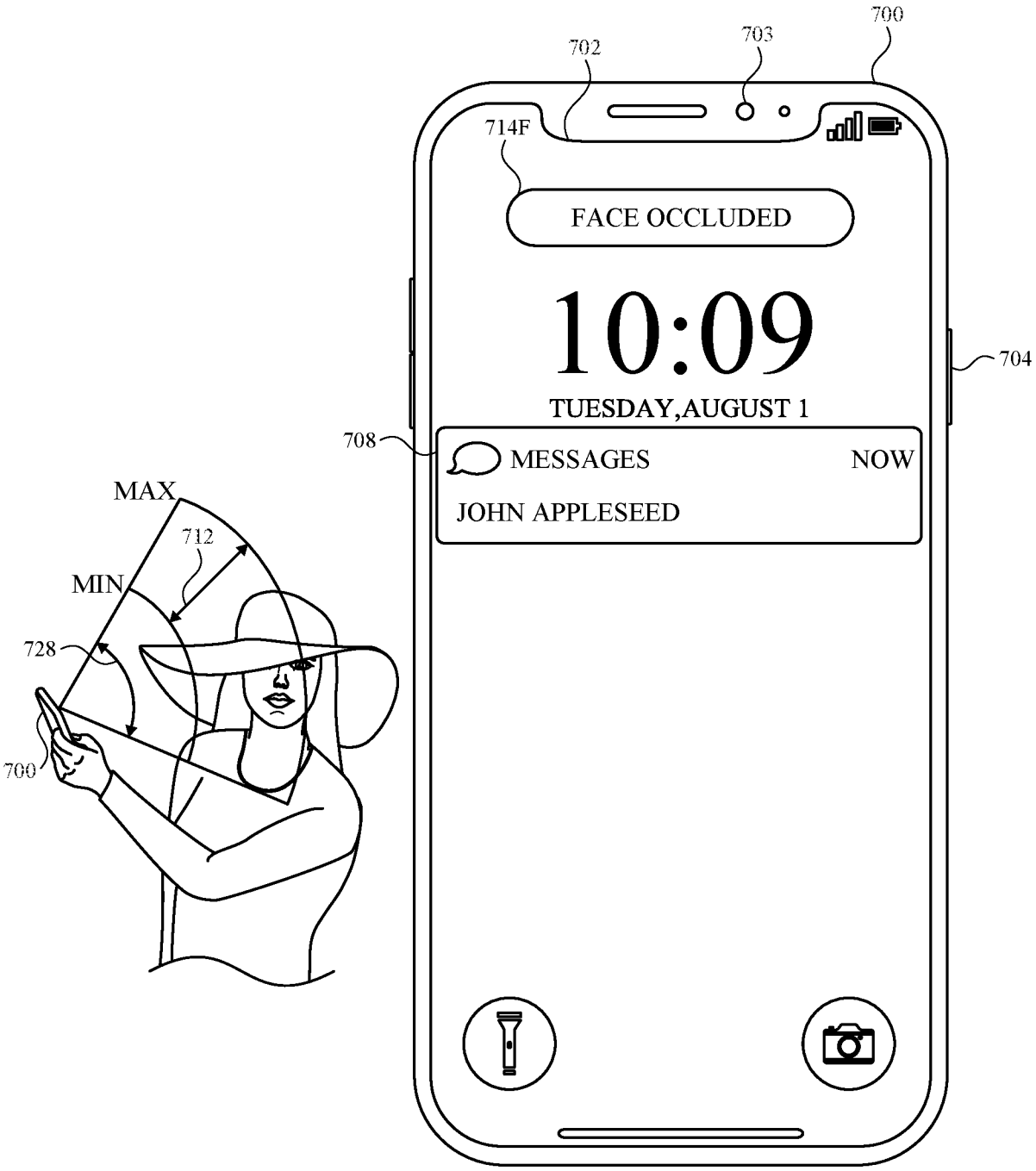


FIG. 7AA

2022279466 30 Nov 2022

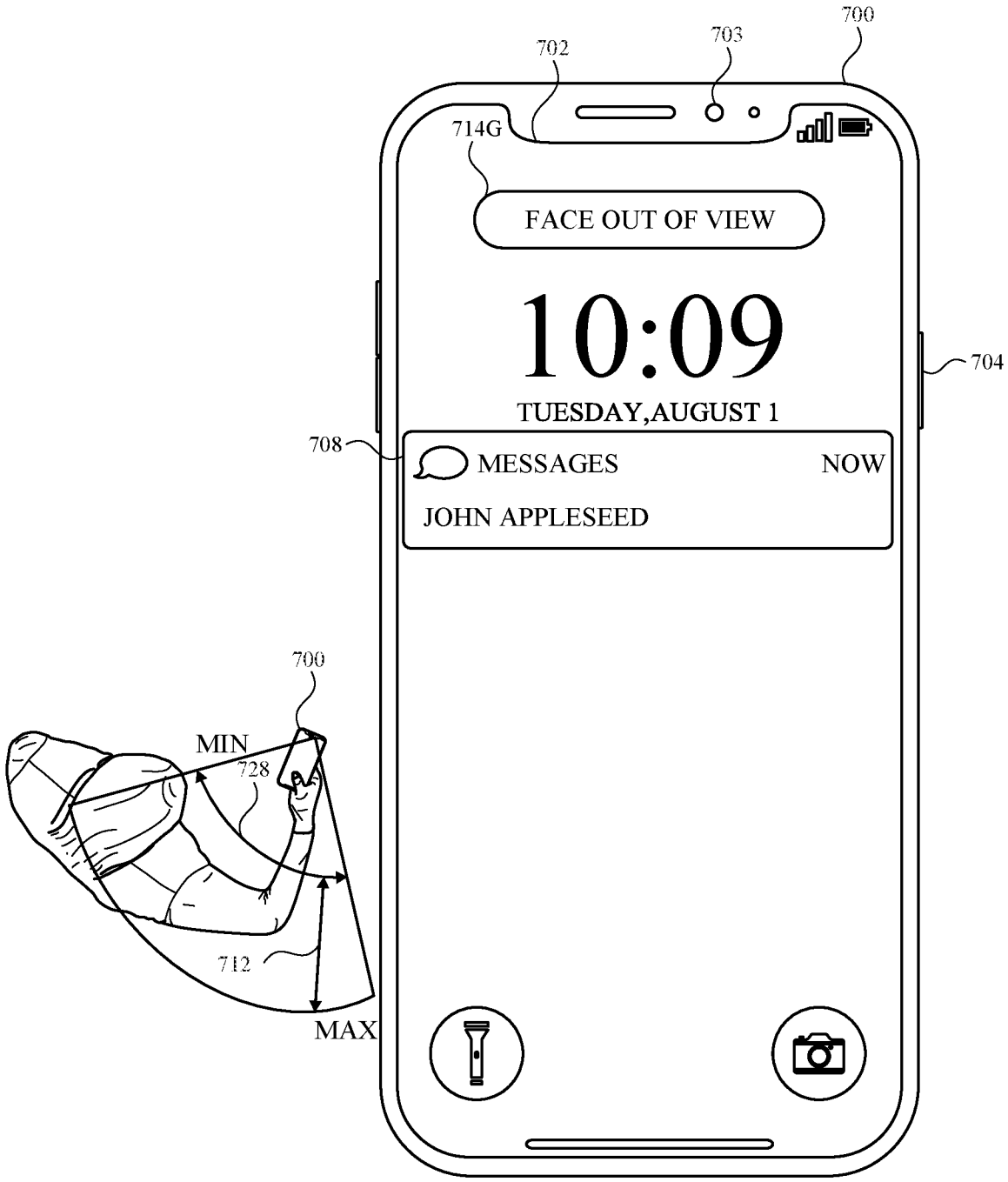


FIG. 7AB

2022279466 30 Nov 2022

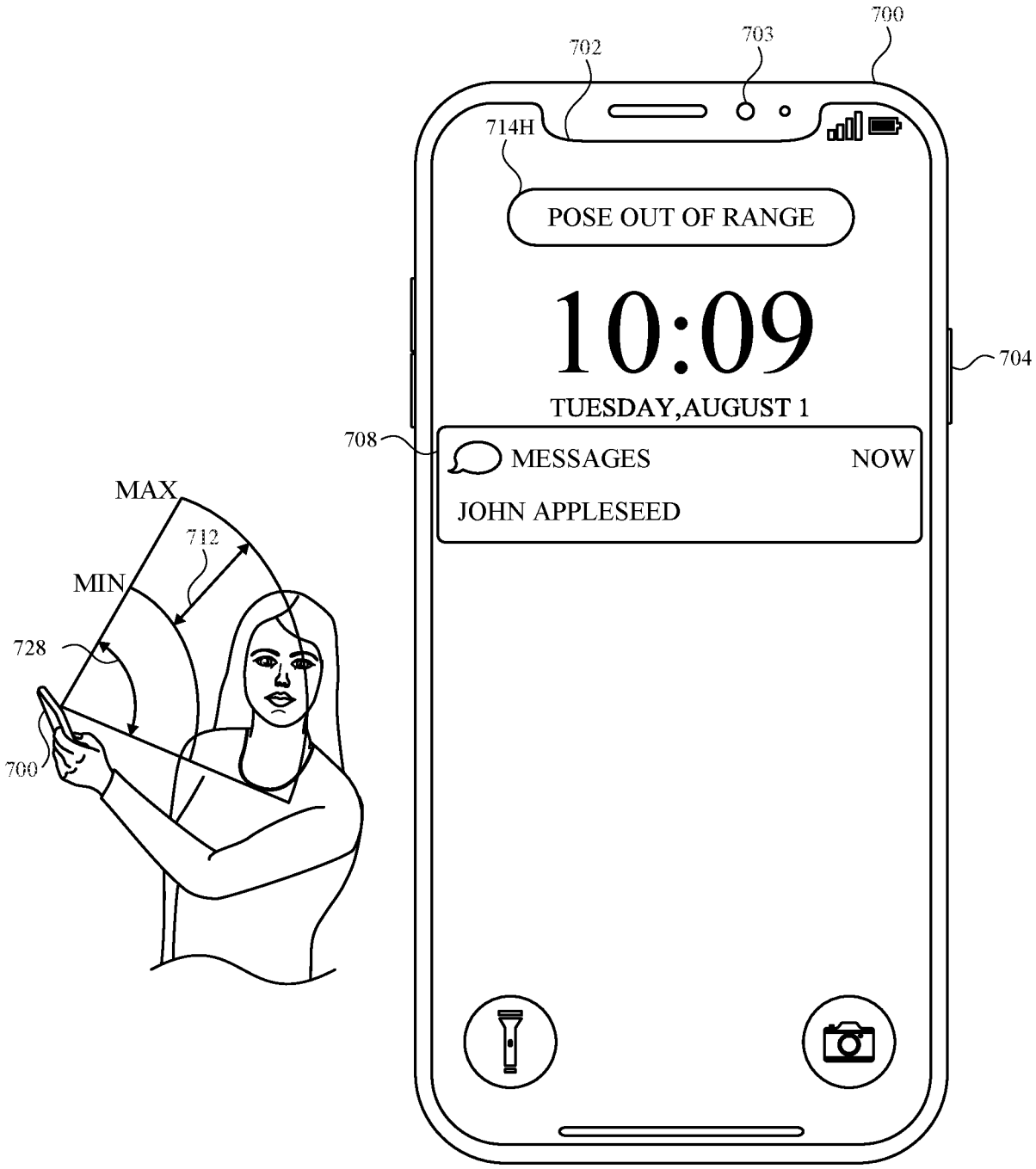


FIG. 7AC

2022279466 30 Nov 2022

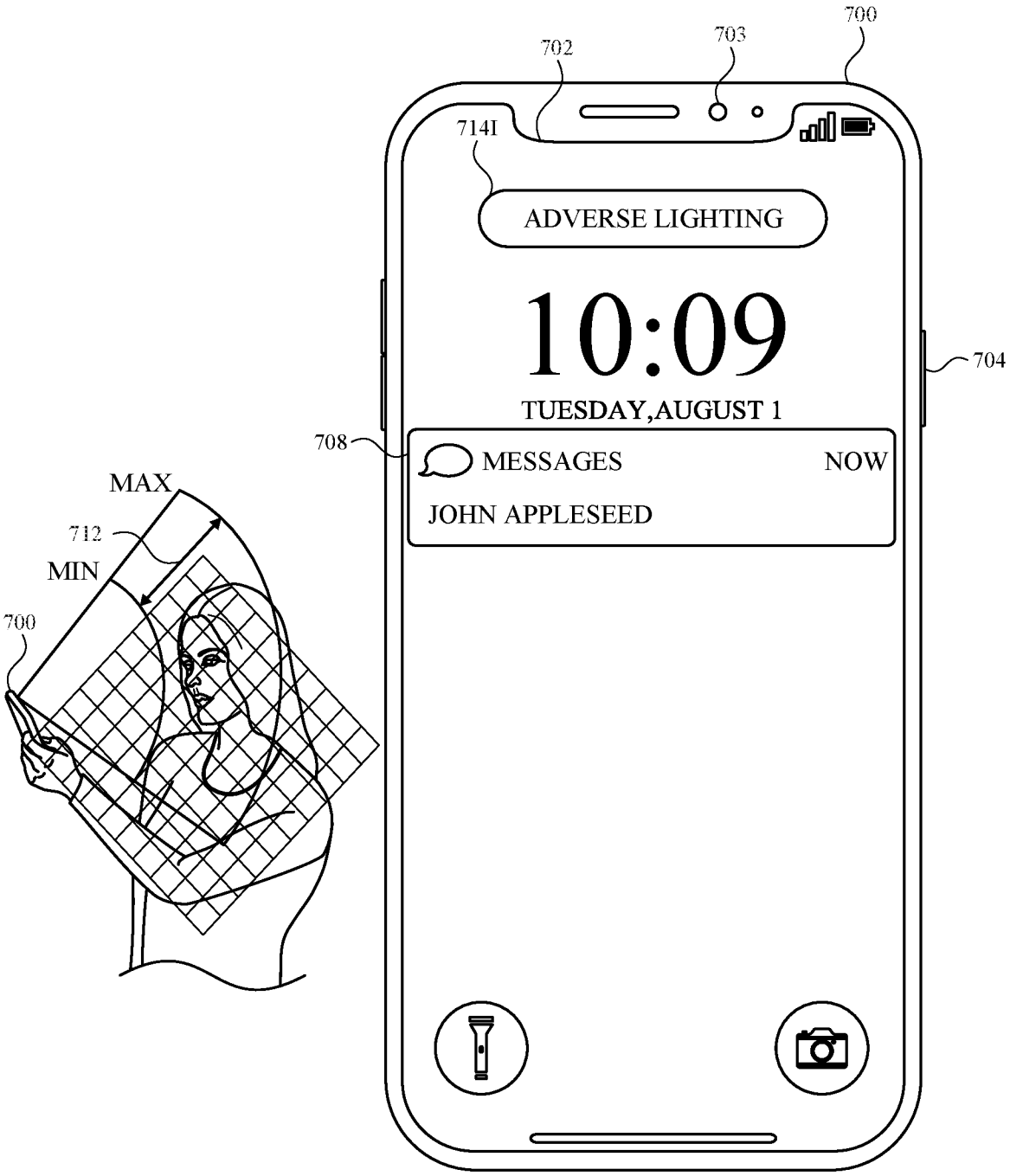


FIG. 7AD

30 Nov 2022
2022279466

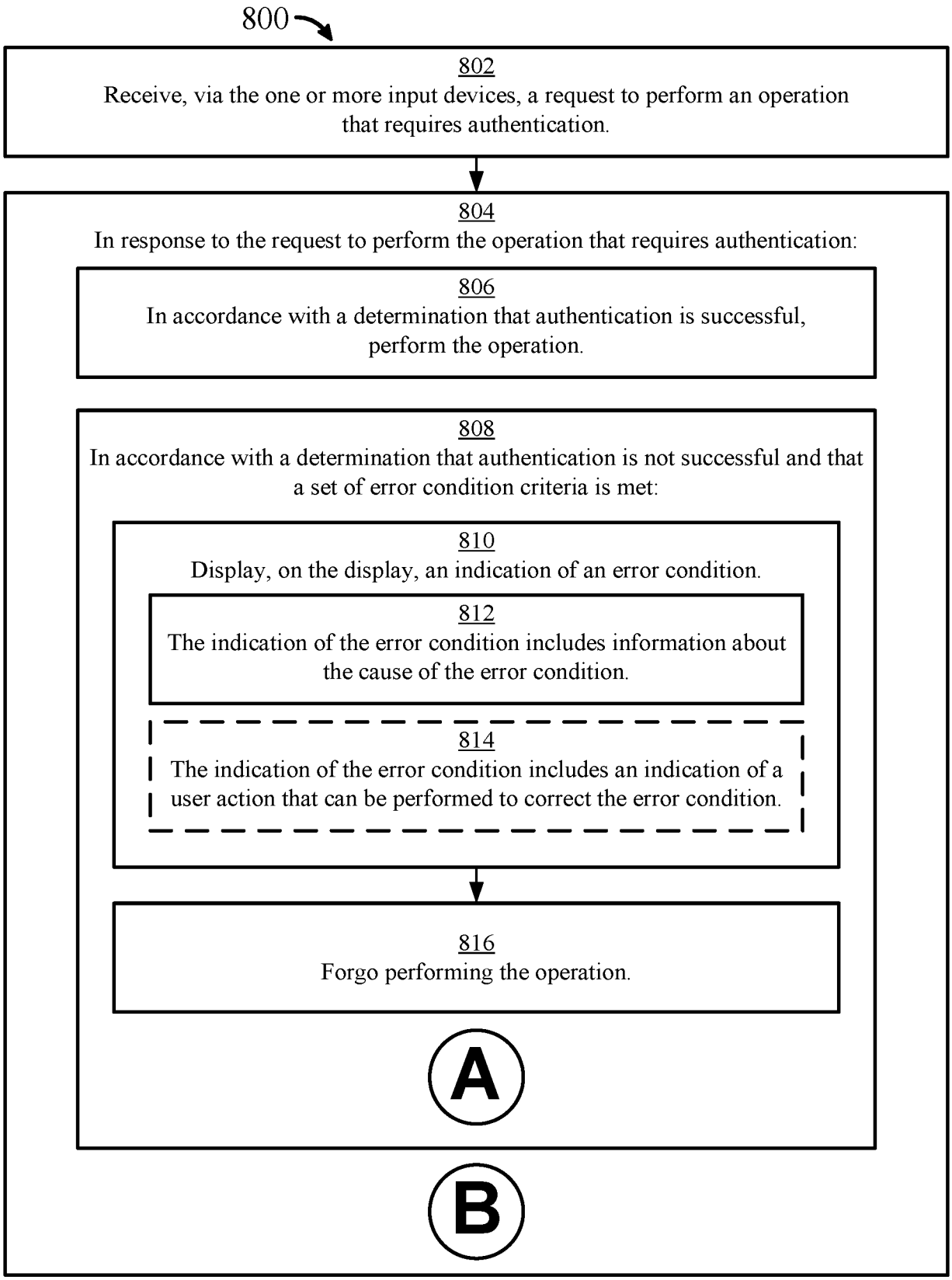


FIG. 8A

2022279466 30 Nov 2022

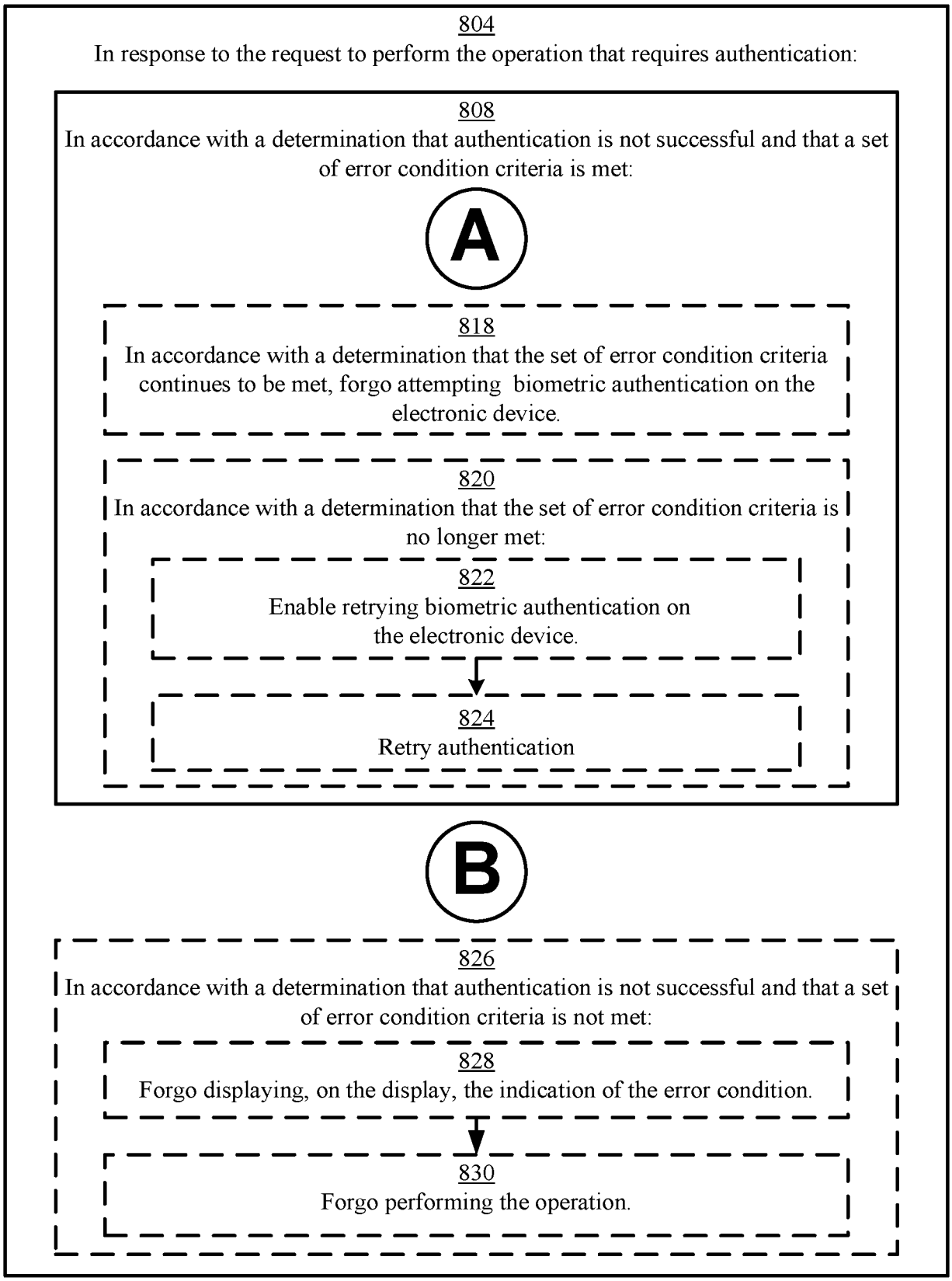


FIG. 8B

2022279466 30 Nov 2022

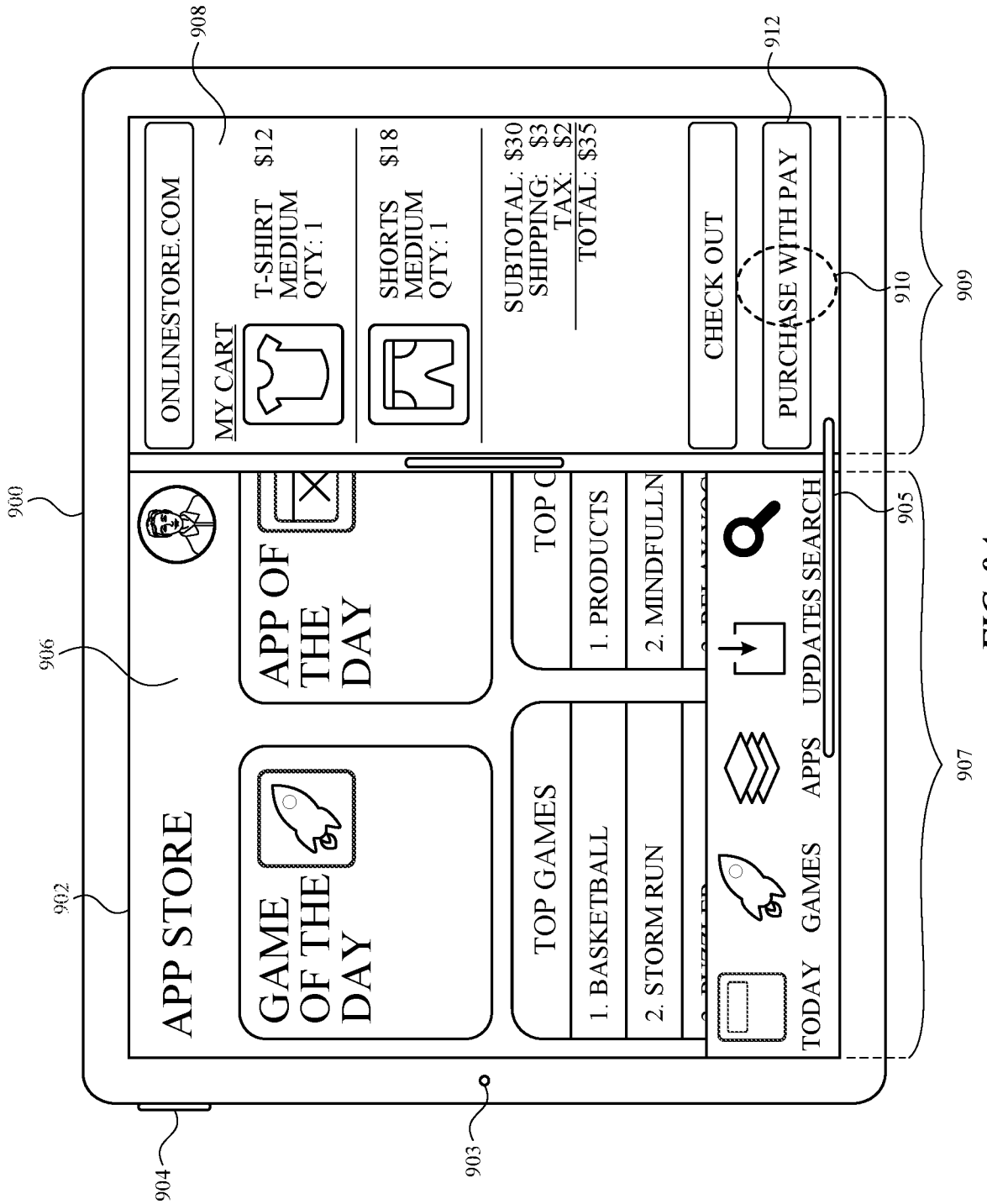


FIG. 9A

2022279466 30 Nov 2022

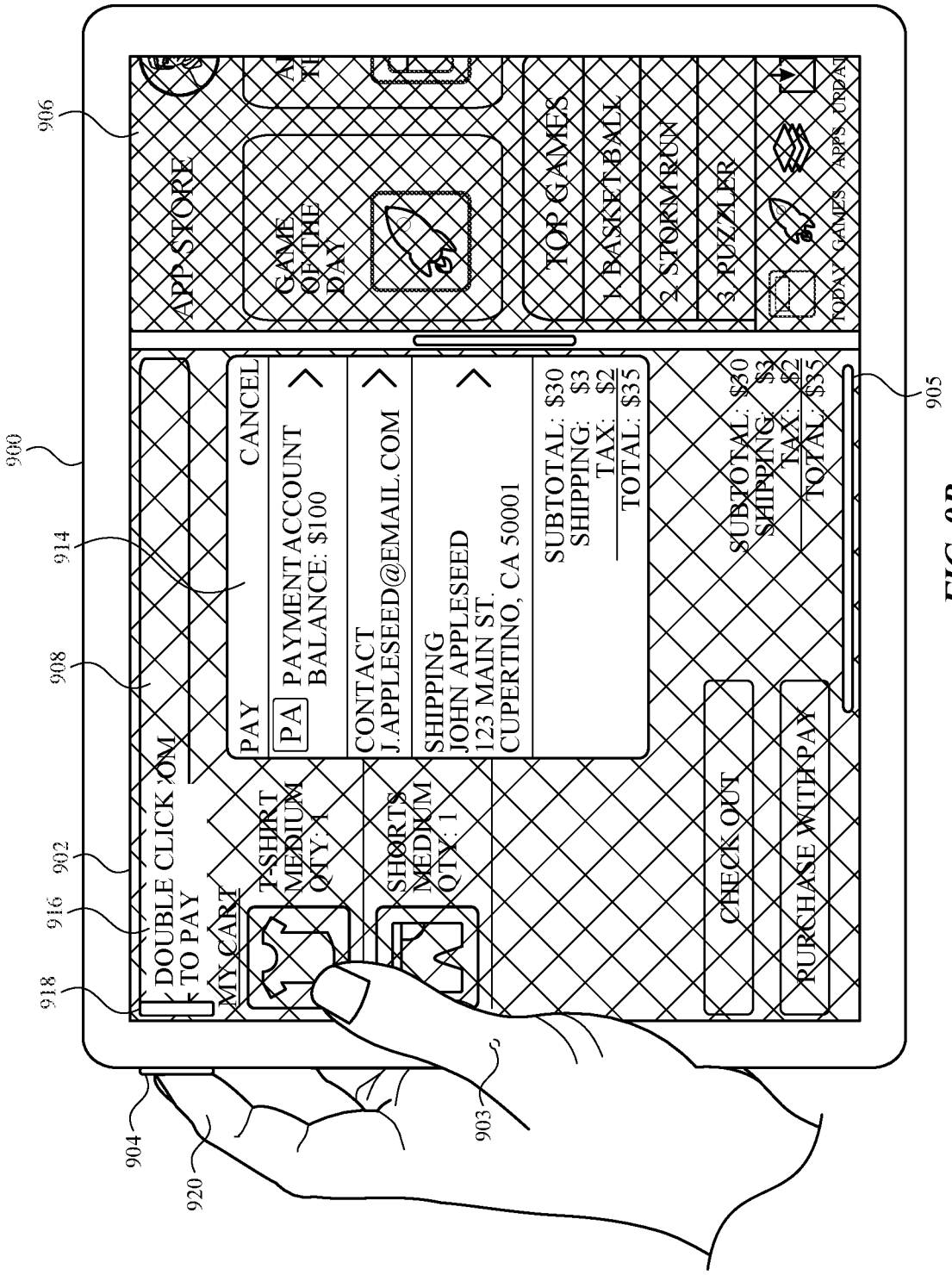


FIG. 9B

2022279466 30 Nov 2022

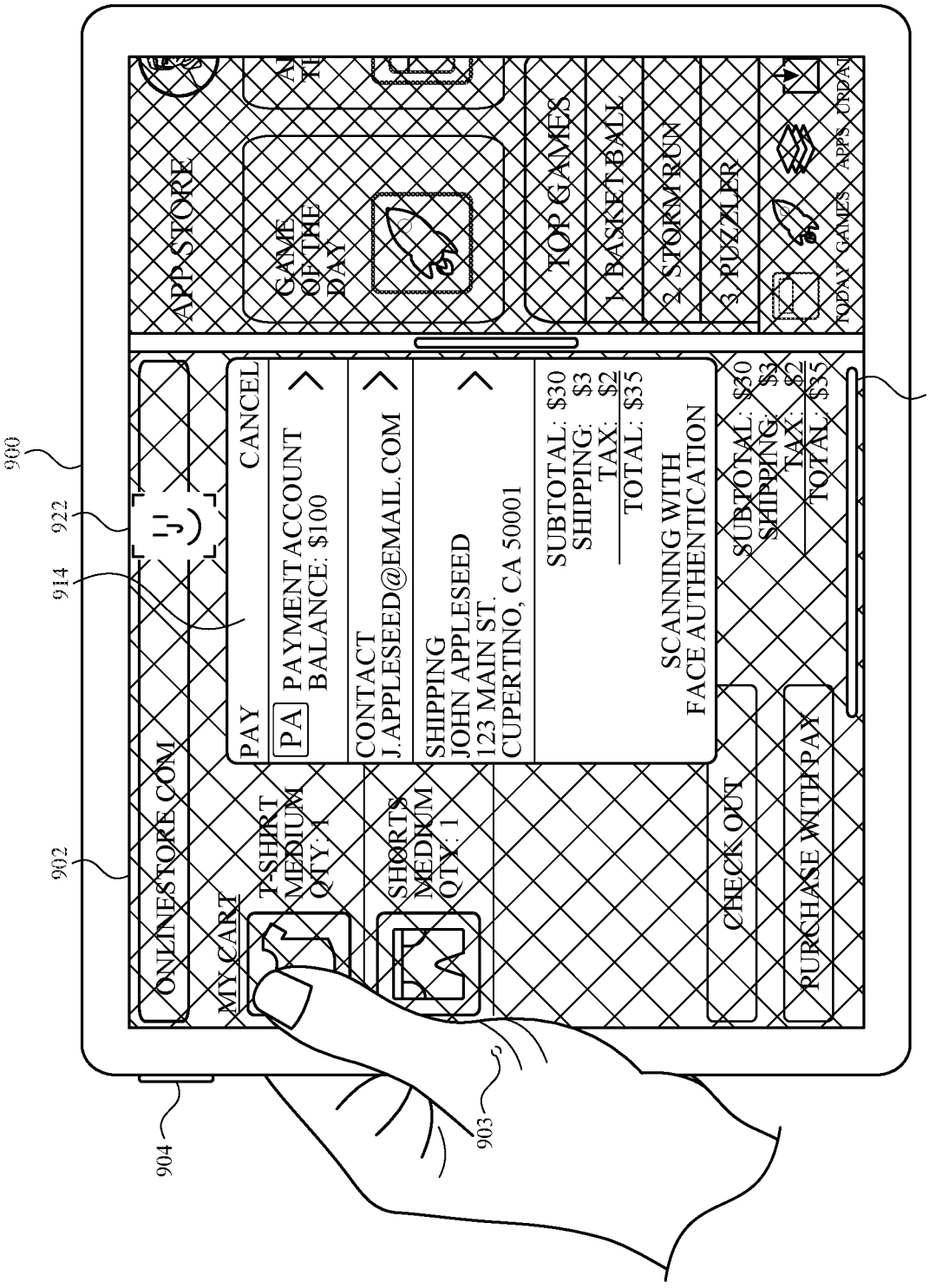


FIG. 9C

2022279466 30 Nov 2022

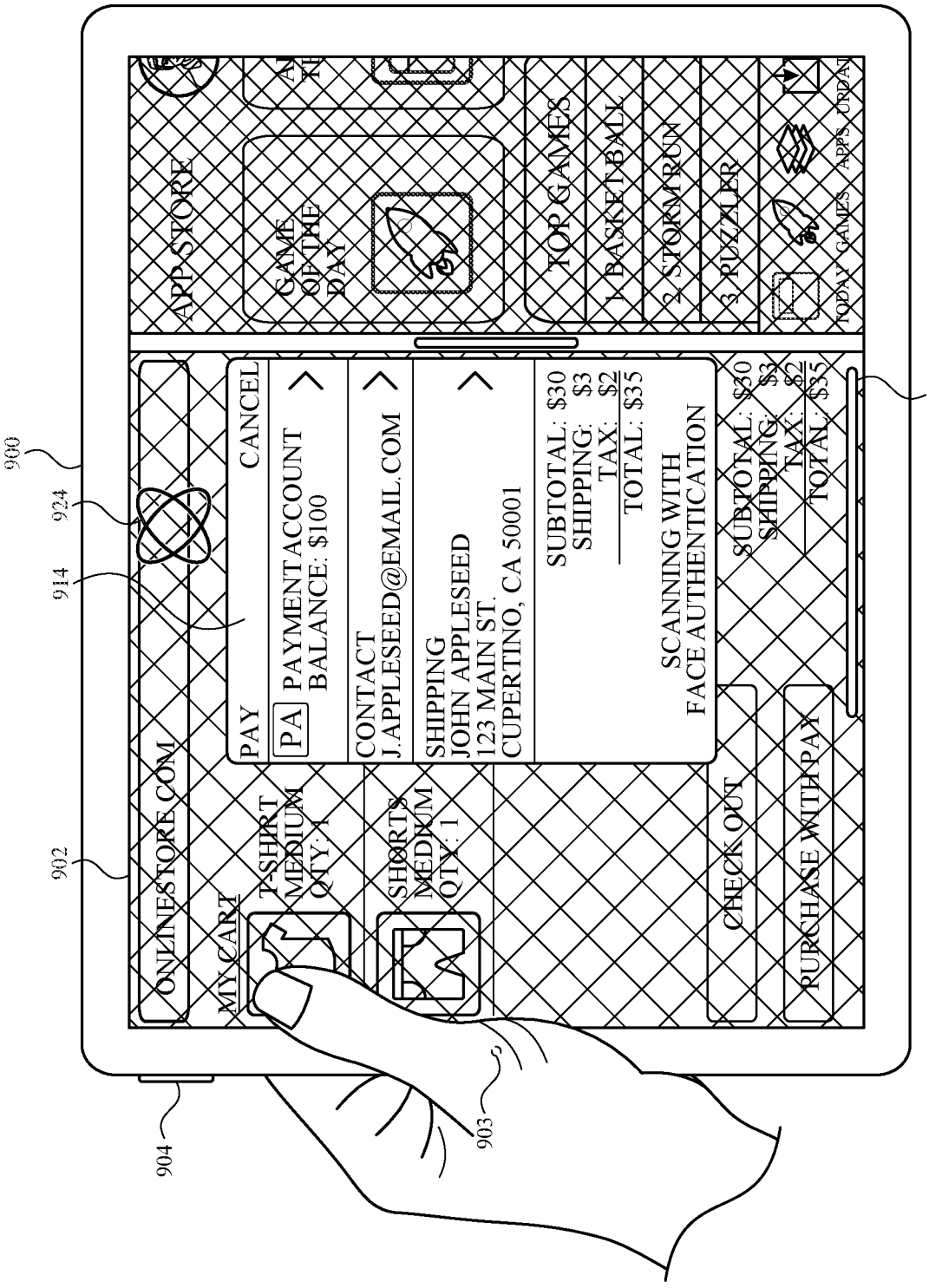


FIG. 9D

2022279466 30 Nov 2022

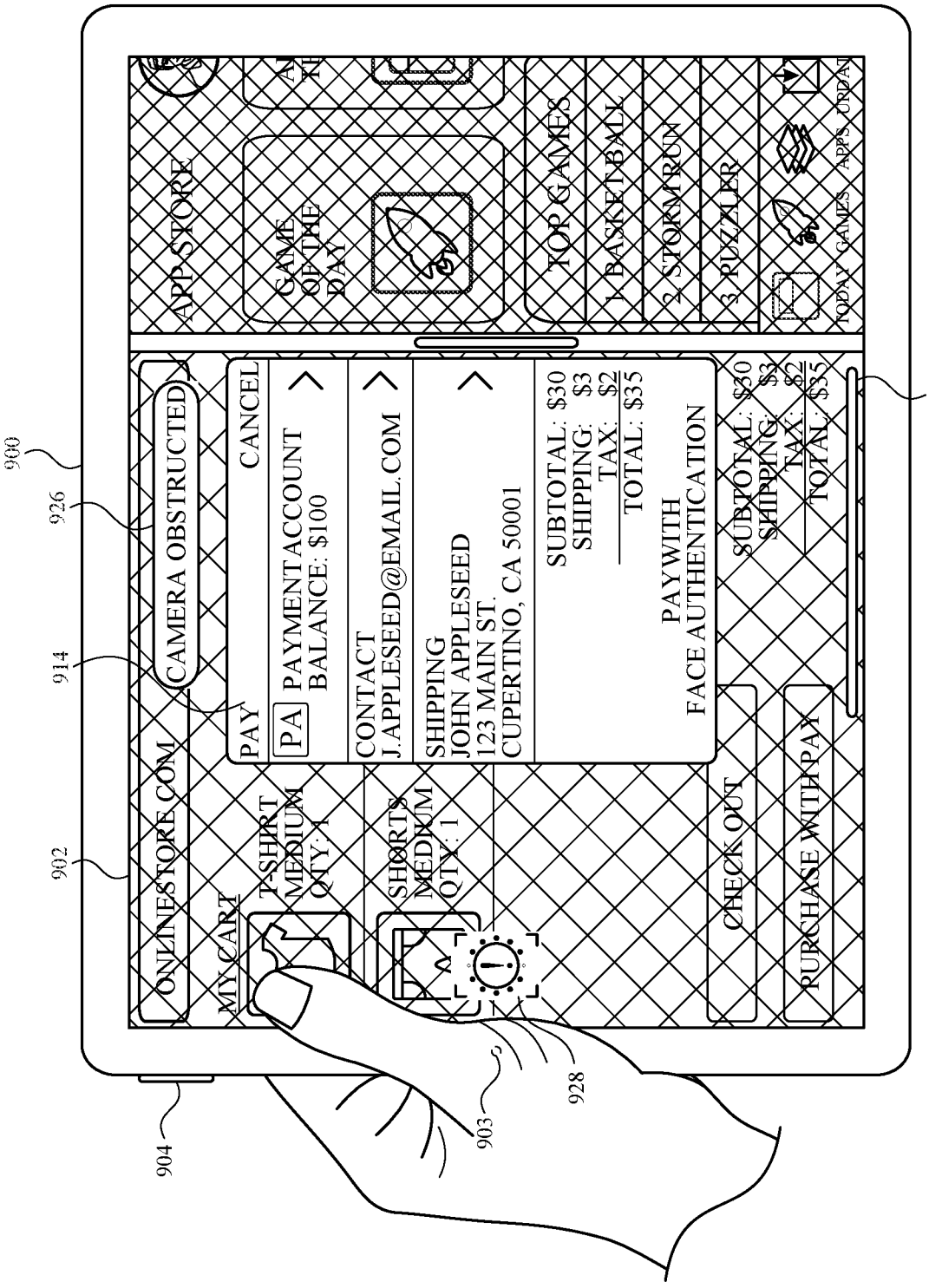


FIG. 9E

2022279466 30 Nov 2022

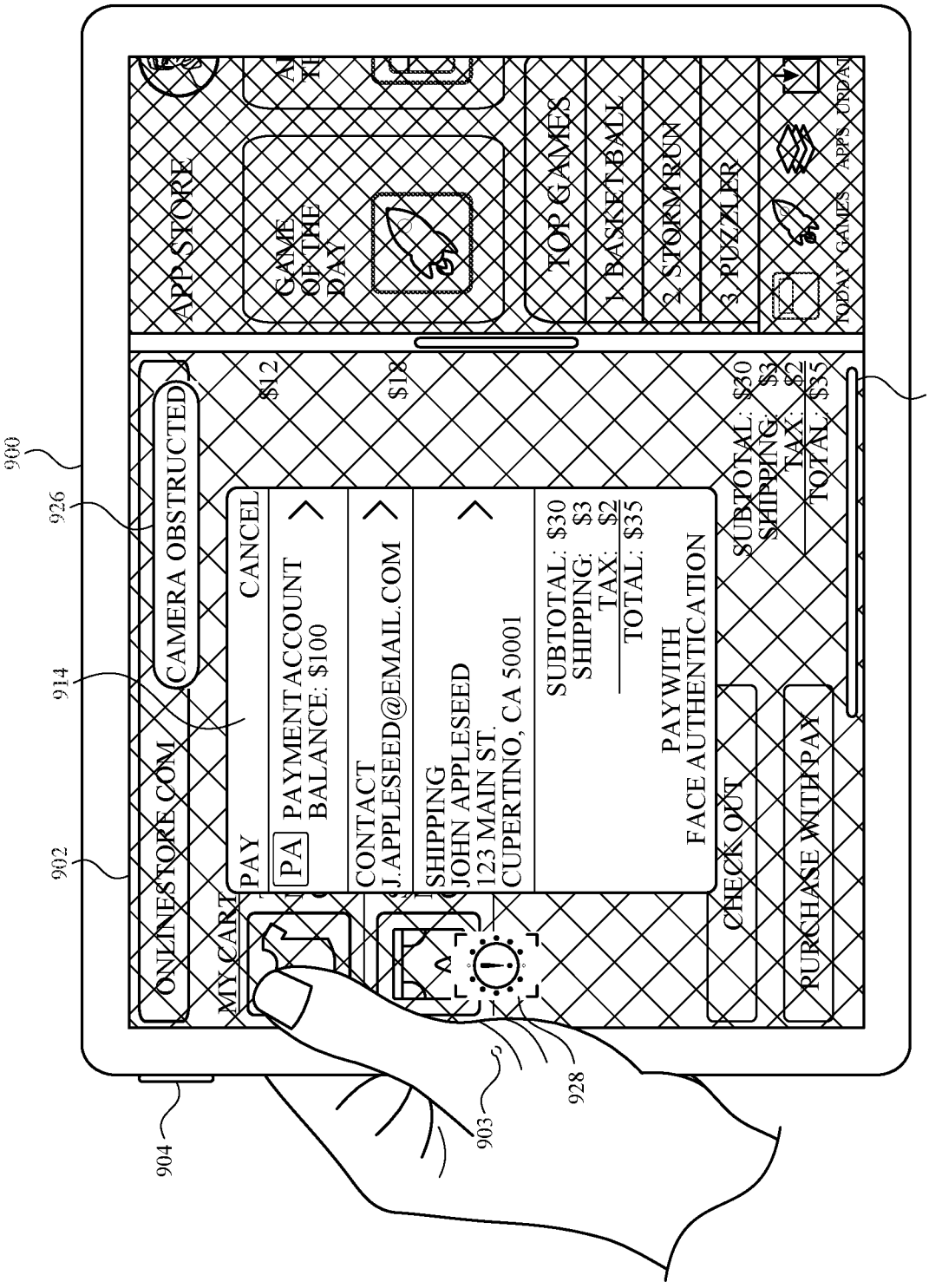


FIG. 9F

2022279466 30 Nov 2022

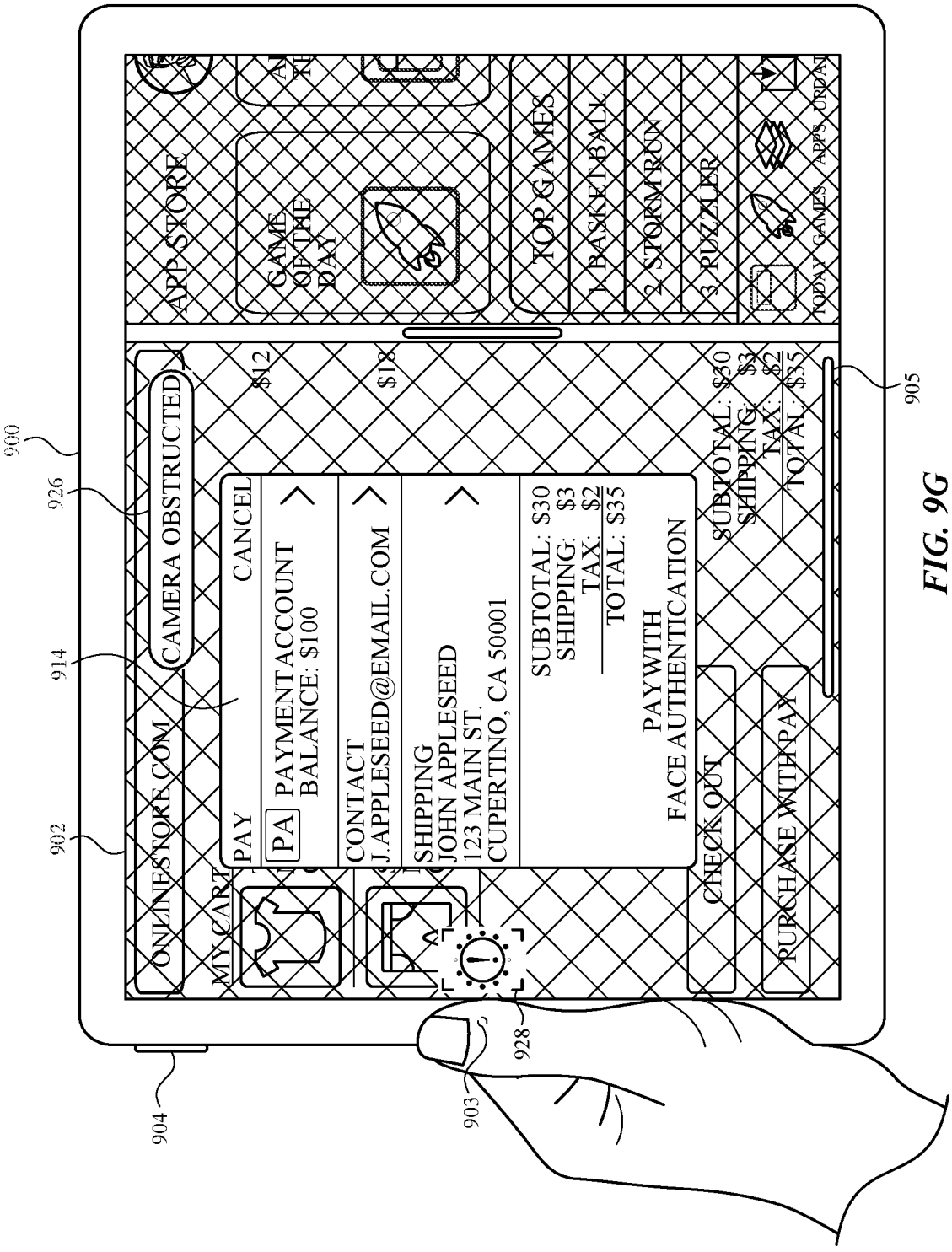


FIG. 9G

2022279466 30 Nov 2022

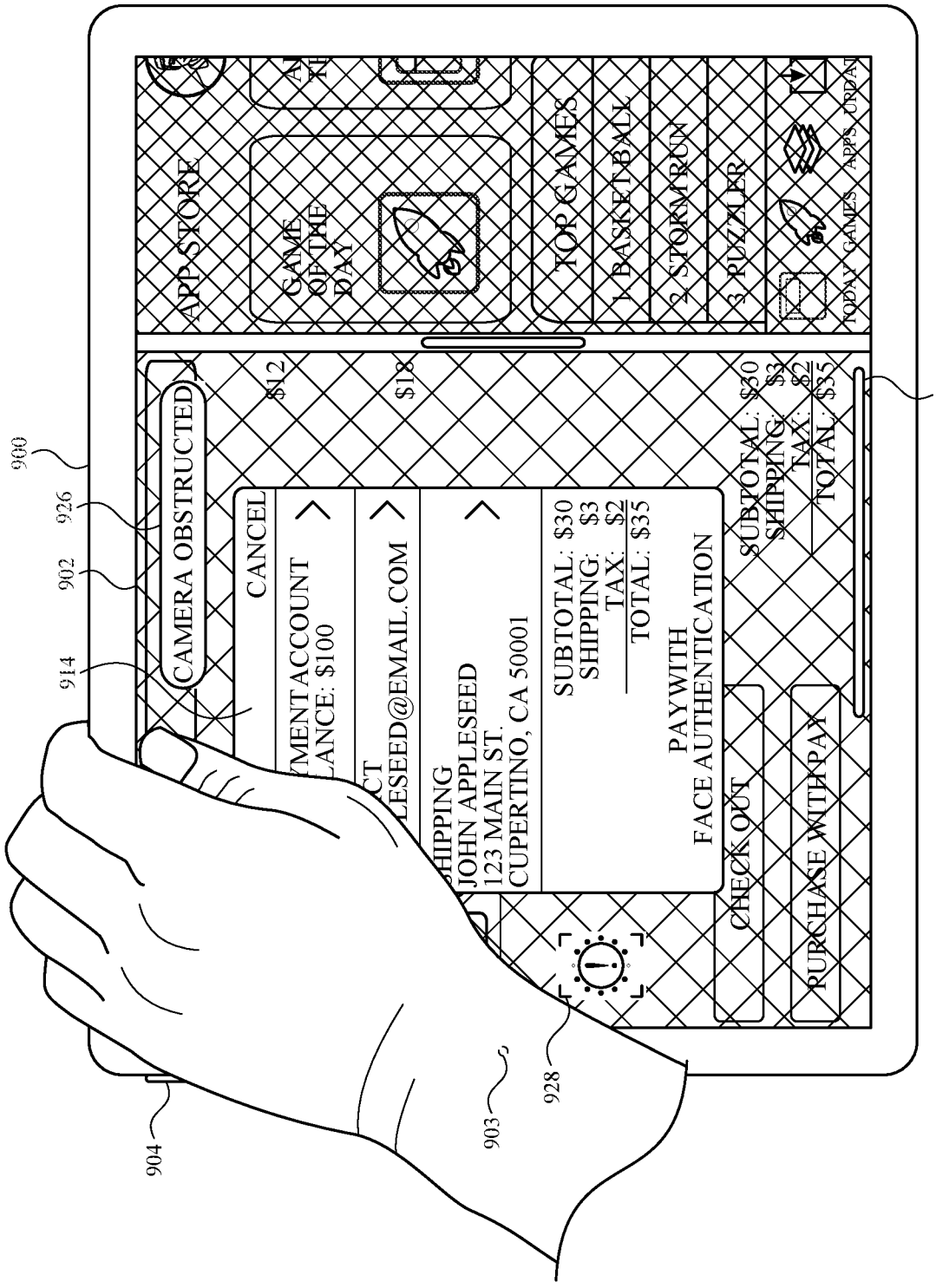


FIG. 9H

2022279466 30 Nov 2022

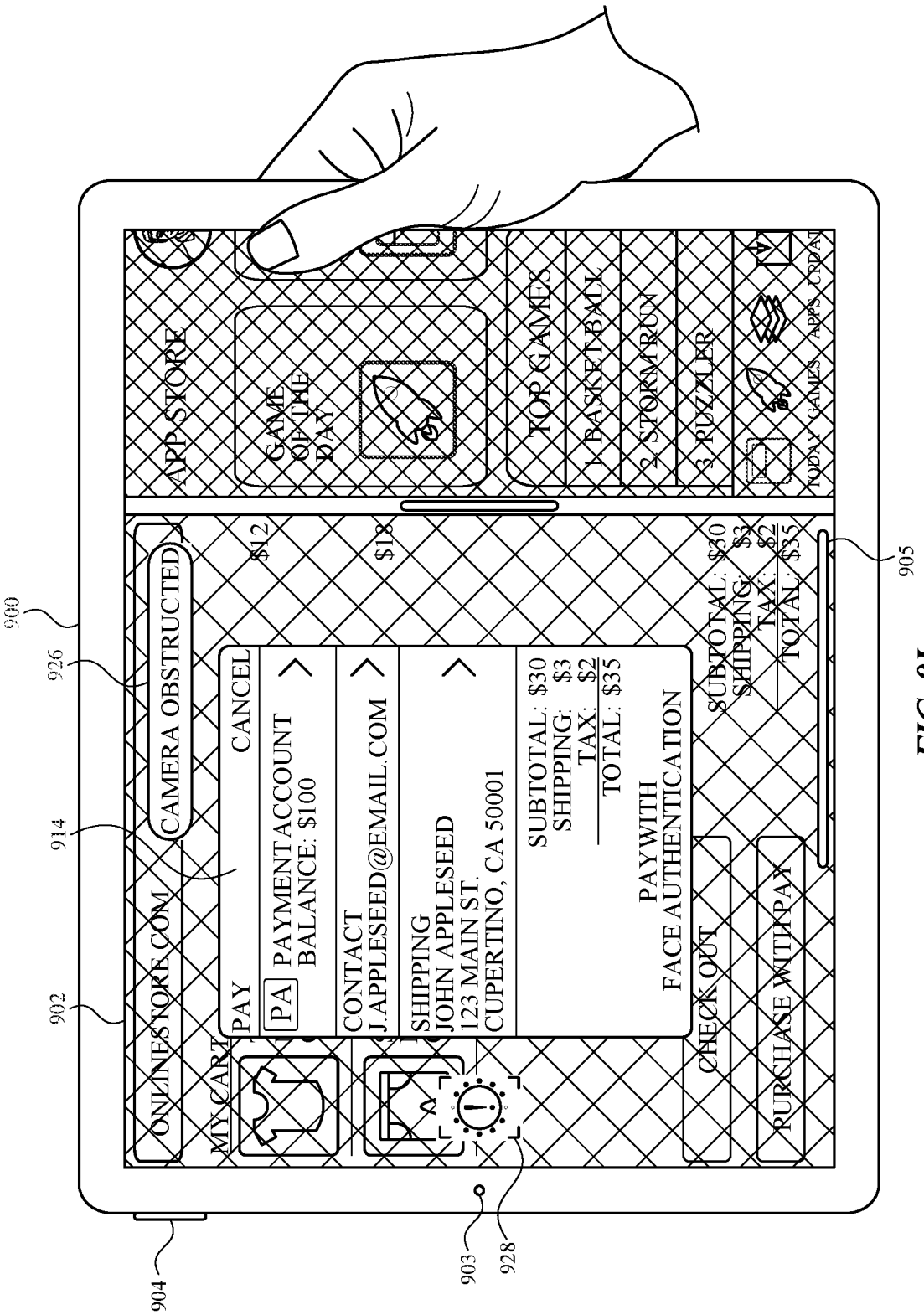


FIG. 9I

2022279466 30 Nov 2022

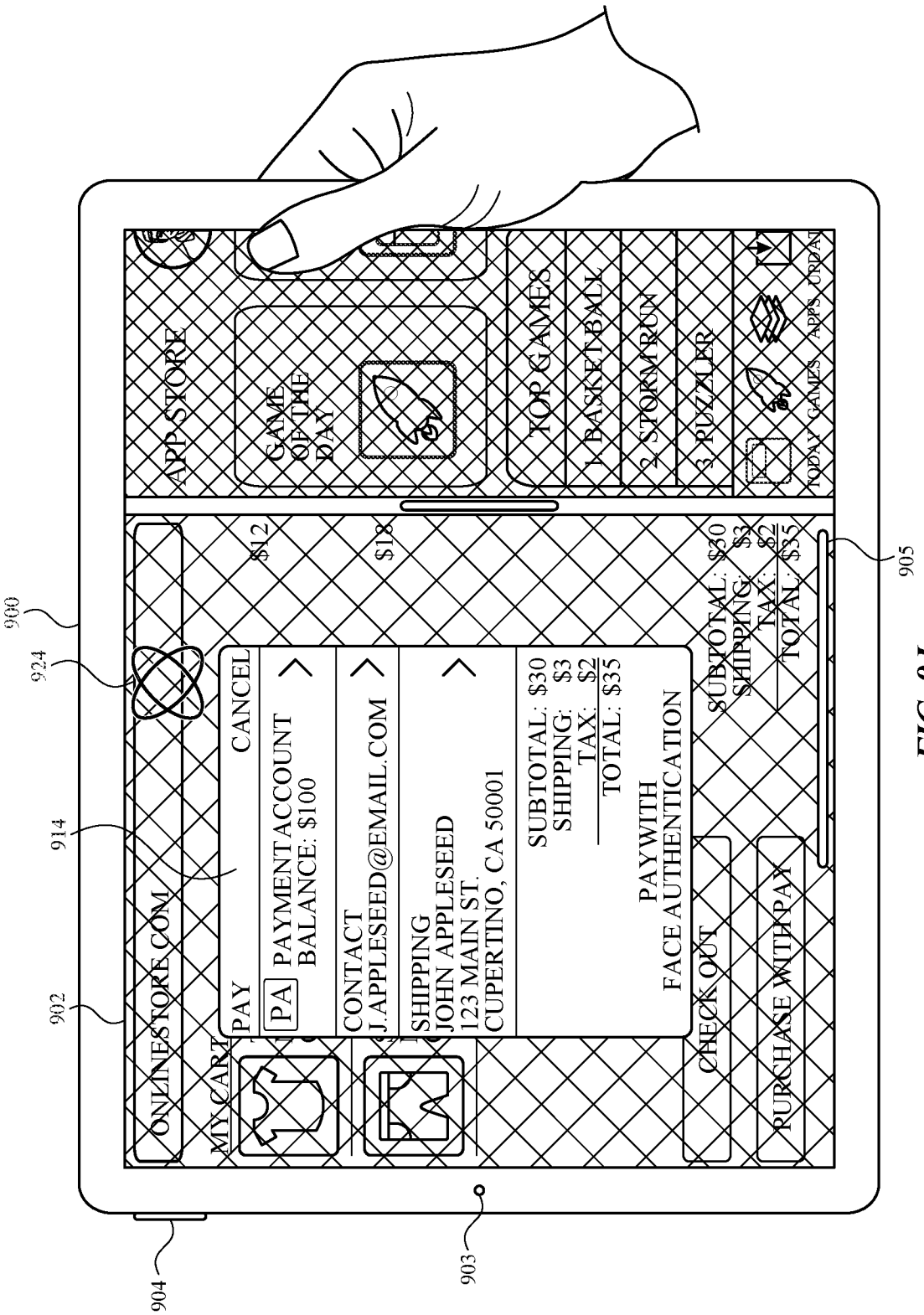


FIG. 9J

2022279466 30 Nov 2022

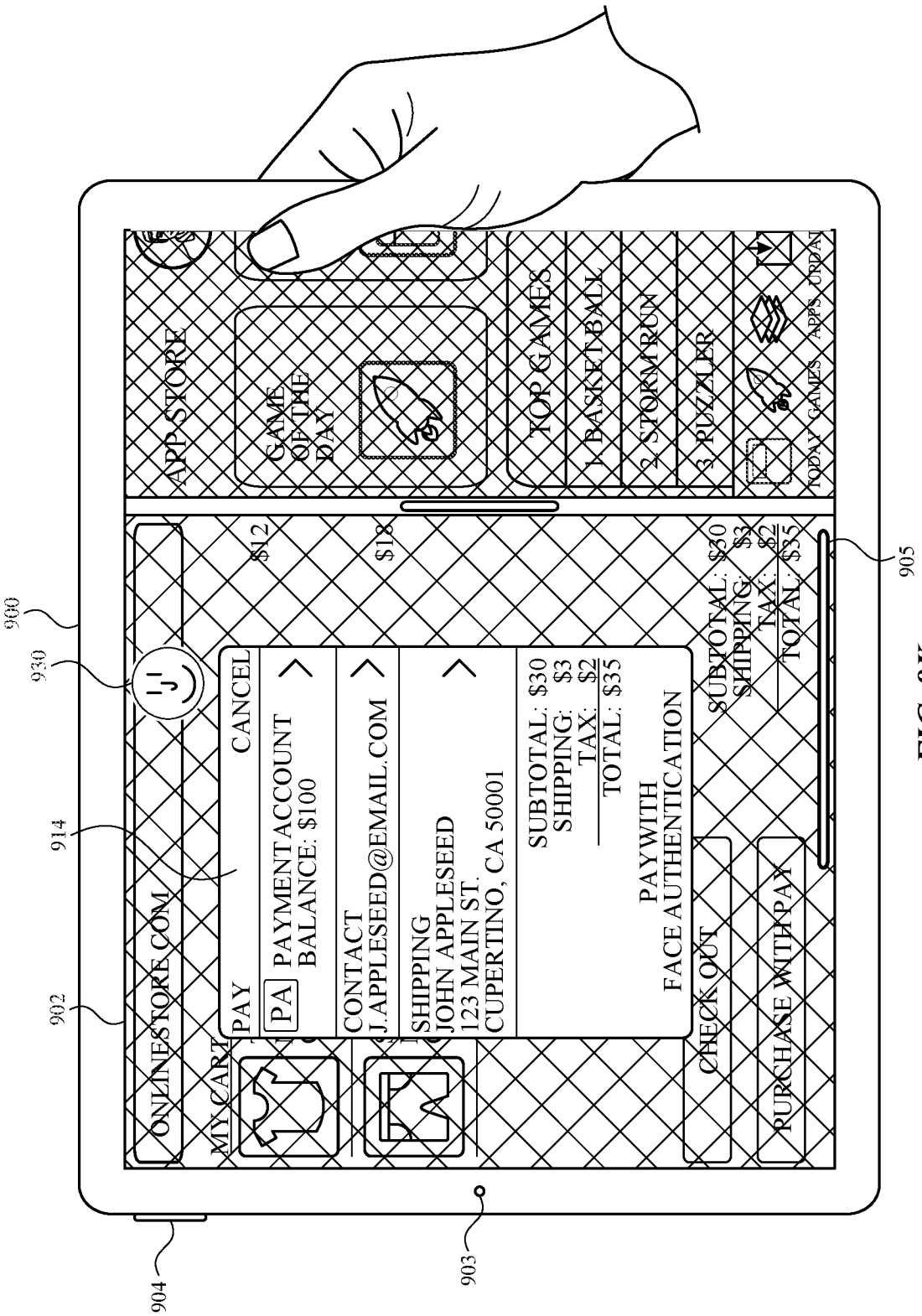


FIG. 9K

2022279466 30 Nov 2022

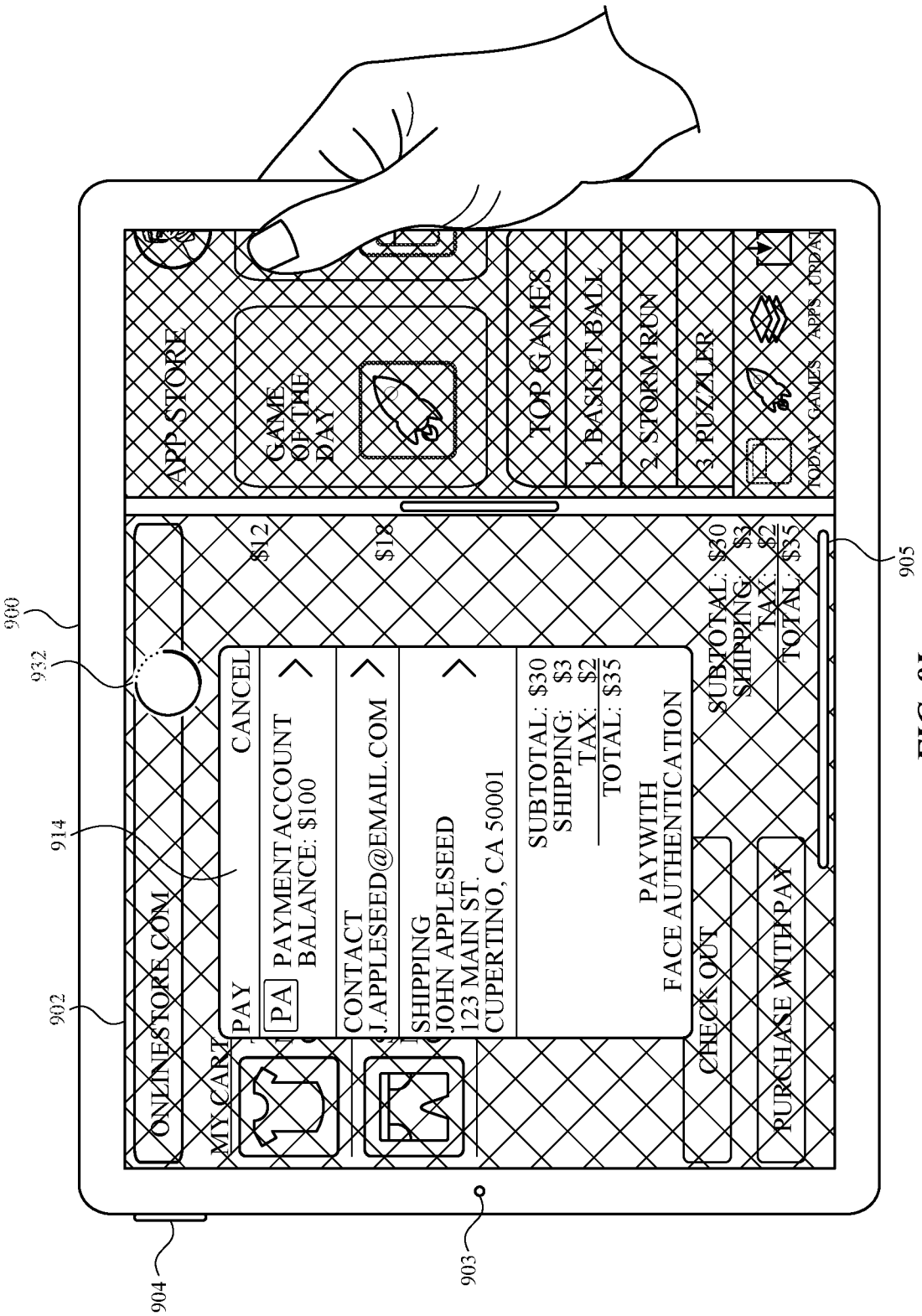


FIG. 9L

2022279466 30 Nov 2022

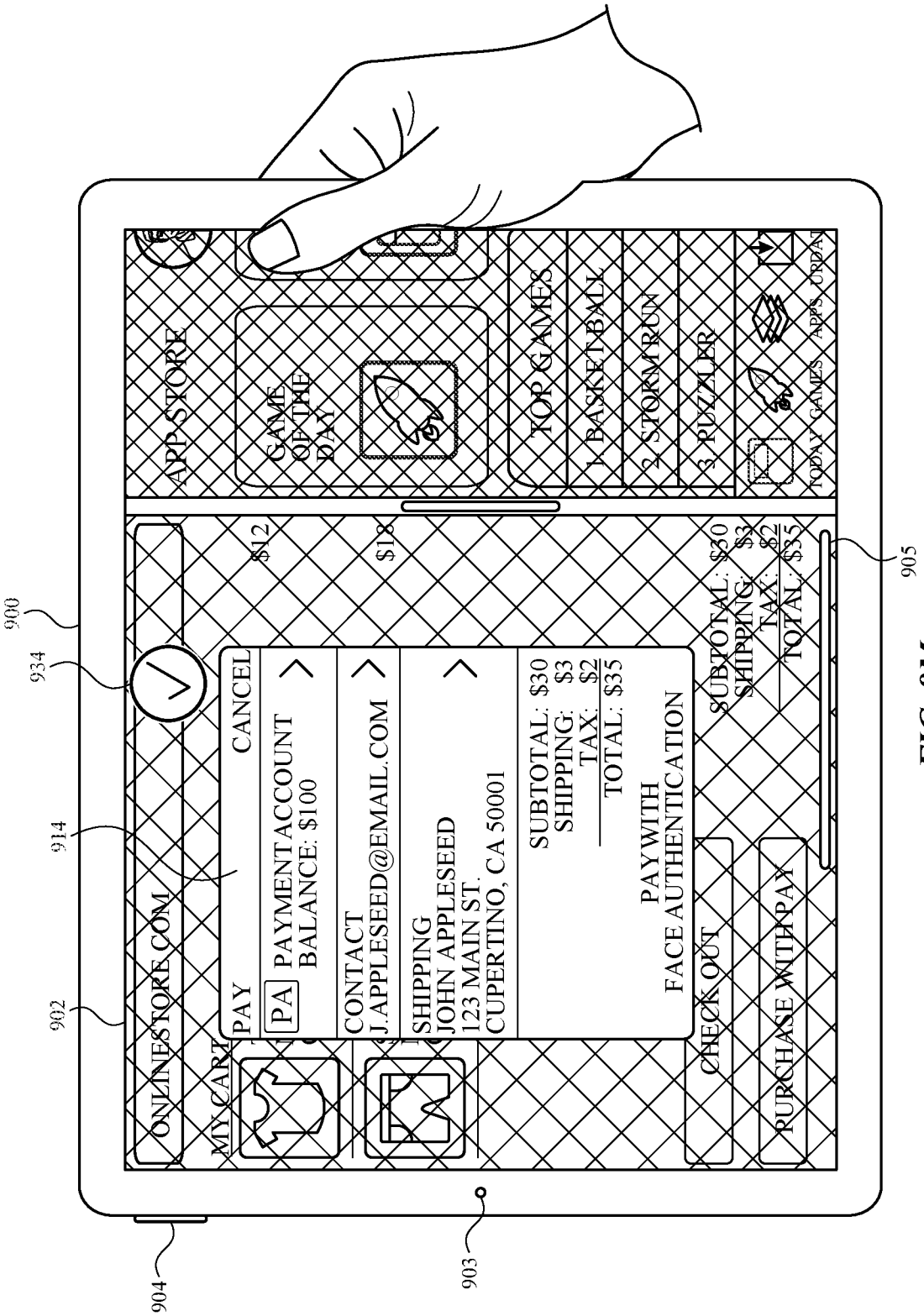


FIG. 9M

2022279466 30 Nov 2022

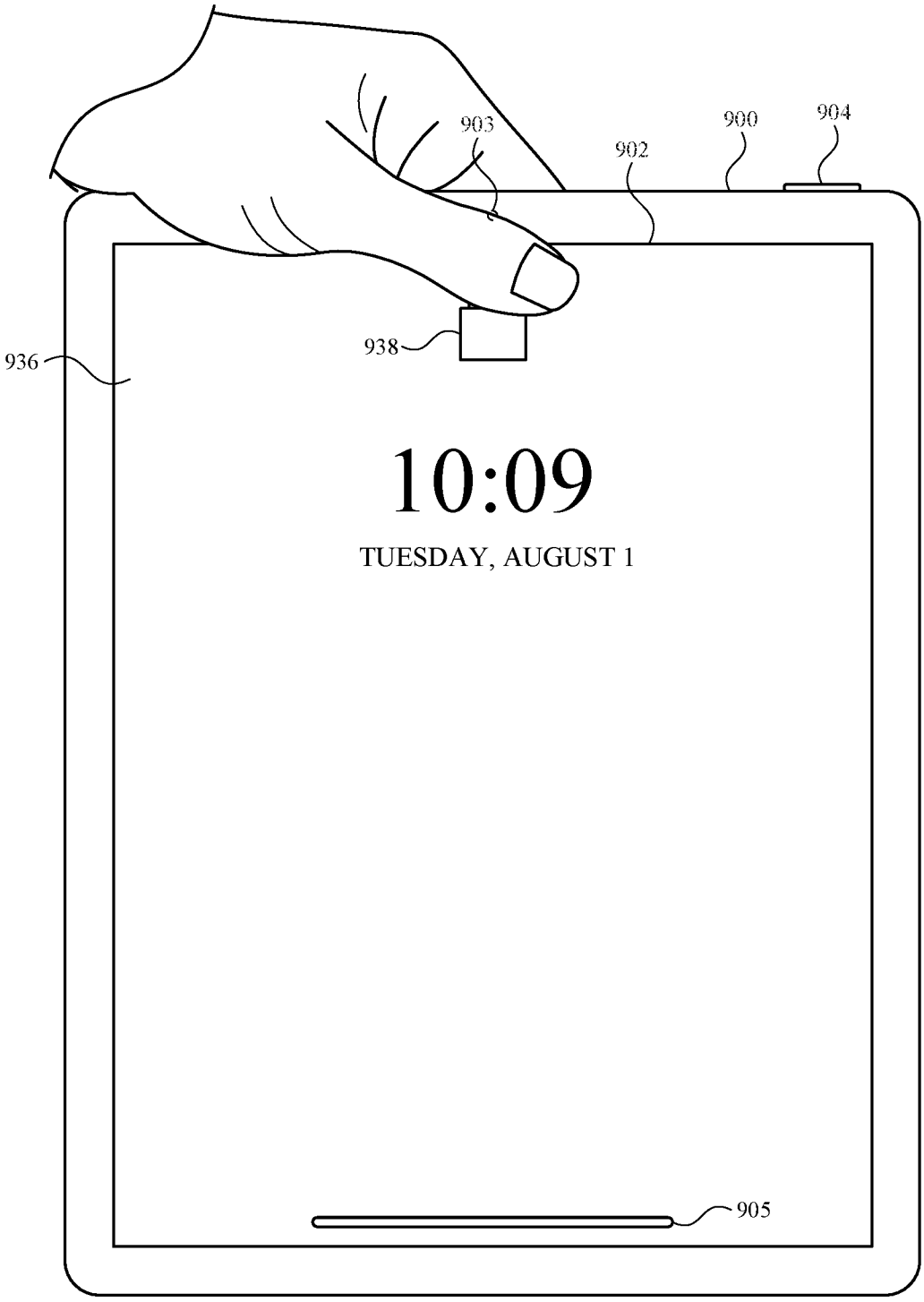


FIG. 9N

2022279466 30 Nov 2022

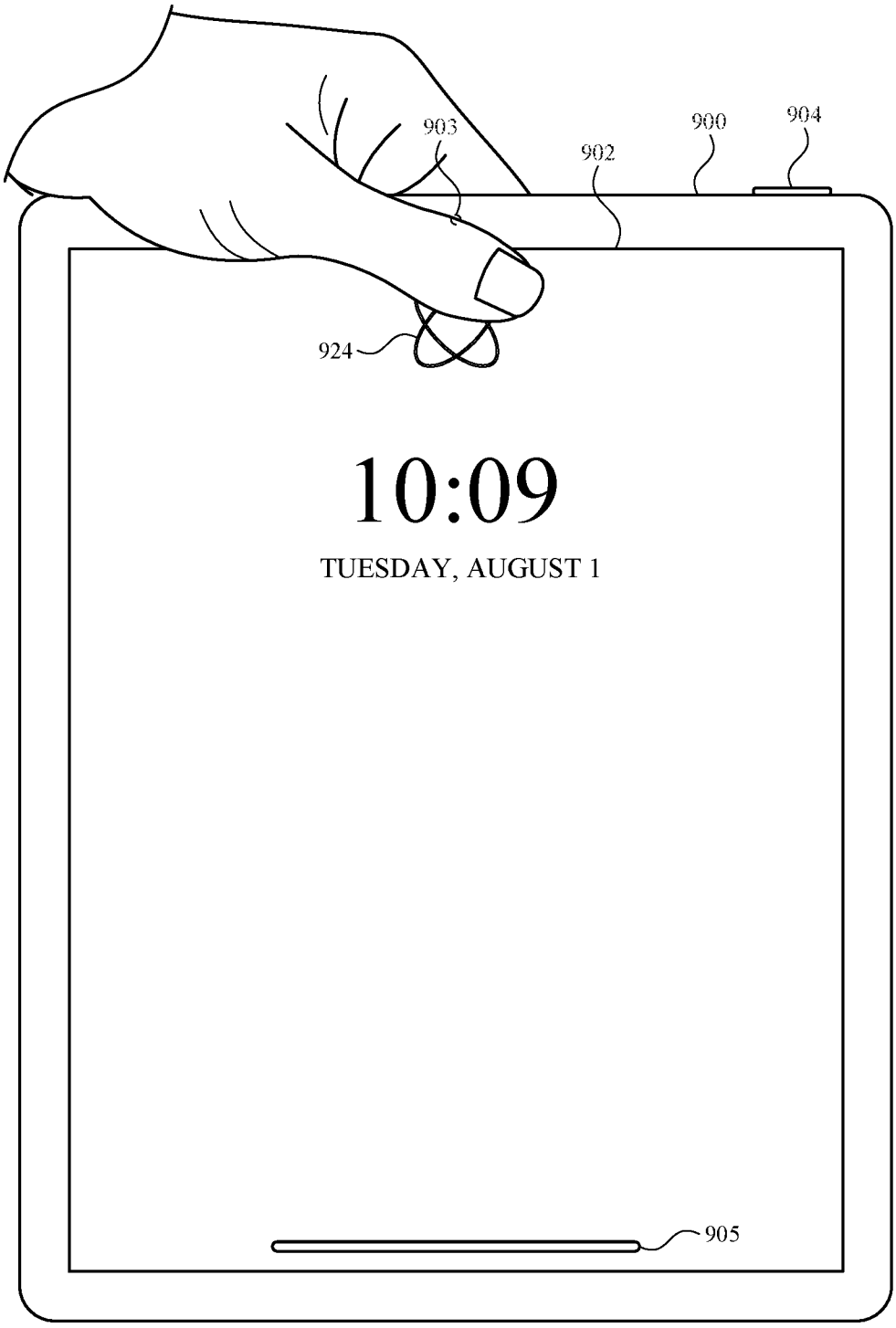


FIG. 9O

2022279466 30 Nov 2022

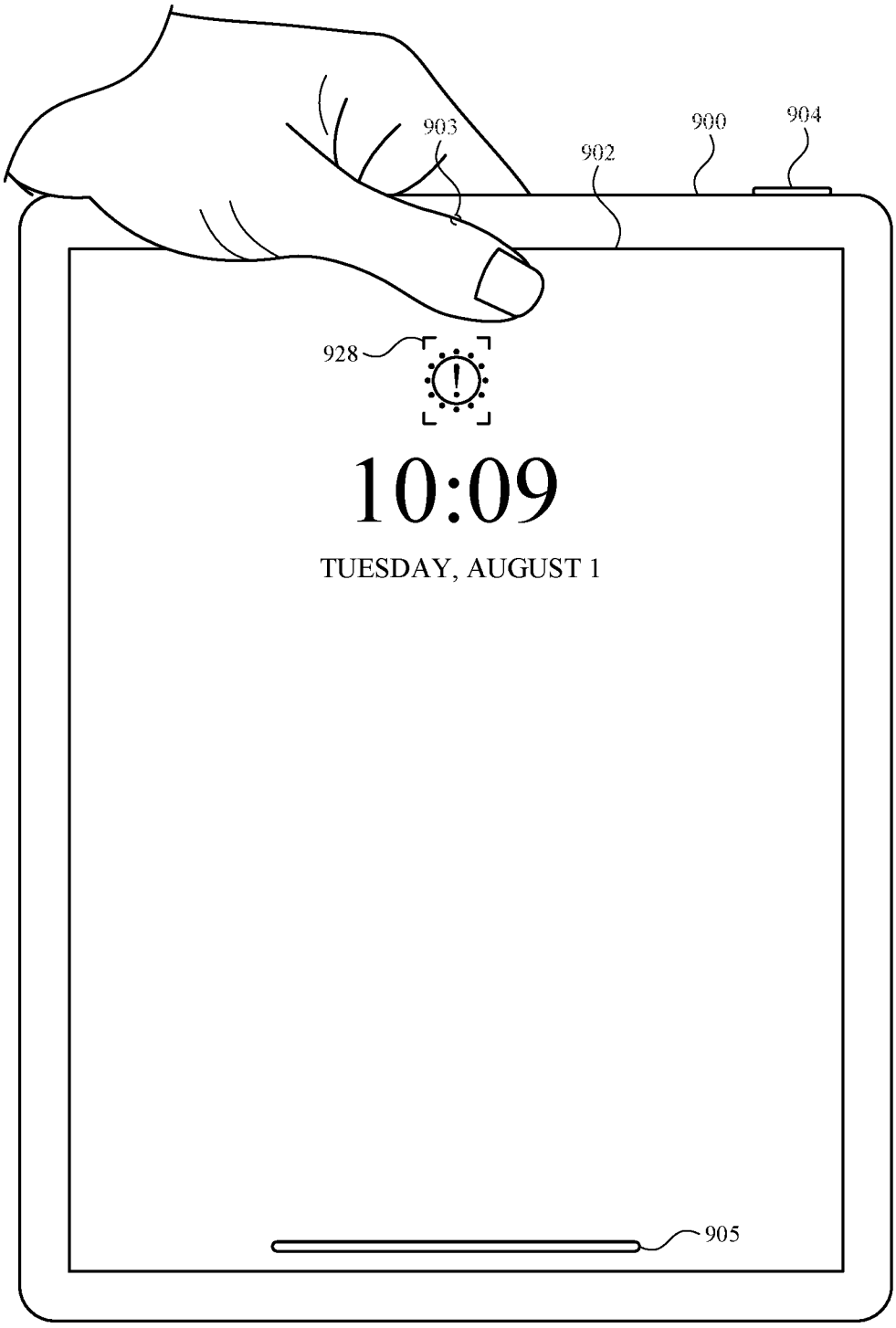


FIG. 9P

2022279466 30 Nov 2022

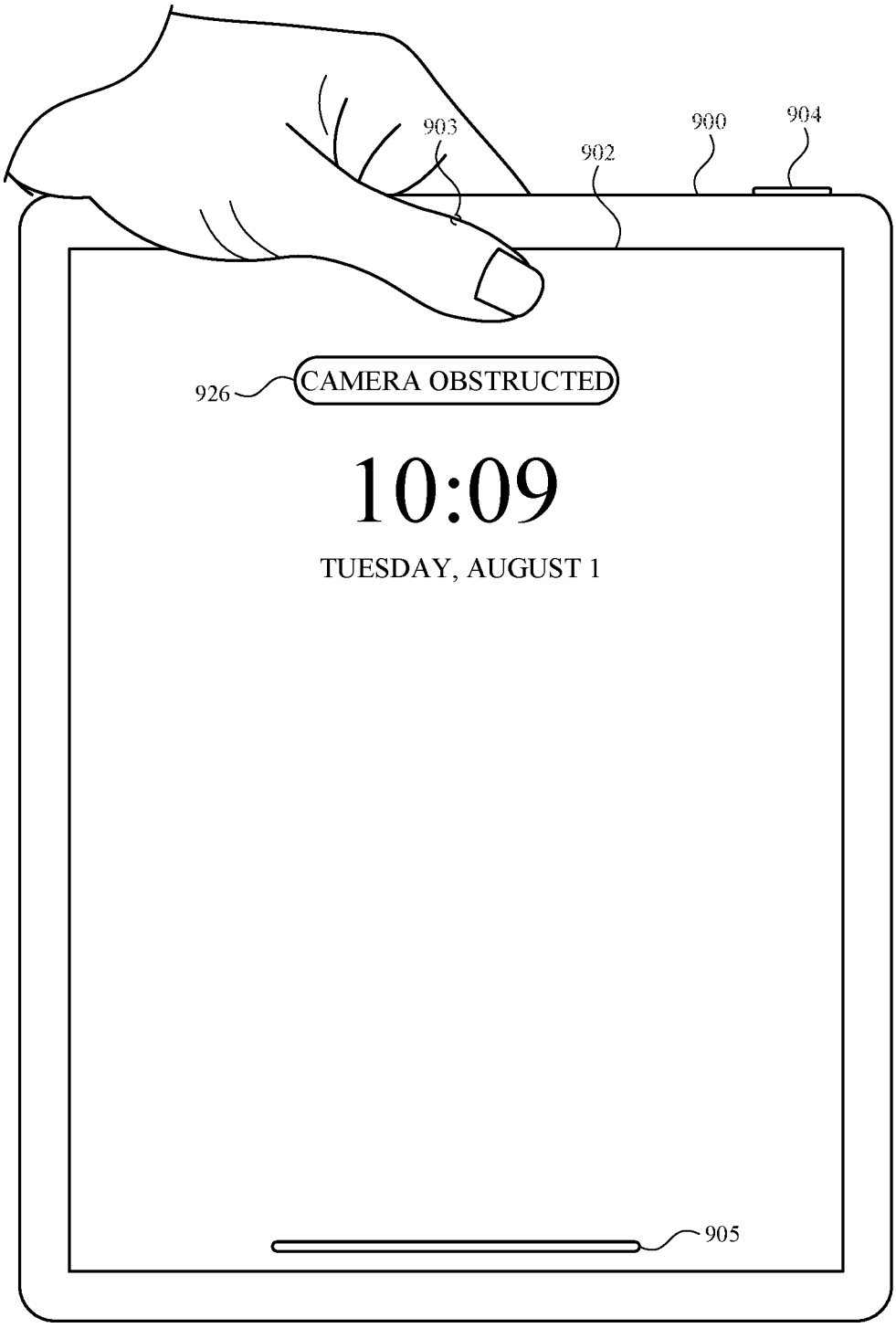


FIG. 9Q

2022279466 30 Nov 2022

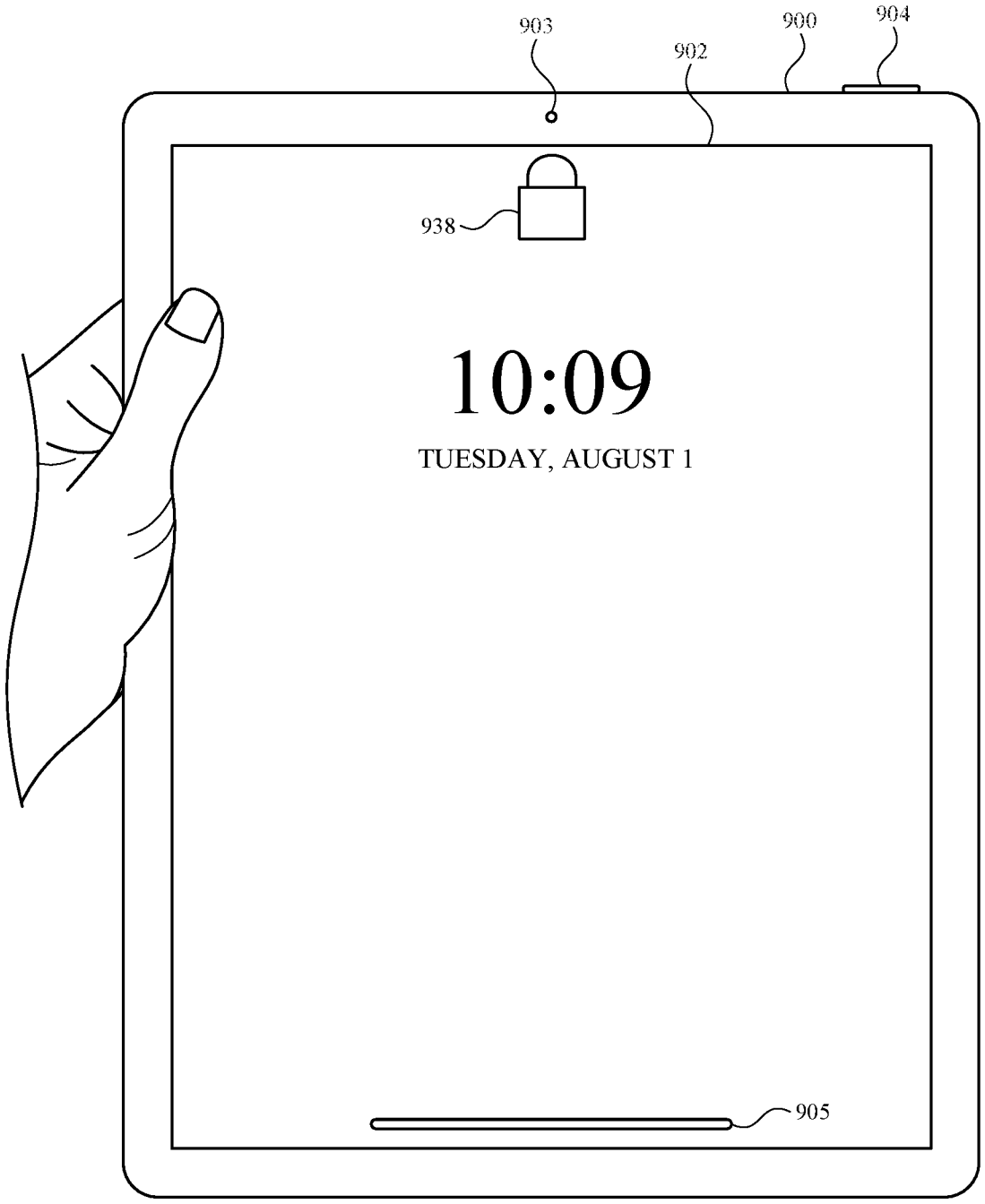


FIG. 9R

2022279466 30 Nov 2022

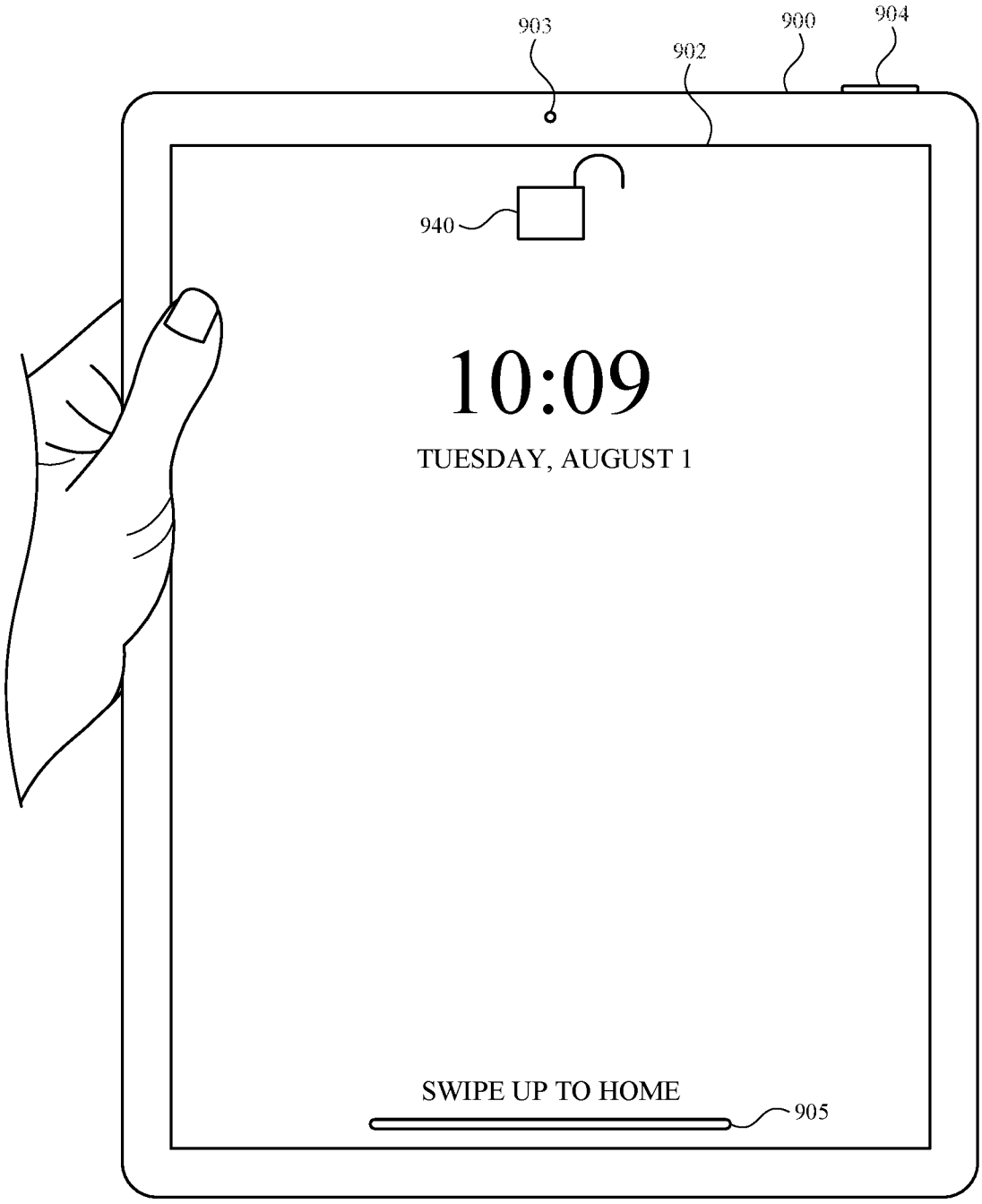


FIG. 9S

2022279466 30 Nov 2022

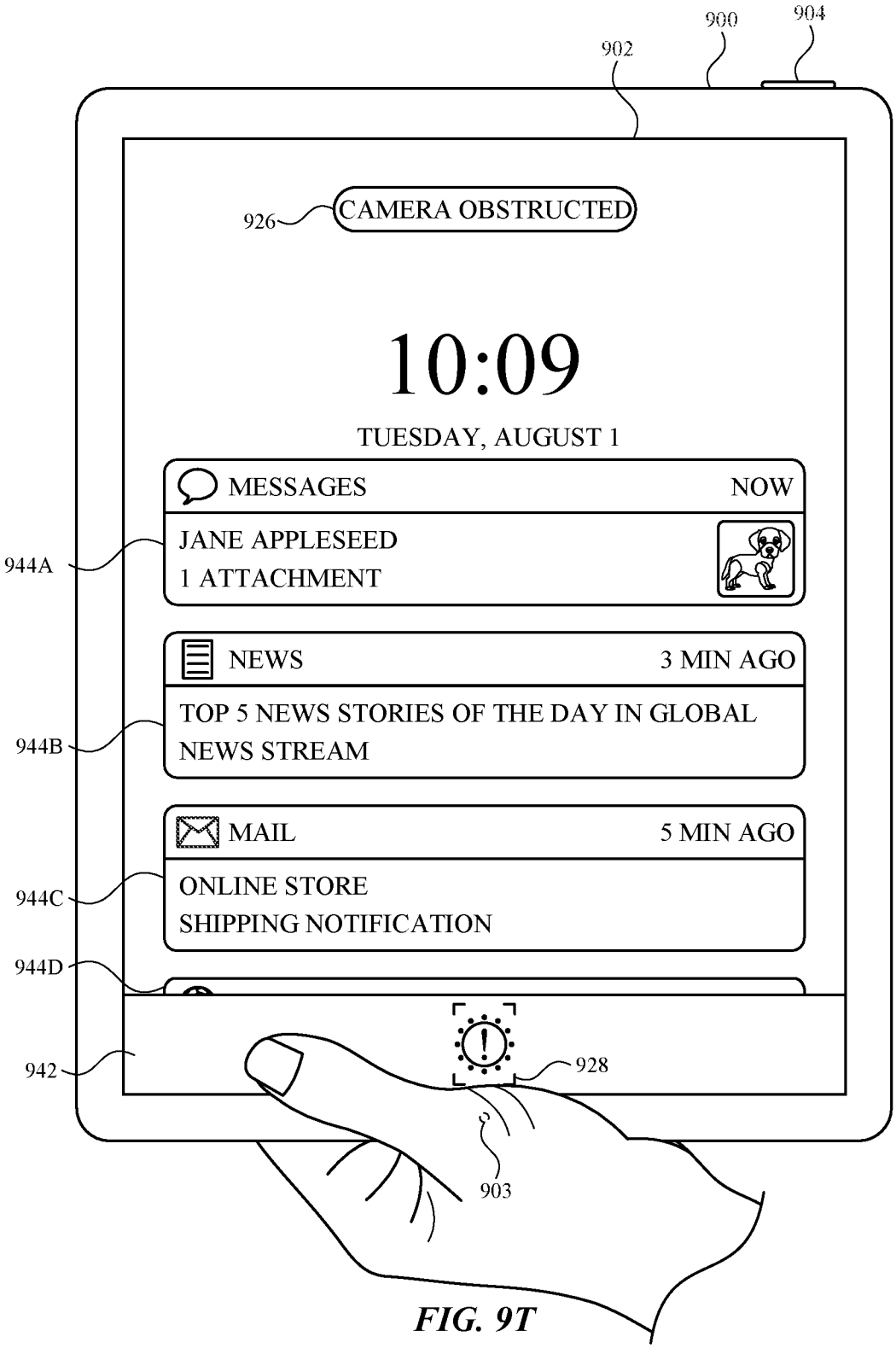


FIG. 9T

30 Nov 2022
2022279466

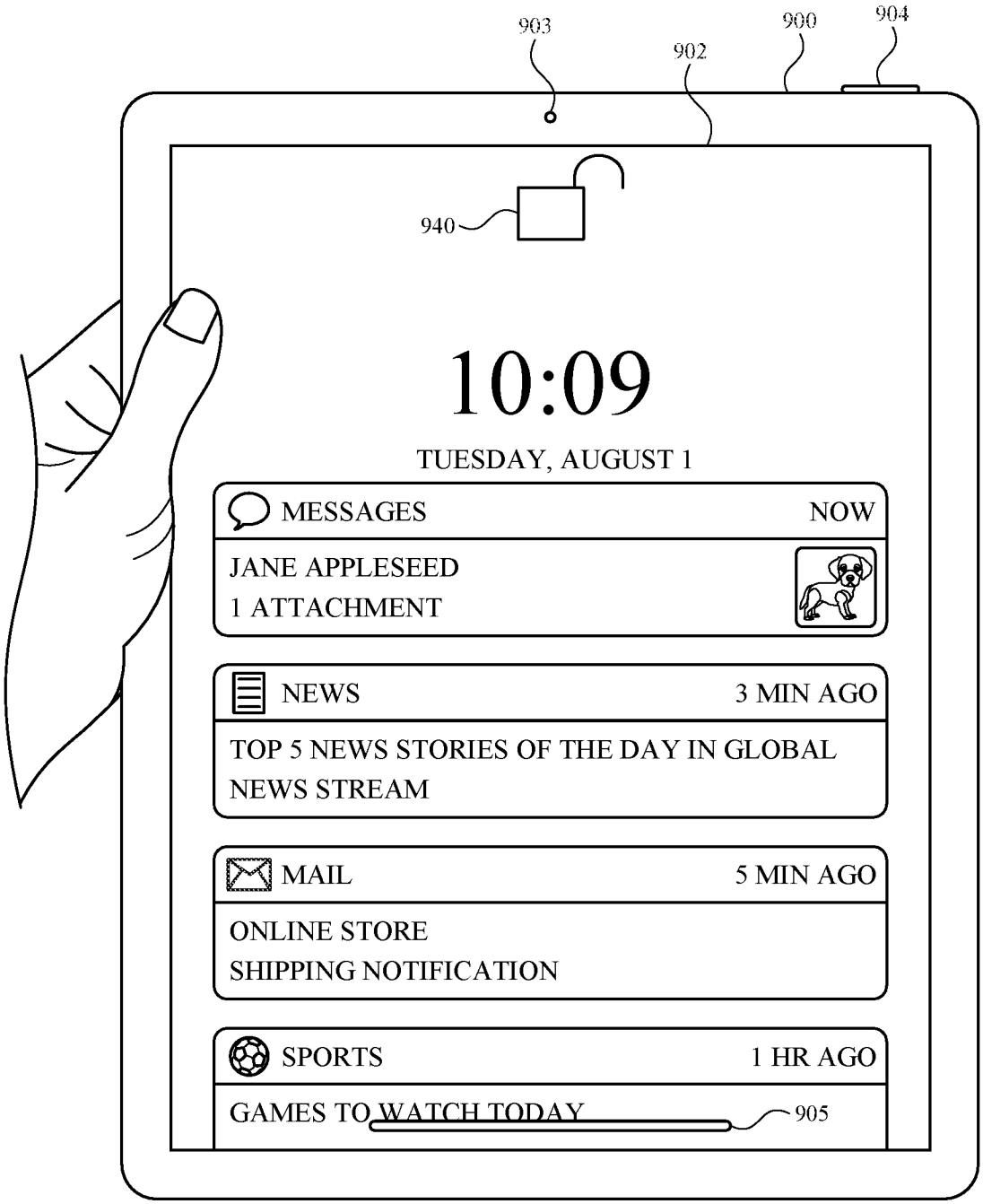


FIG. 9U

30 Nov 2022
2022279466

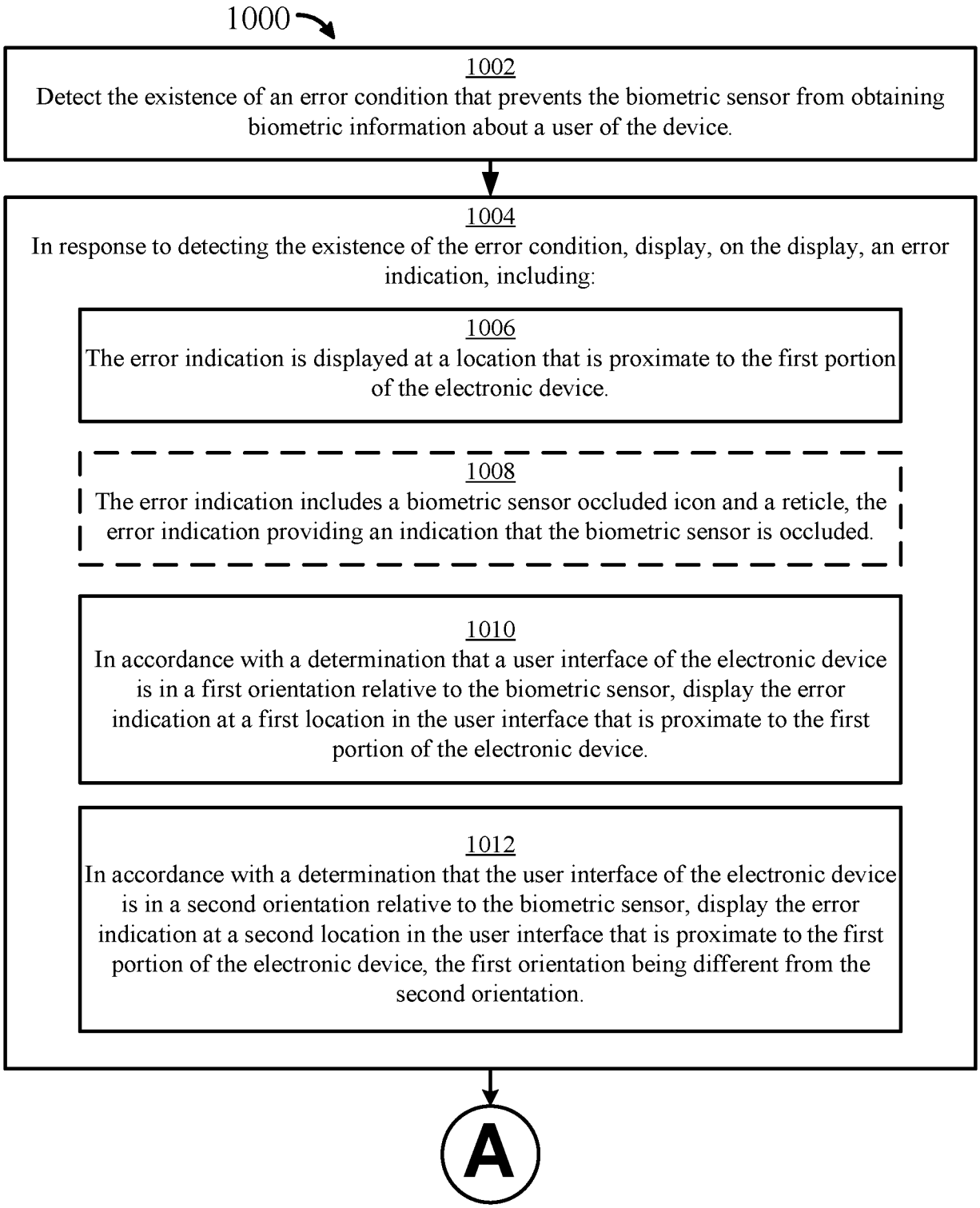


FIG. 10A

30 Nov 2022 2022279466

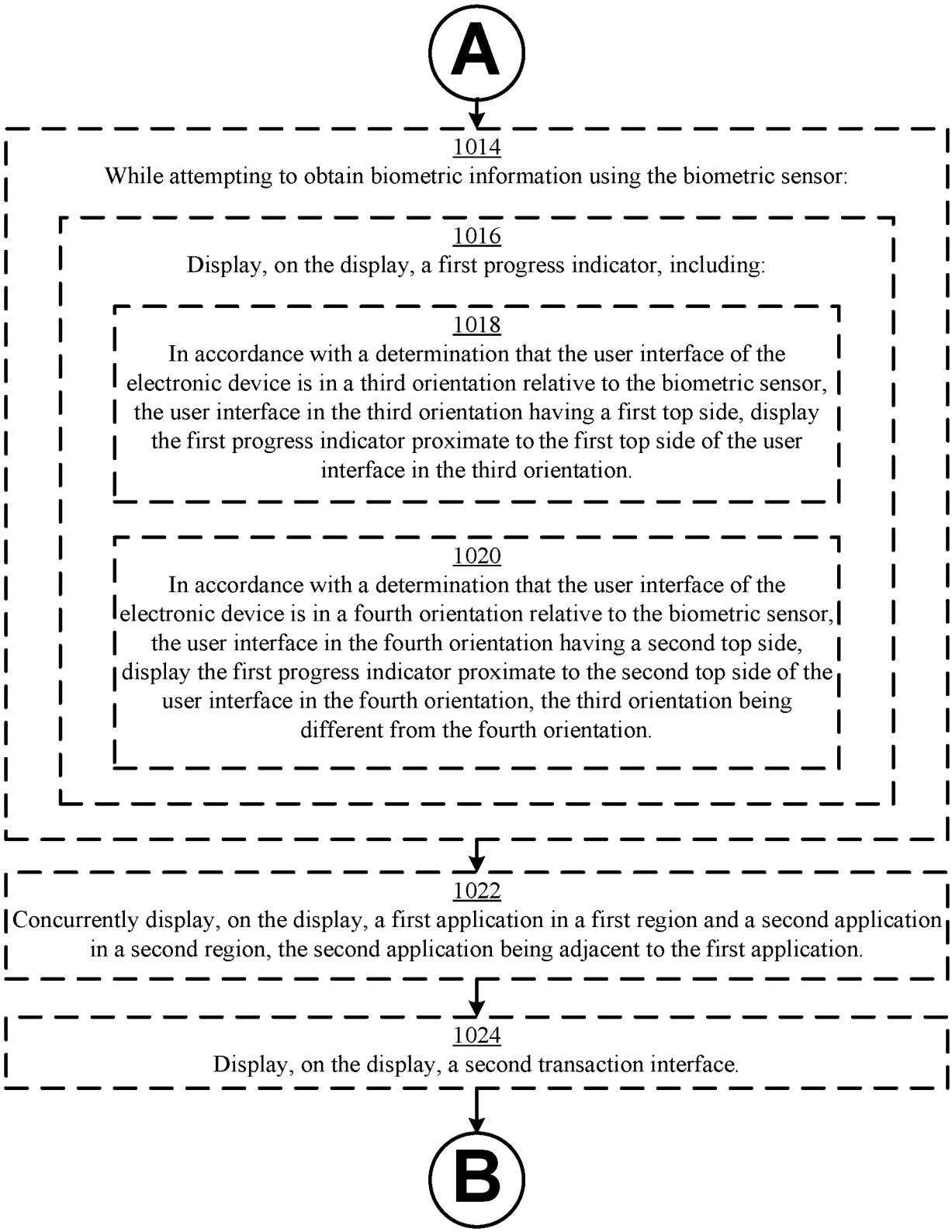


FIG. 10B

2022279466 30 Nov 2022

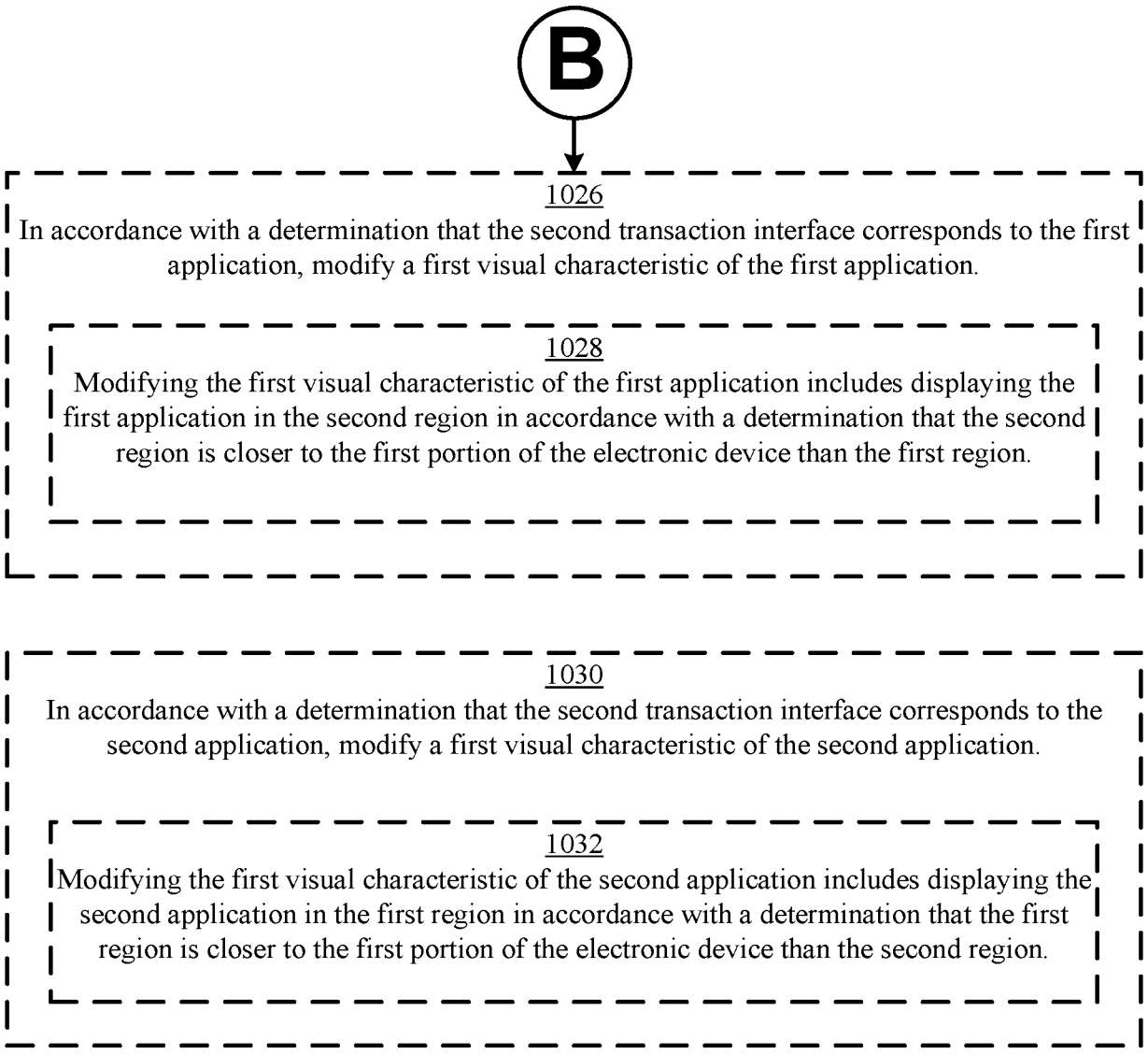


FIG. 10C

2022279466 30 Nov 2022

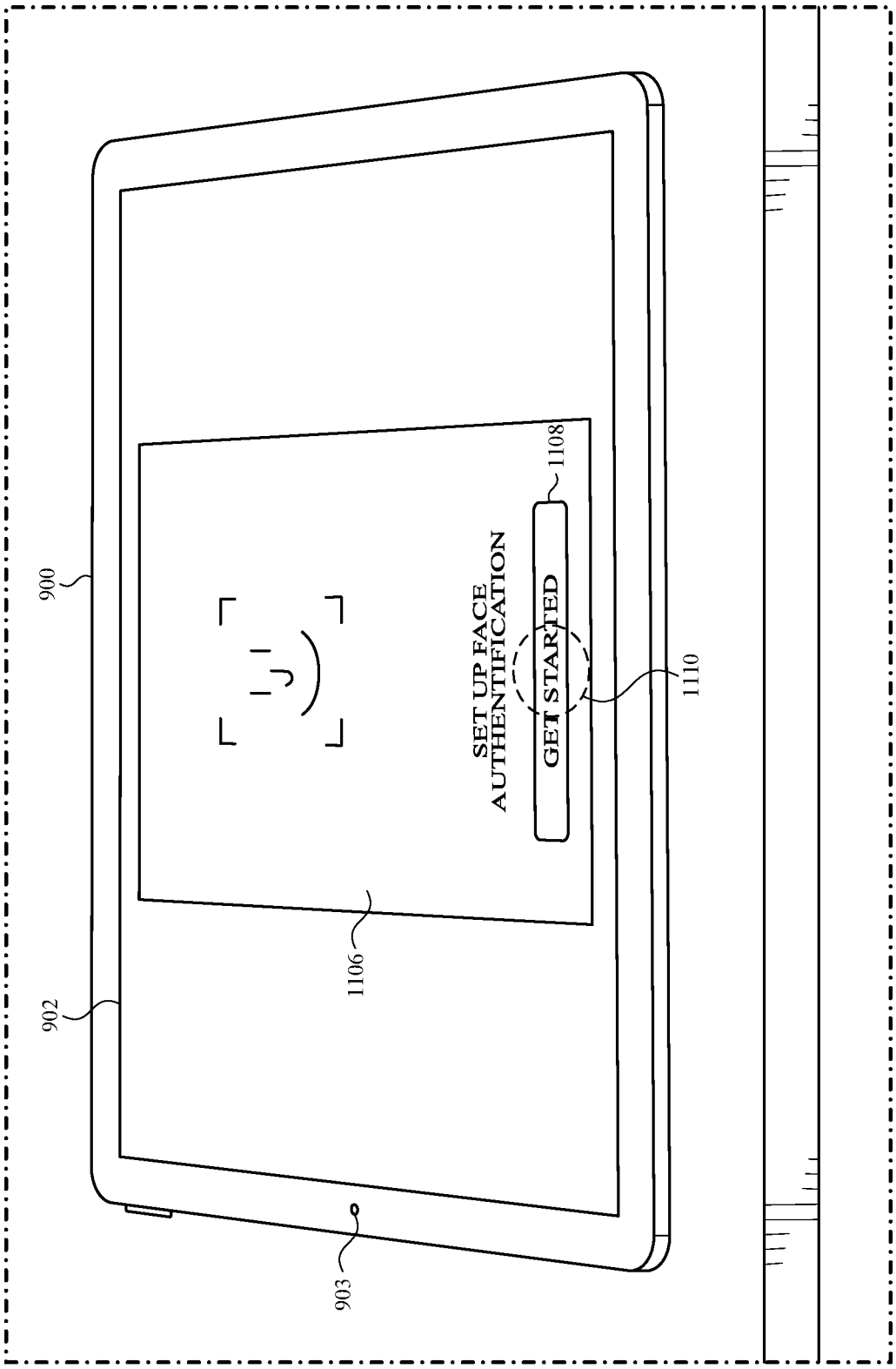


FIG. 11A

2022279466 30 Nov 2022

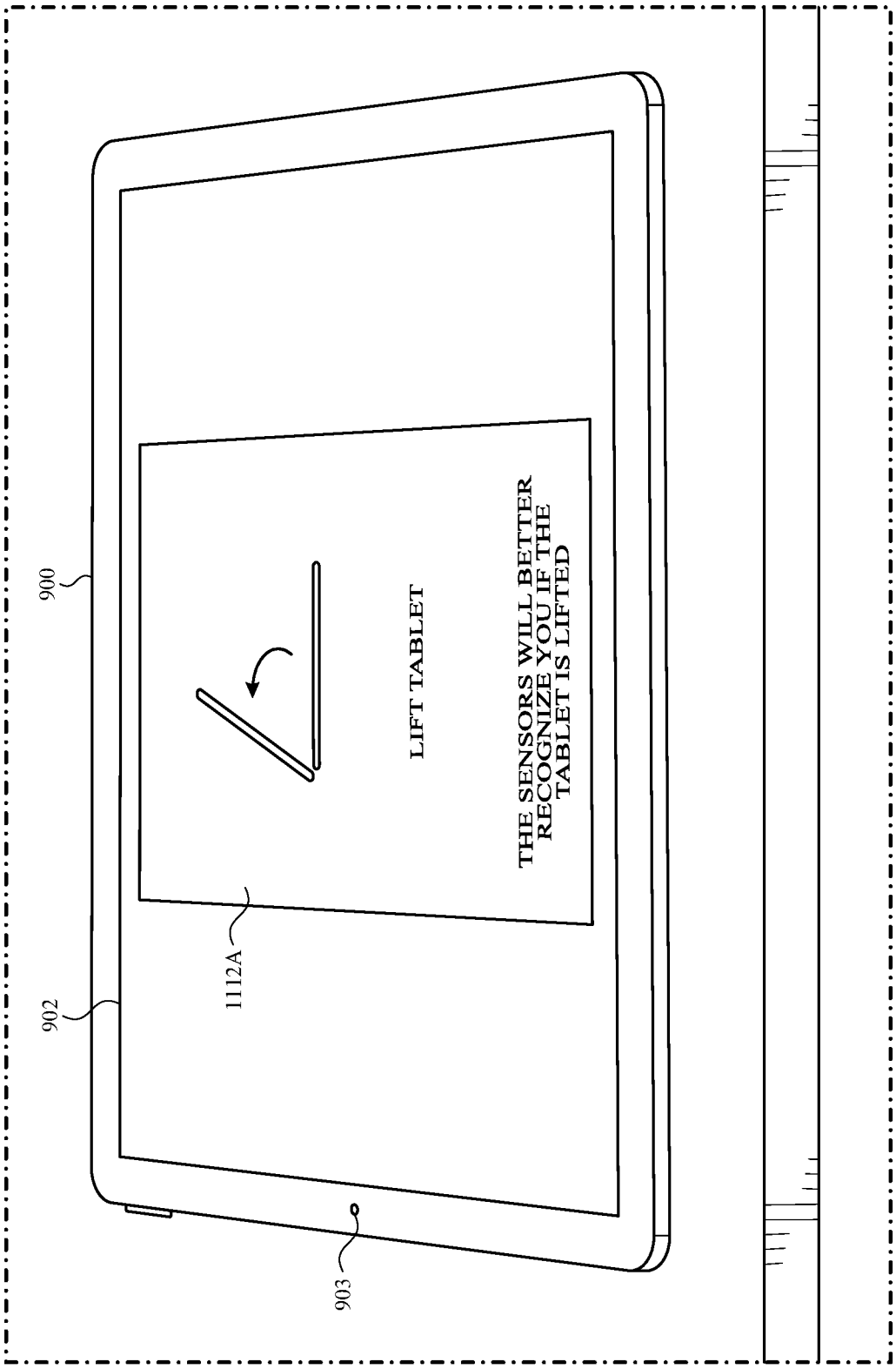


FIG. 11B

2022279466 30 Nov 2022

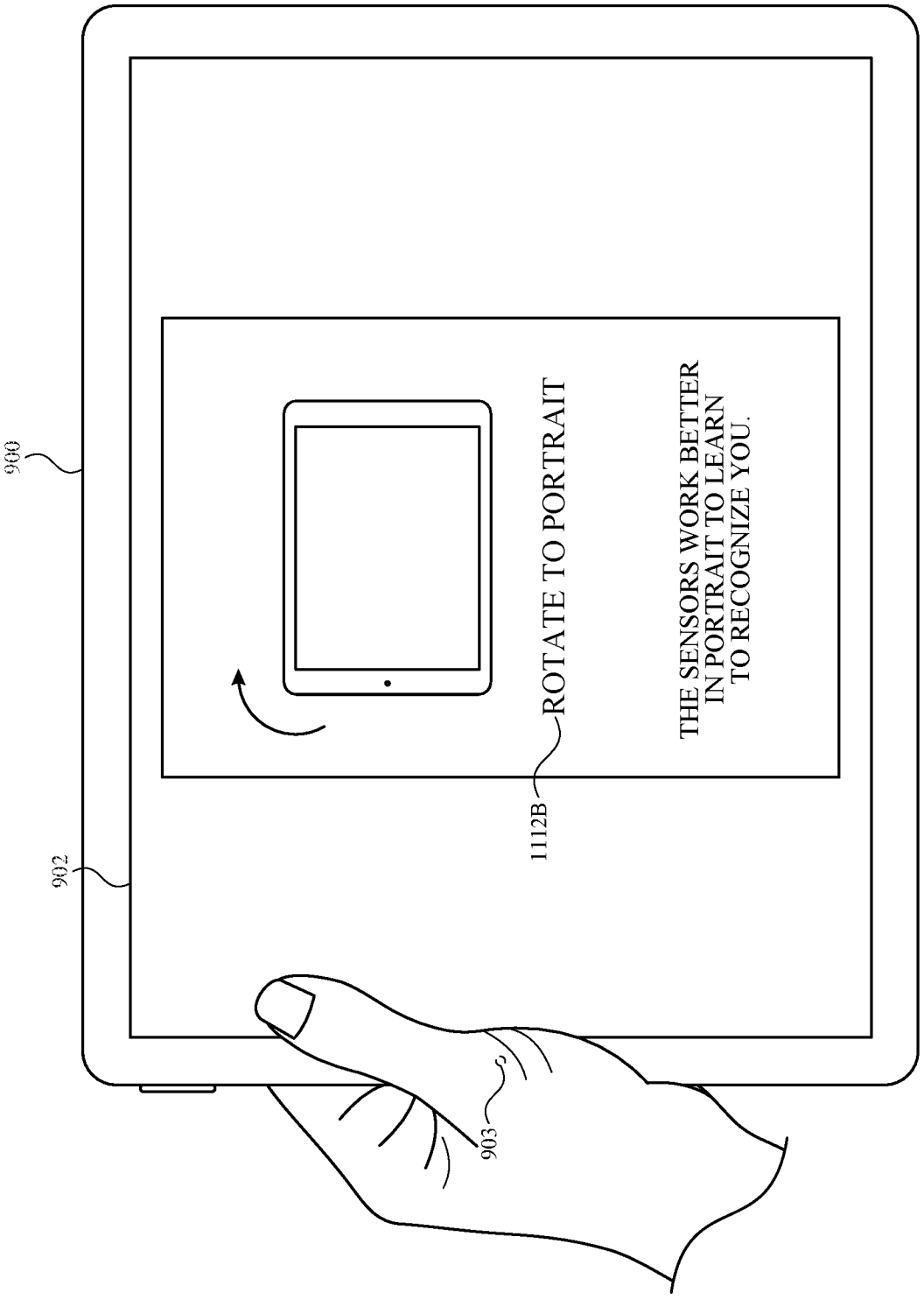


FIG. 11C

2022279466 30 Nov 2022

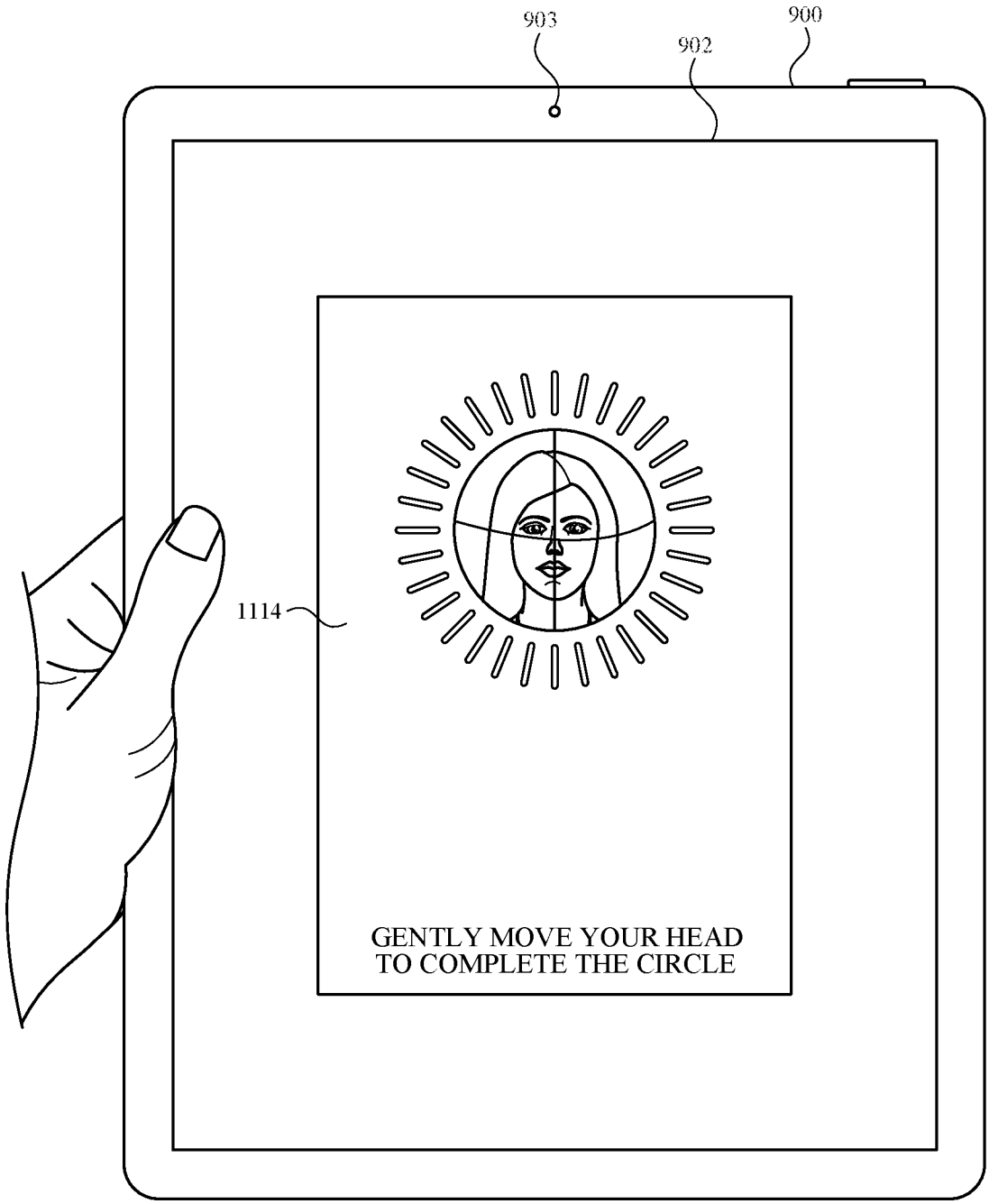


FIG. 11D

2022279466 30 Nov 2022

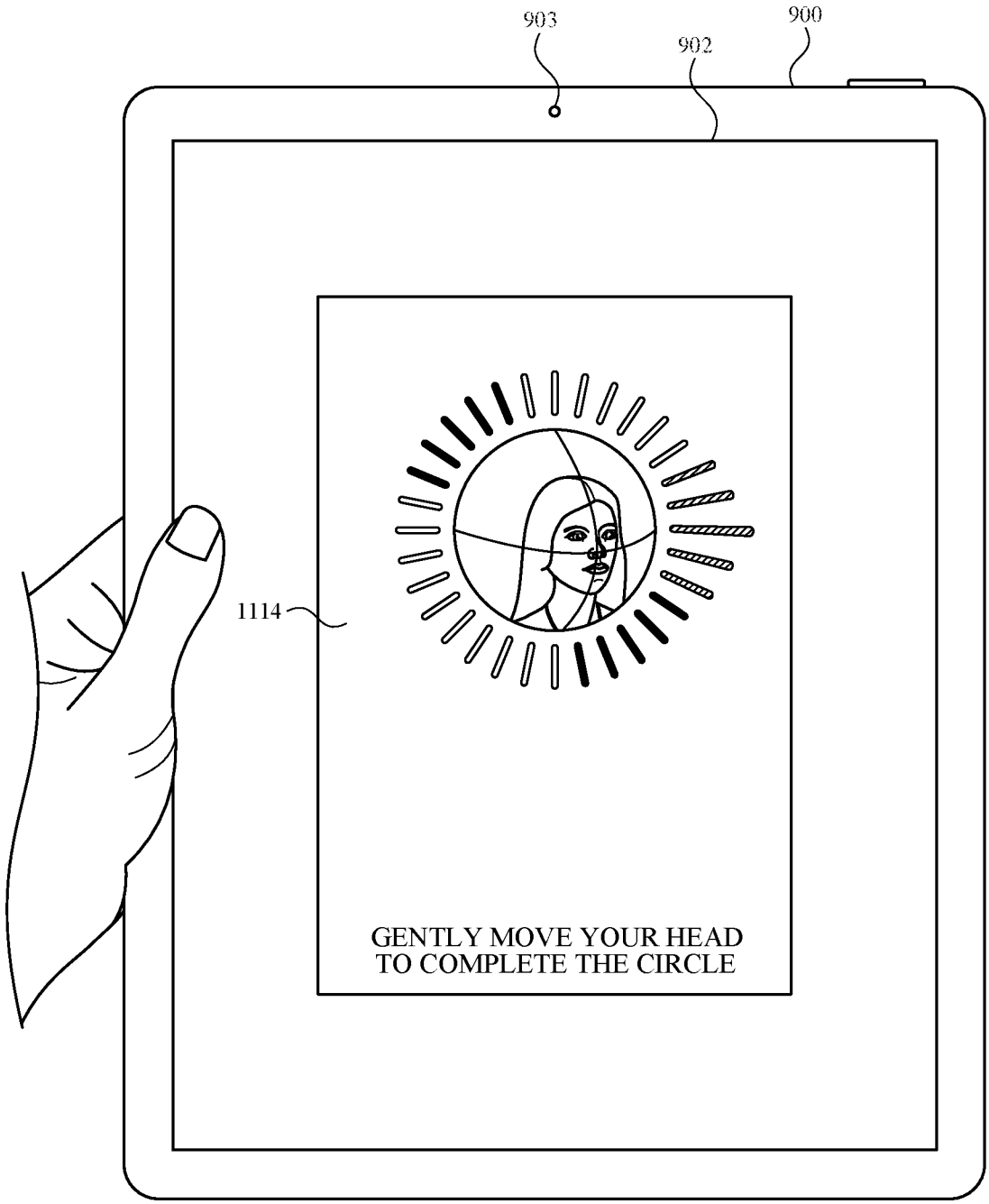


FIG. 11E

30 Nov 2022
2022279466

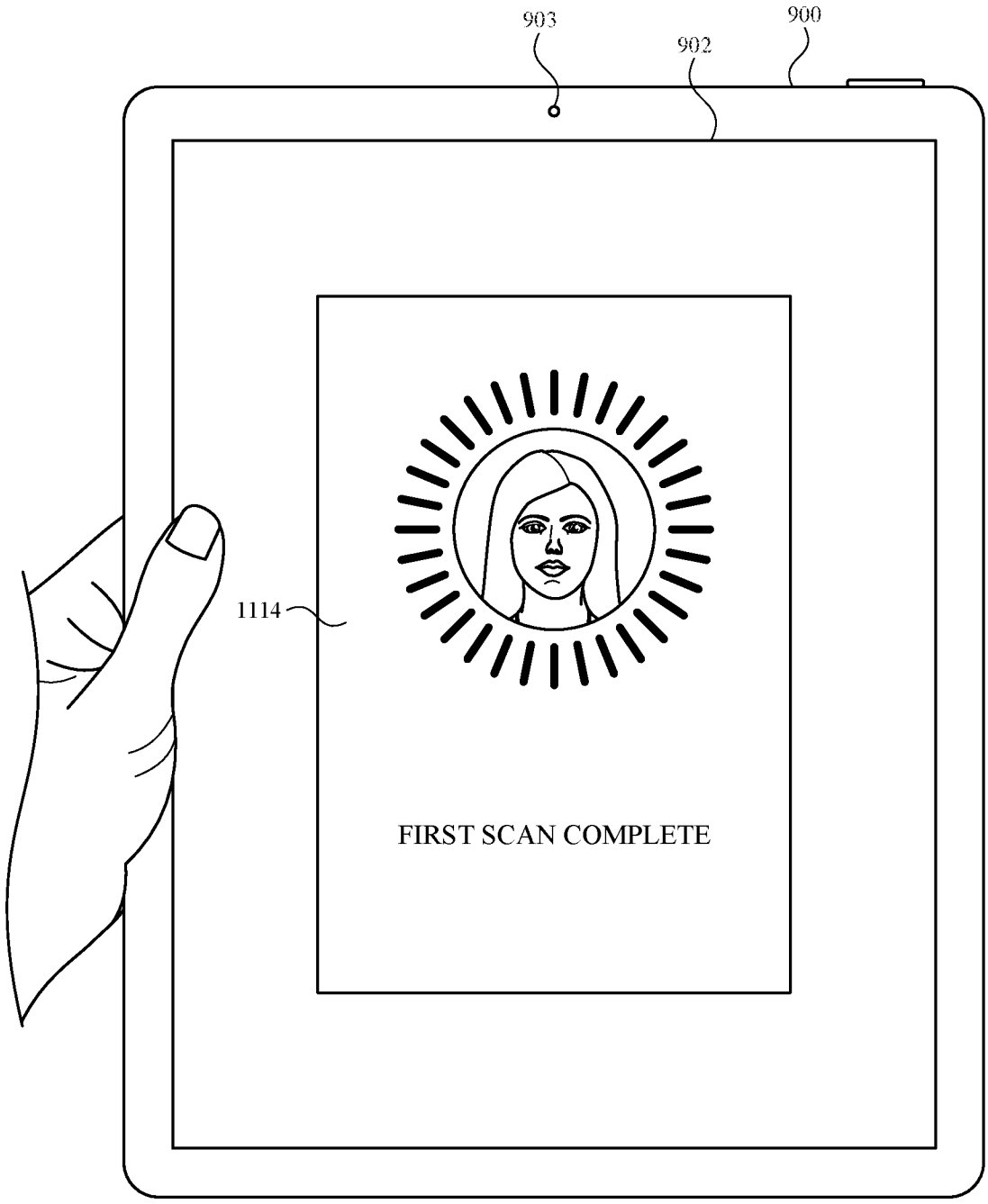


FIG. 11F

30 Nov 2022
2022279466

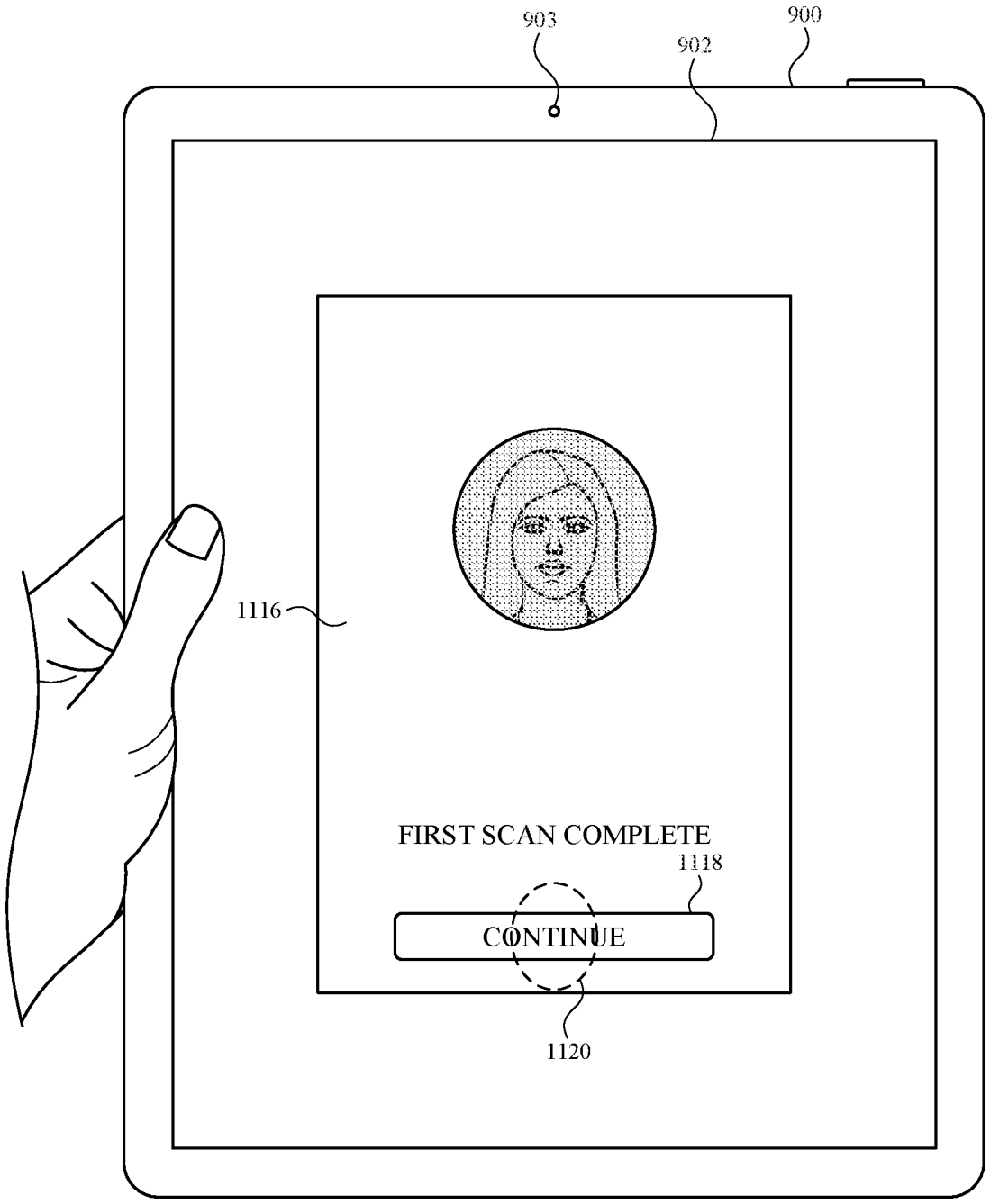


FIG. 11G

2022279466 30 Nov 2022

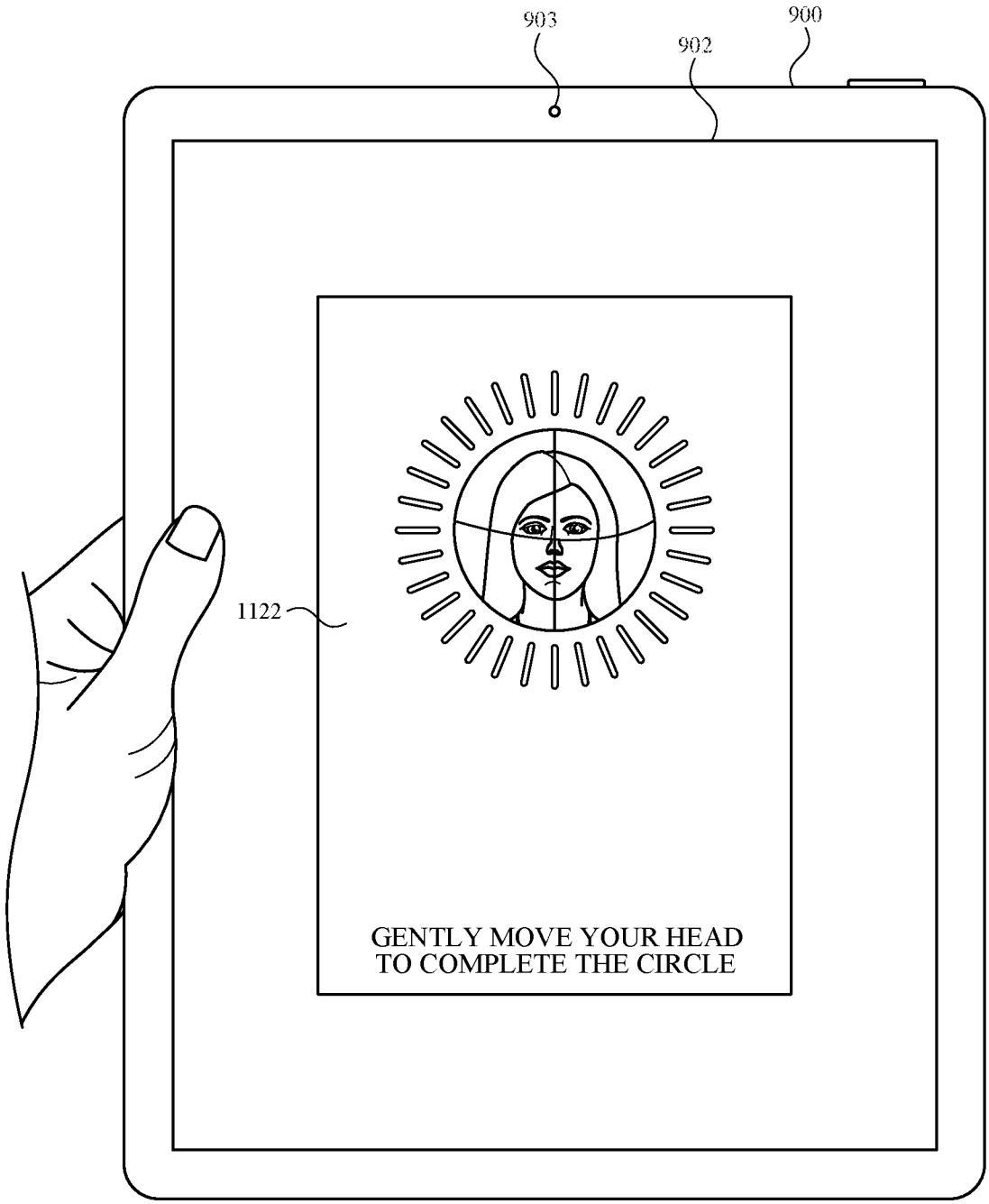


FIG. 11H

30 Nov 2022
2022279466

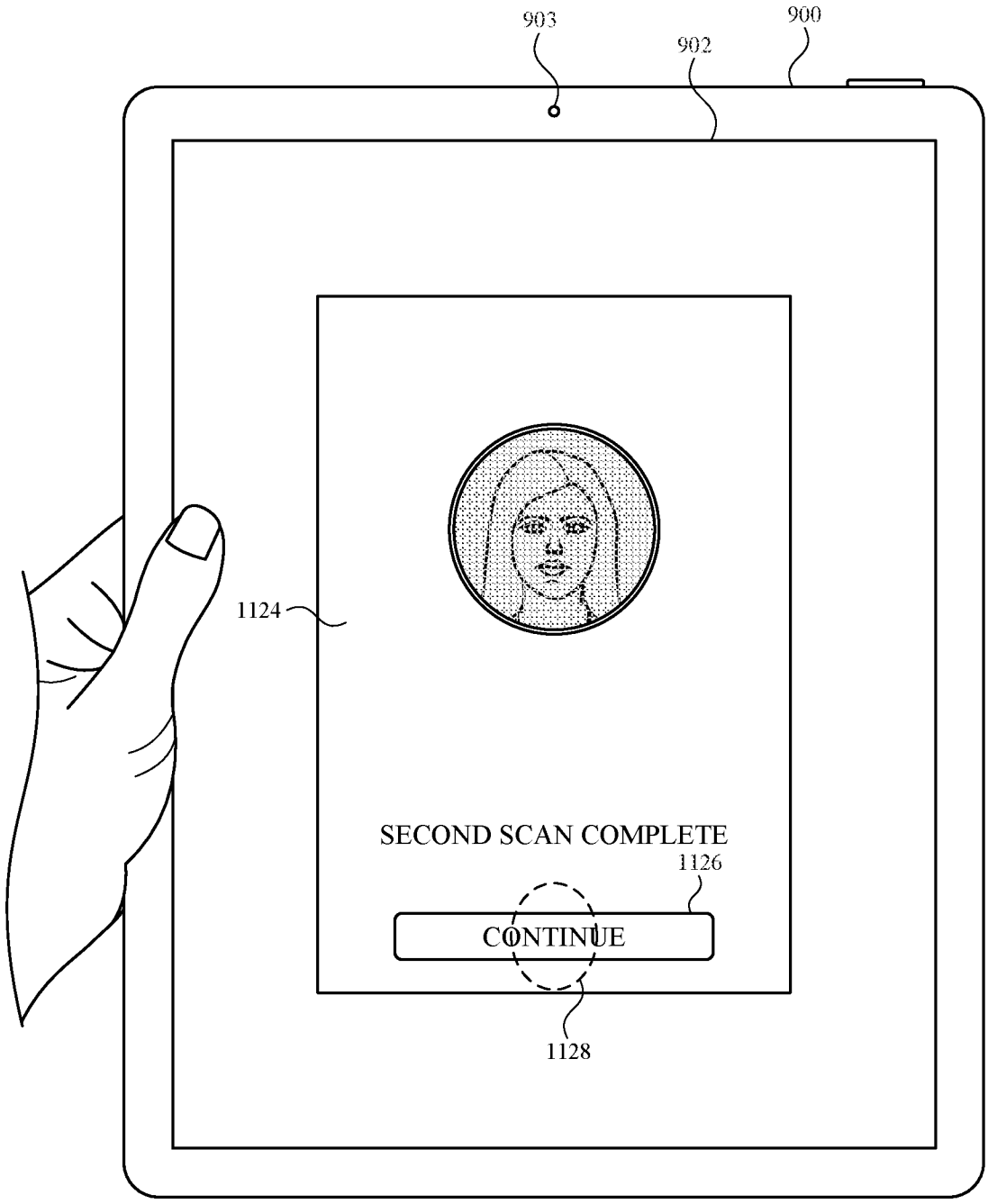


FIG. 11I

30 Nov 2022
2022279466

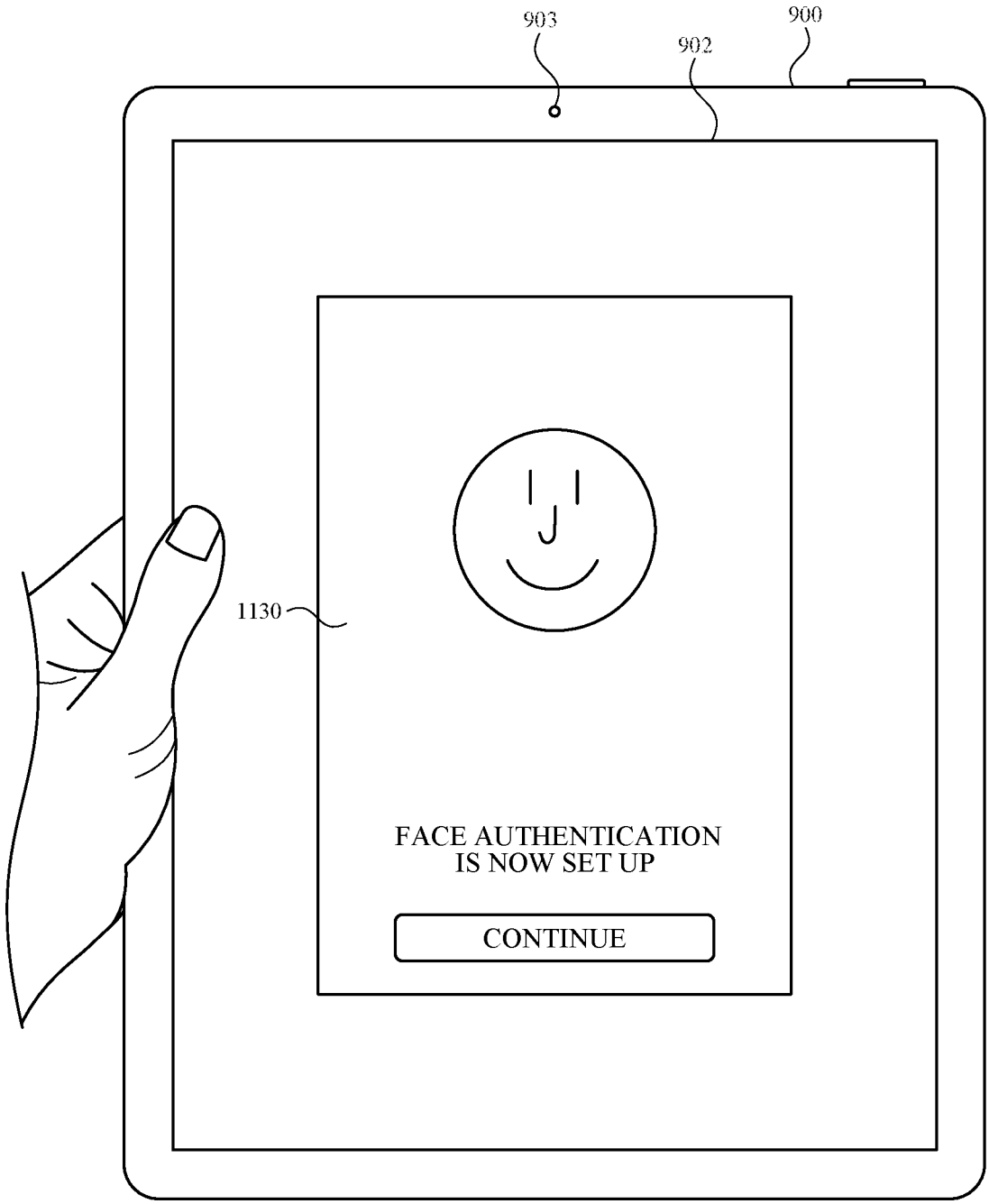


FIG. 11J

2022279466 30 Nov 2022

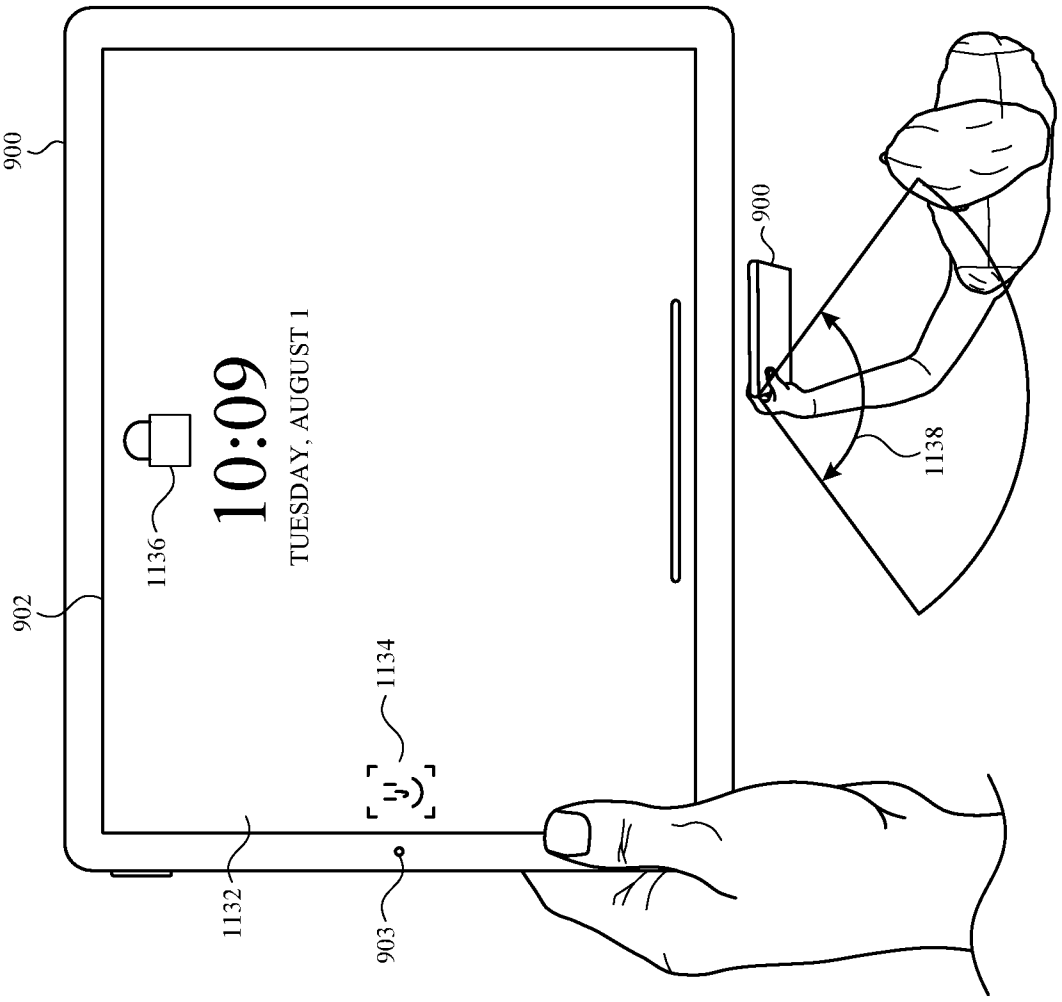


FIG. 11K

2022279466 30 Nov 2022

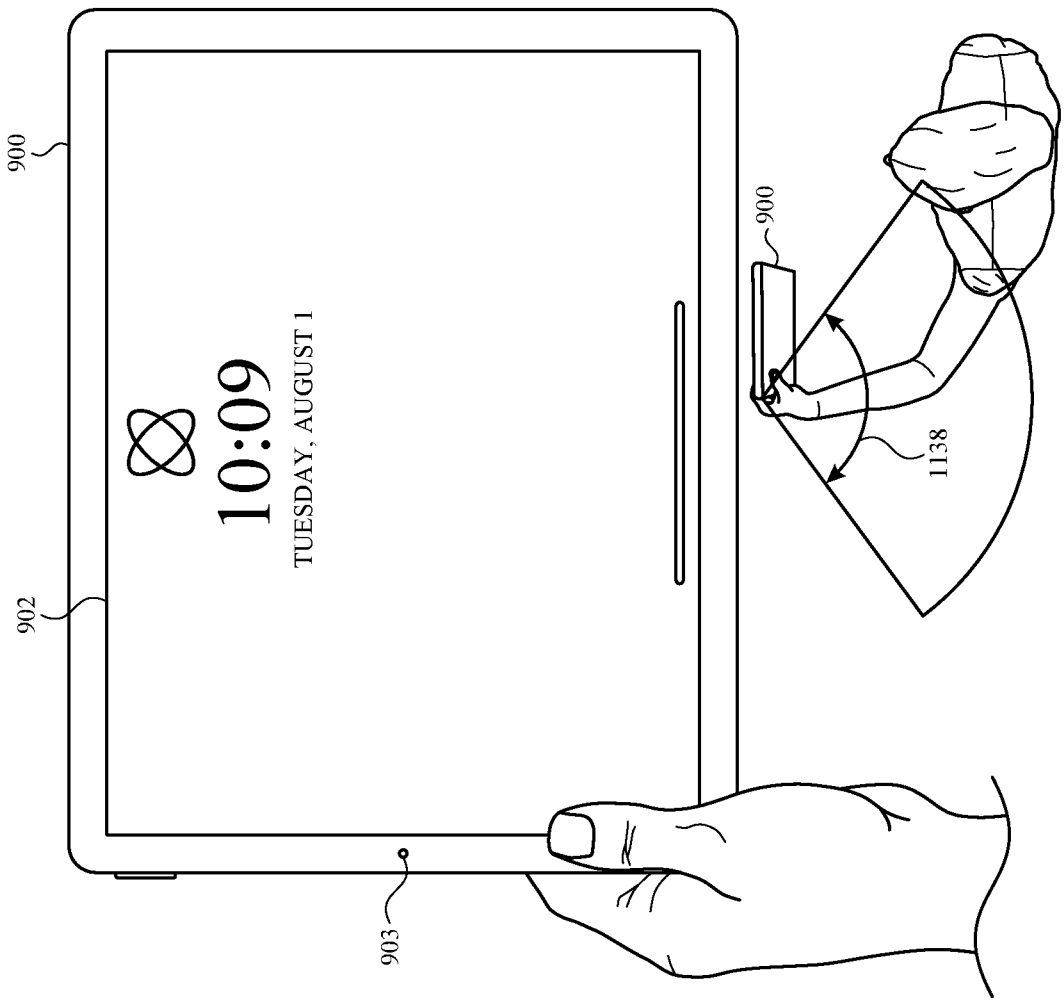


FIG. 11L

2022279466 30 Nov 2022

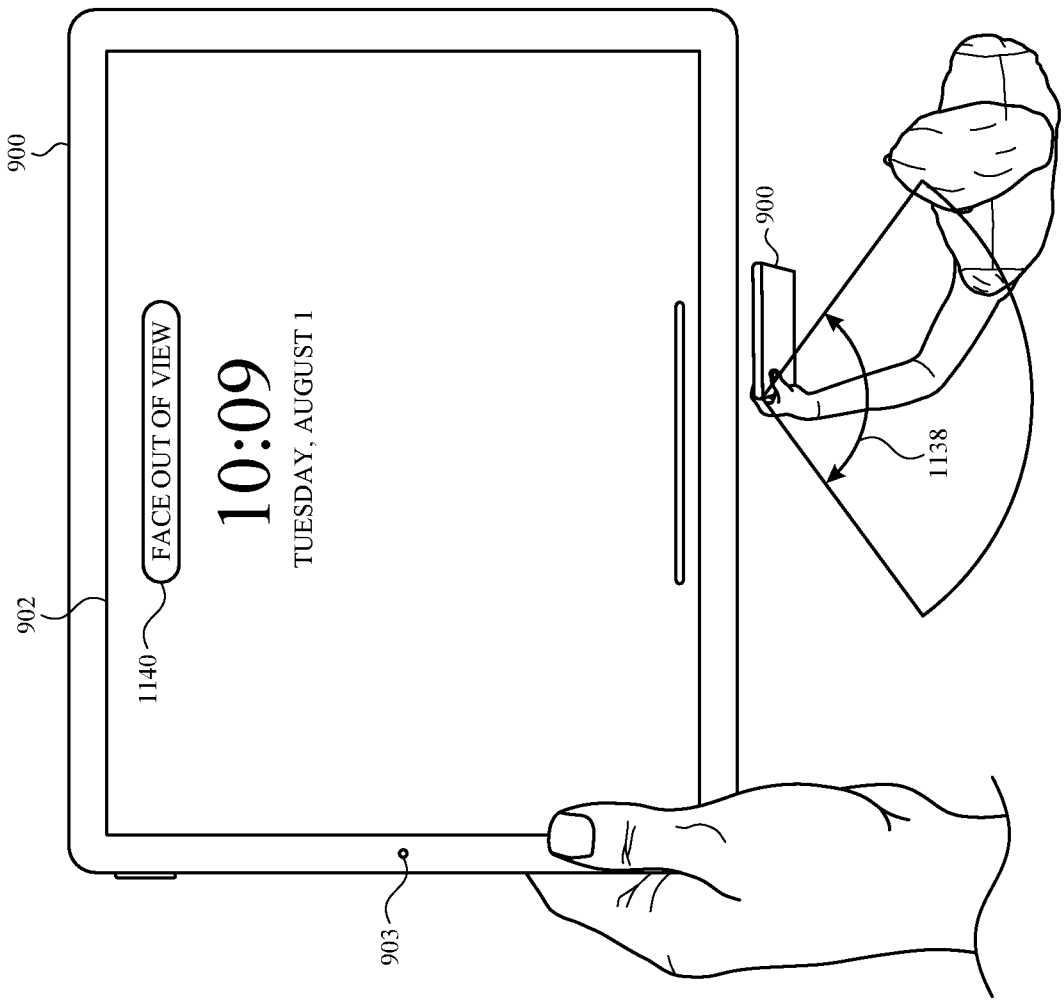


FIG. 11M

2022279466 30 Nov 2022

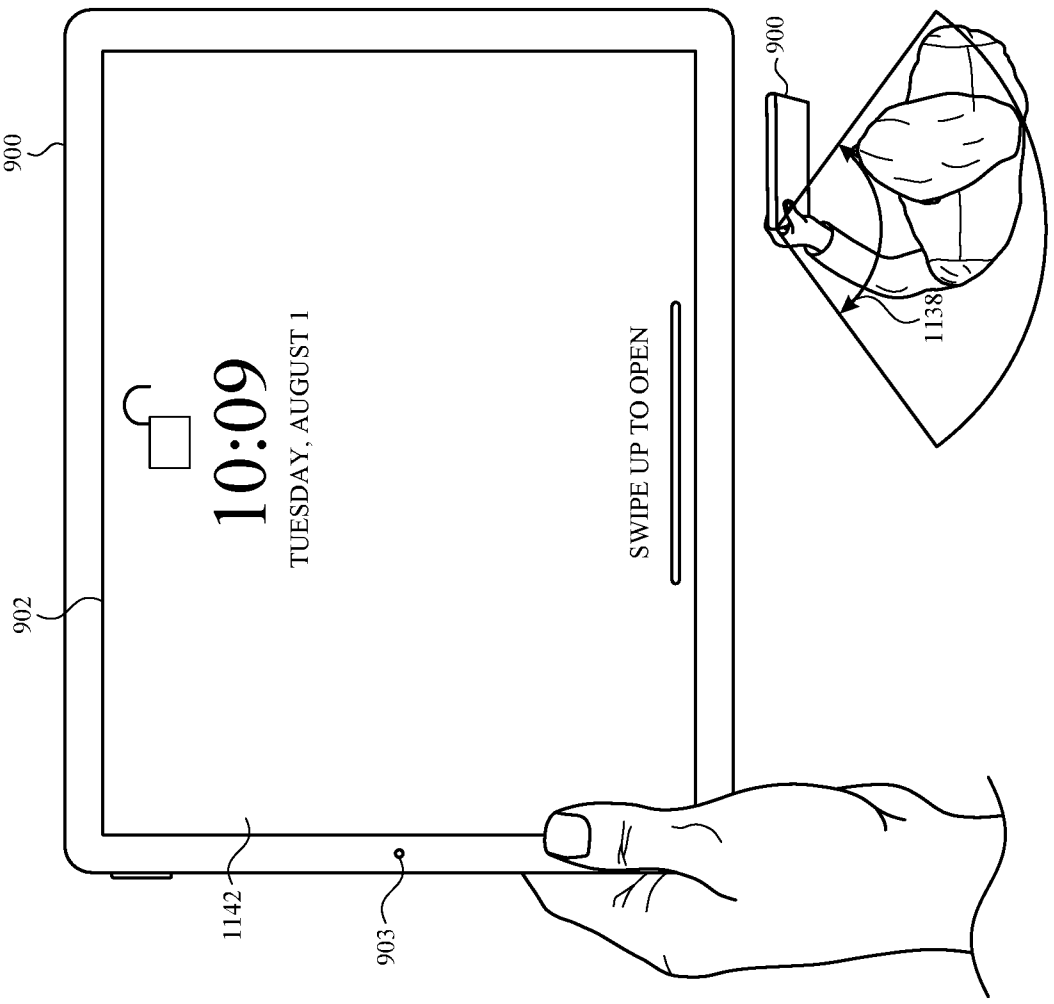


FIG. 11N

2022279466 30 Nov 2022

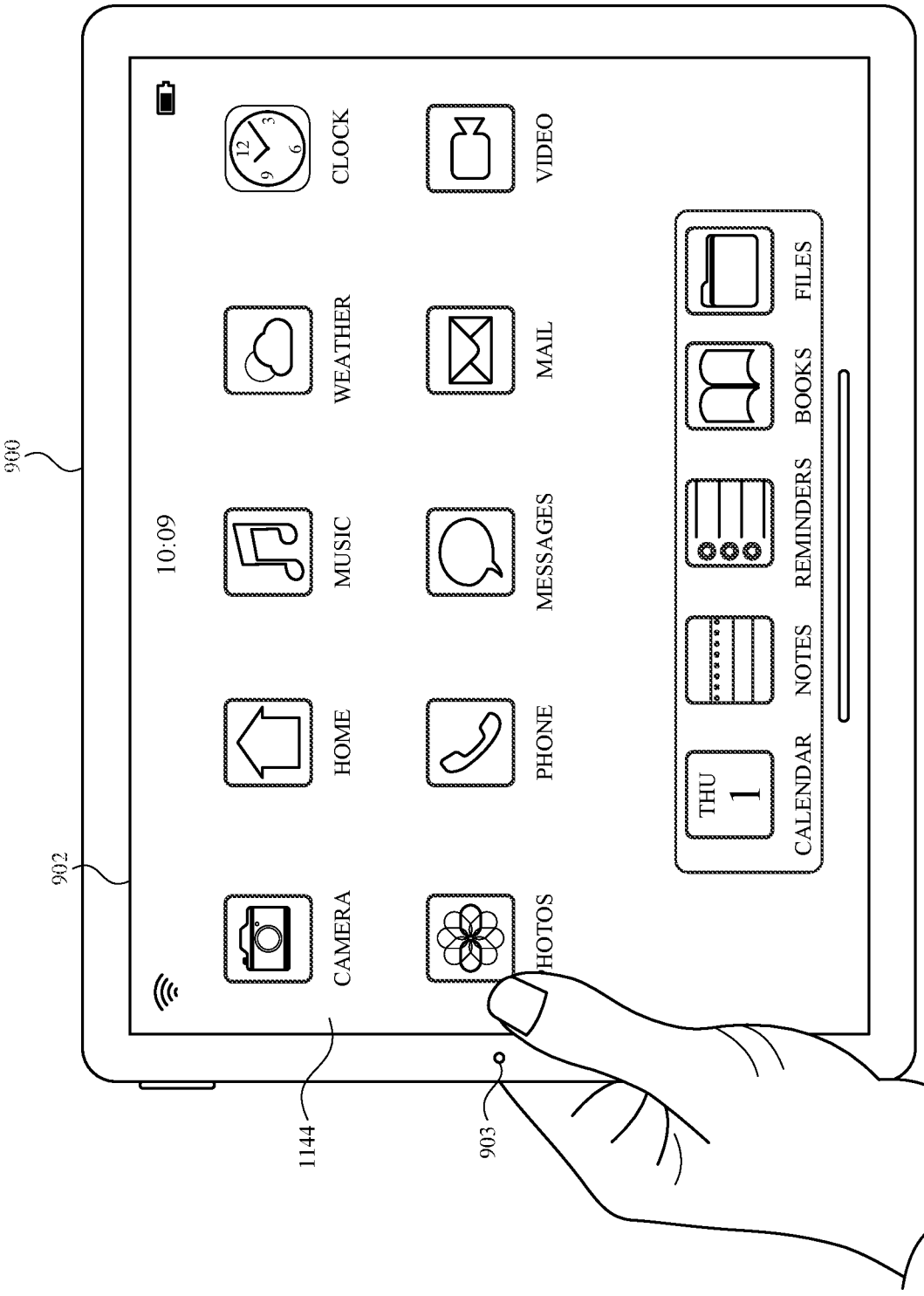


FIG. 110

2022279466 30 Nov 2022

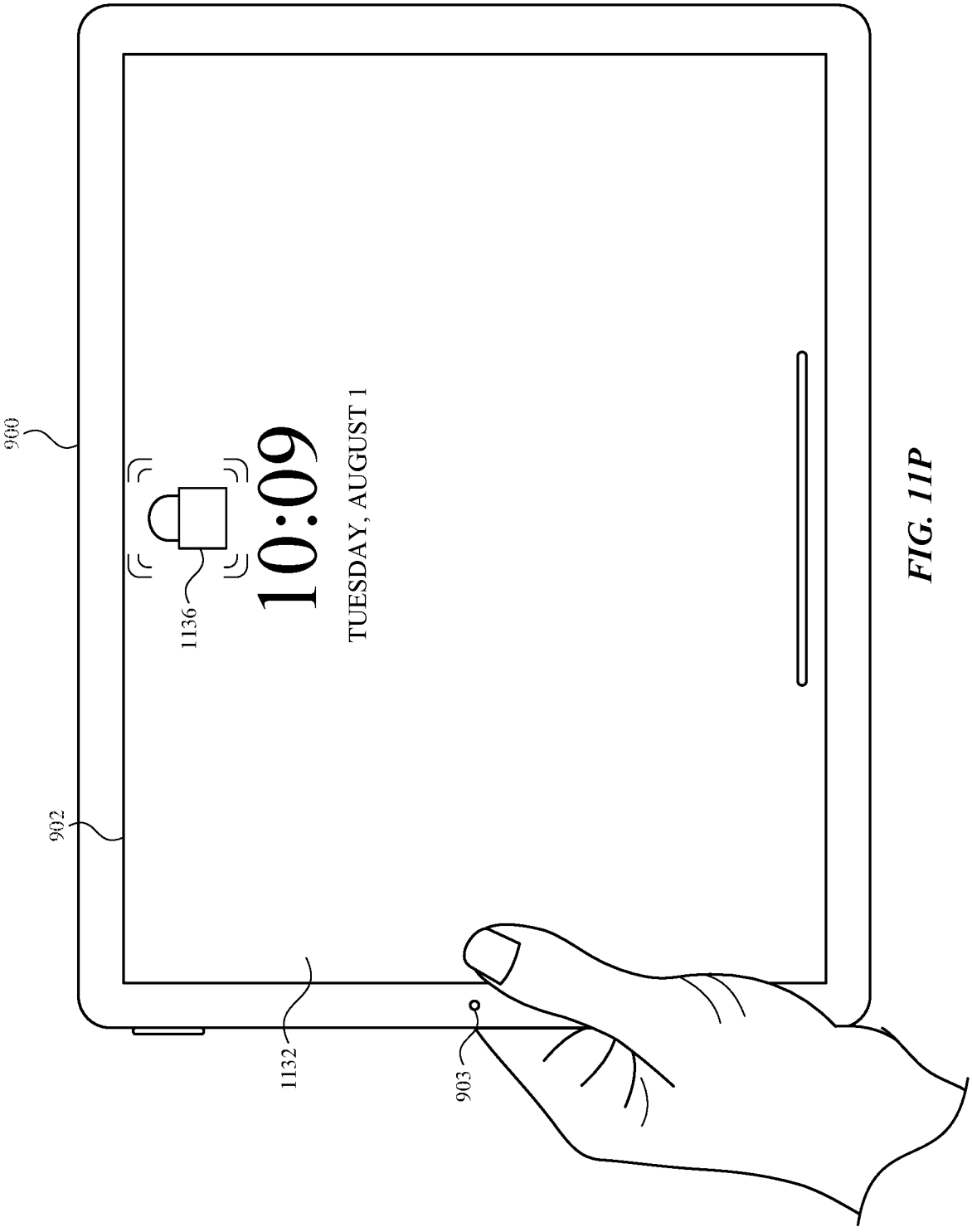


FIG. 11P

2022279466 30 Nov 2022

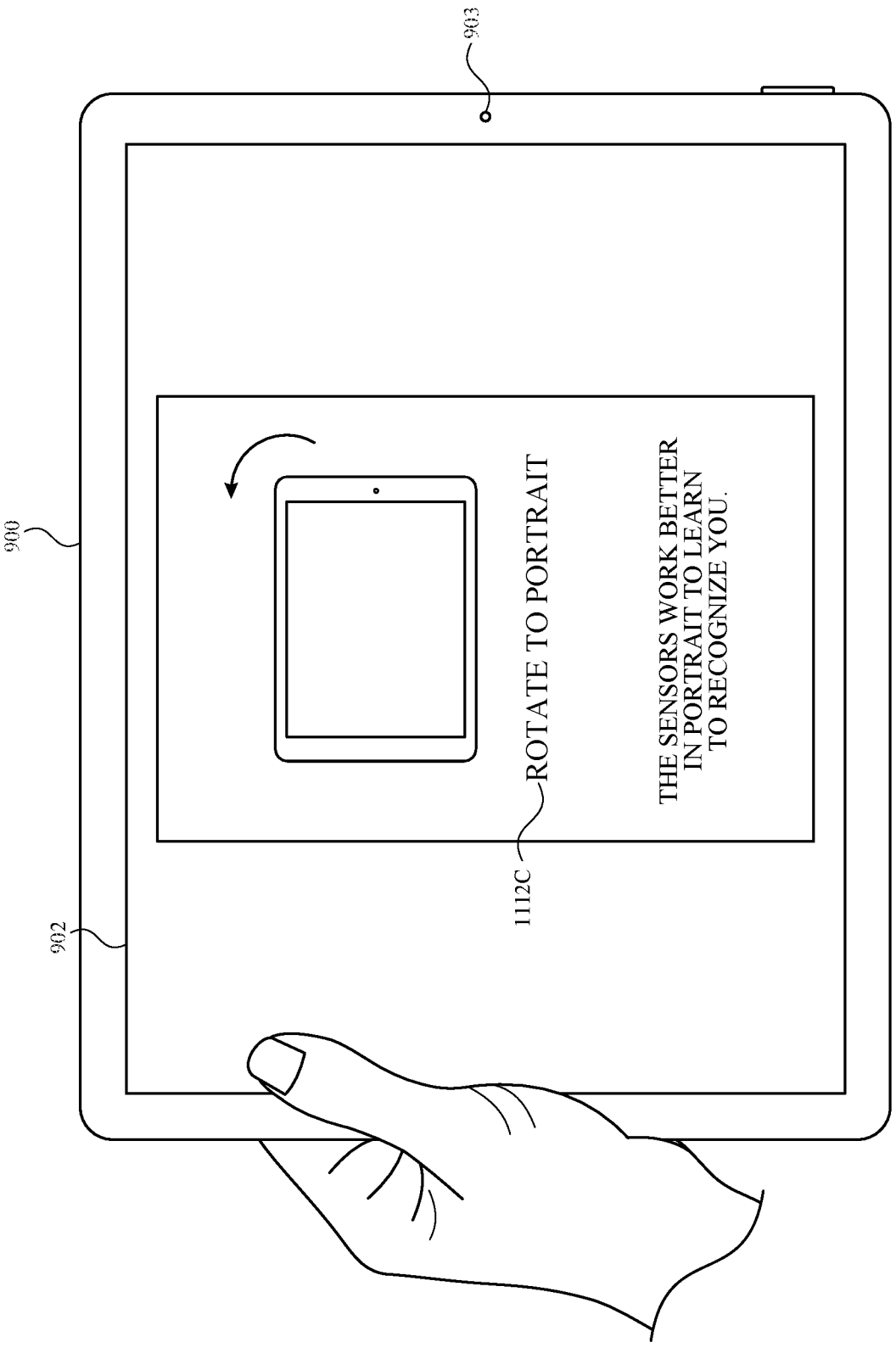


FIG. 11Q

2022279466 30 Nov 2022

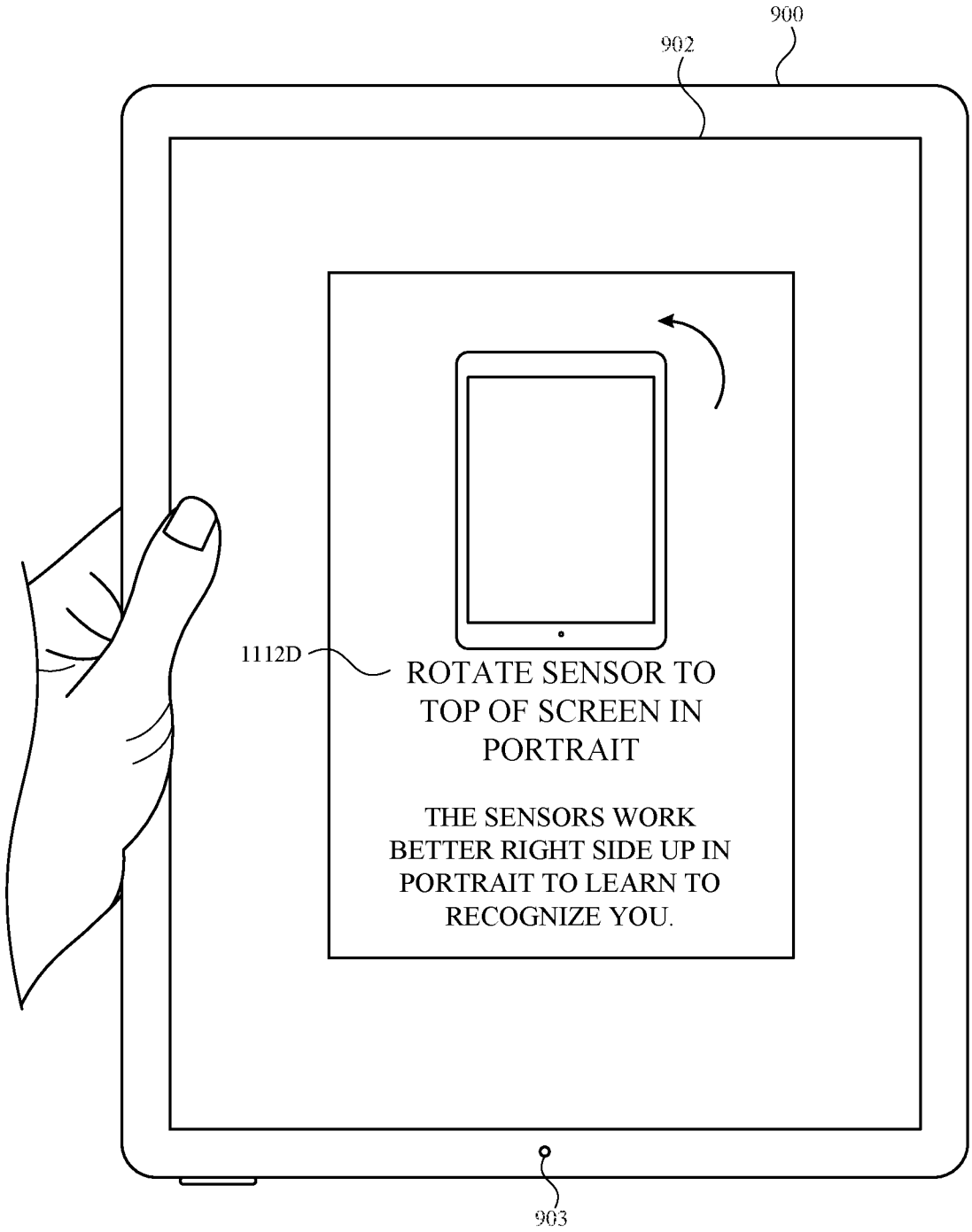


FIG. 11R

2022279466 30 Nov 2022

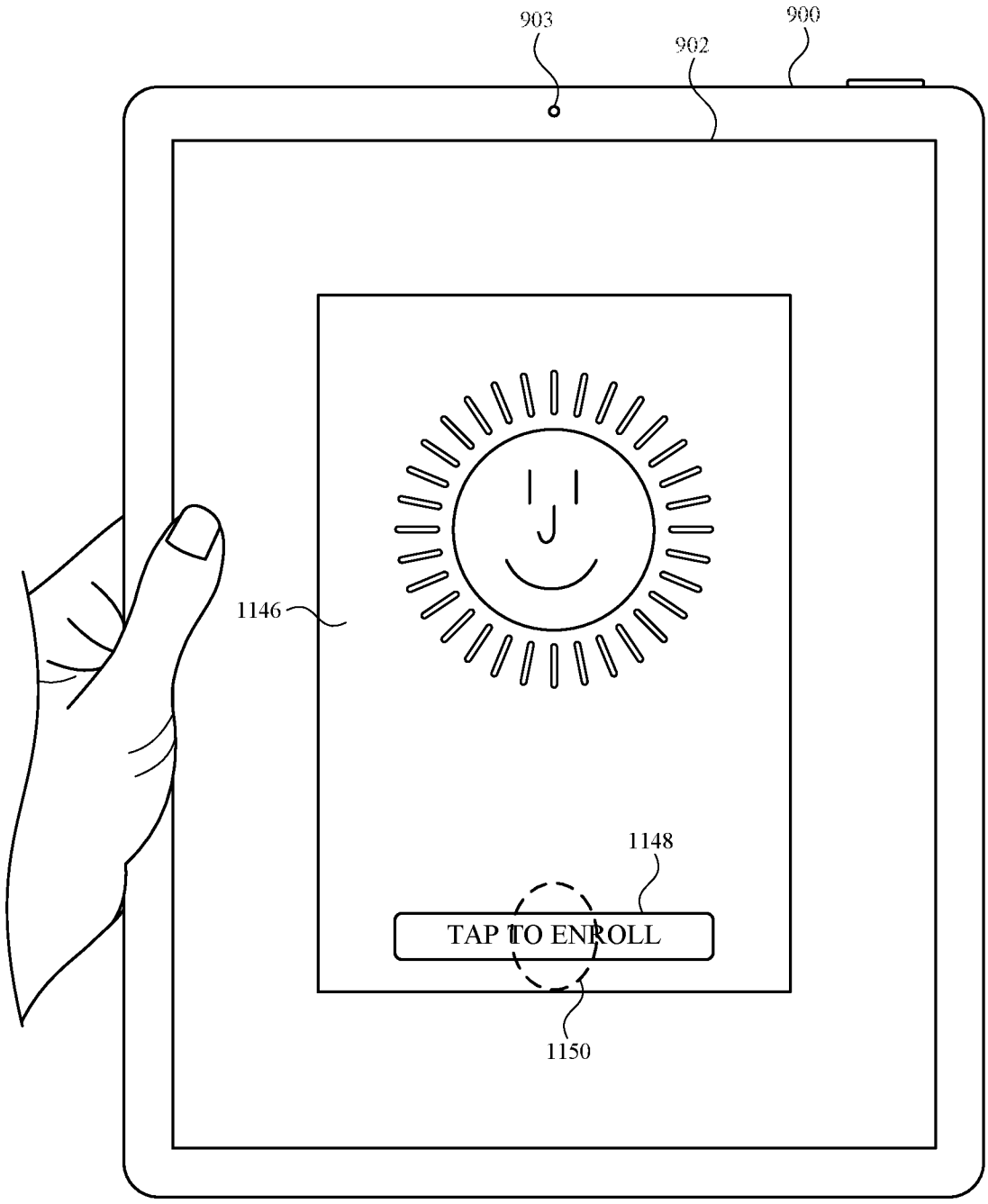


FIG. 11S

30 Nov 2022
2022279466

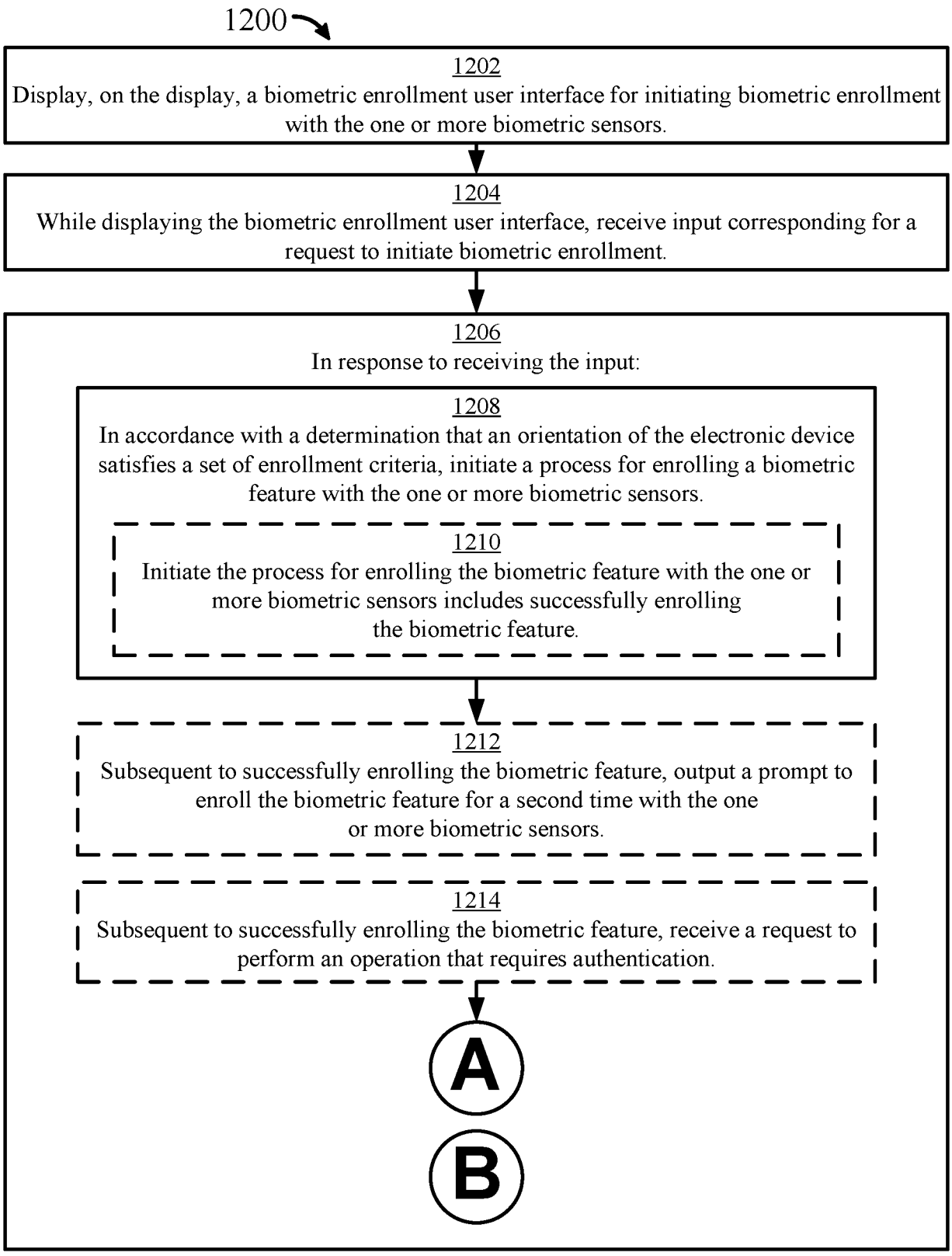


FIG. 12A

30 Nov 2022
2022279466

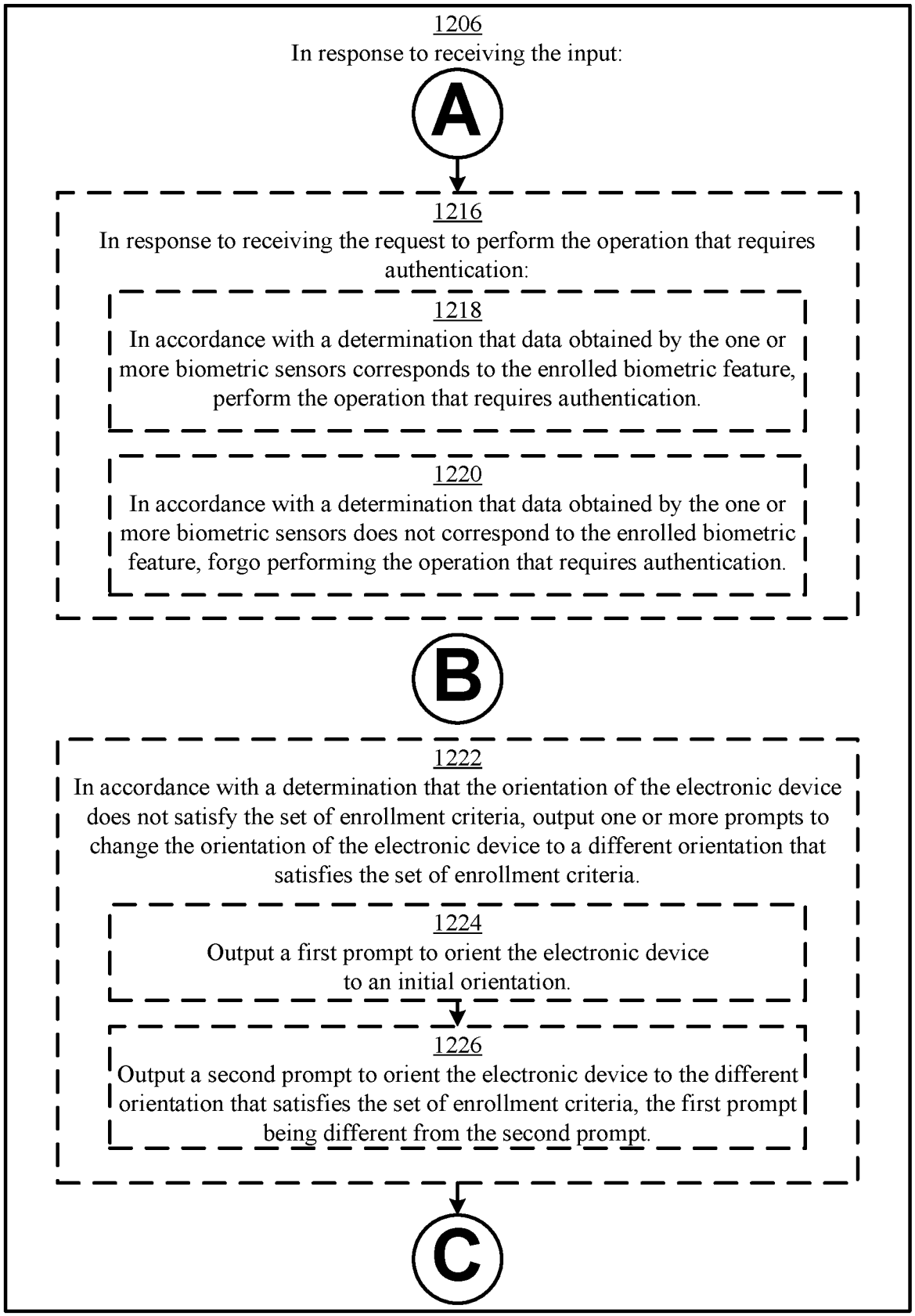


FIG. 12B

2022279466 30 Nov 2022

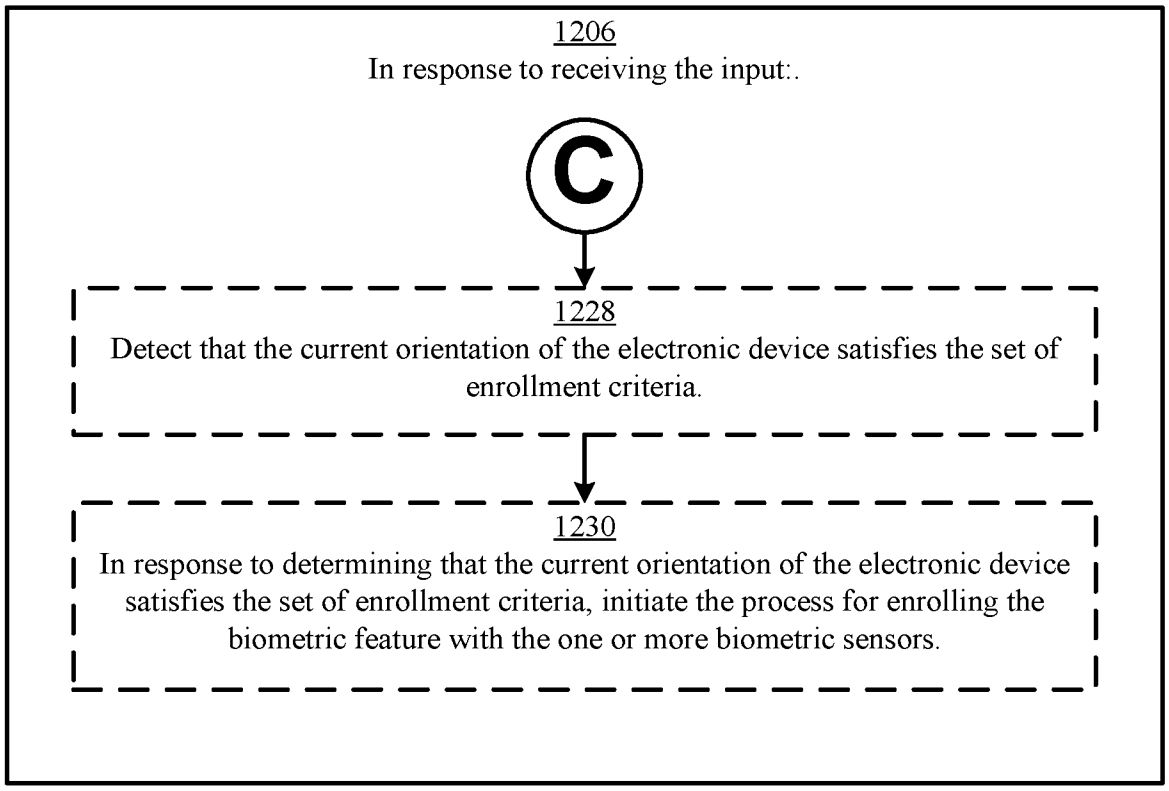


FIG. 12C

2022279466 30 Nov 2022

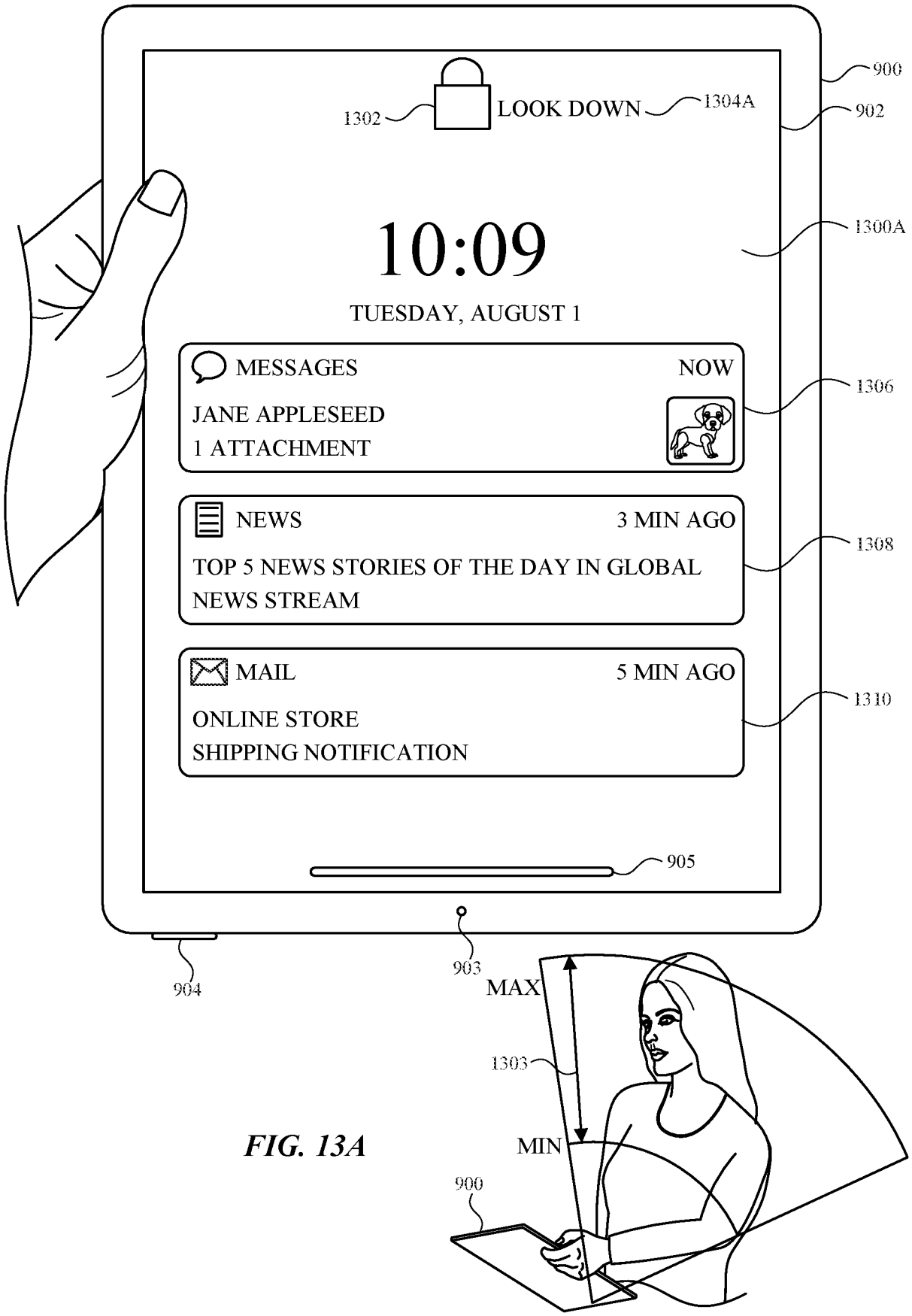


FIG. 13A

2022279466 30 Nov 2022

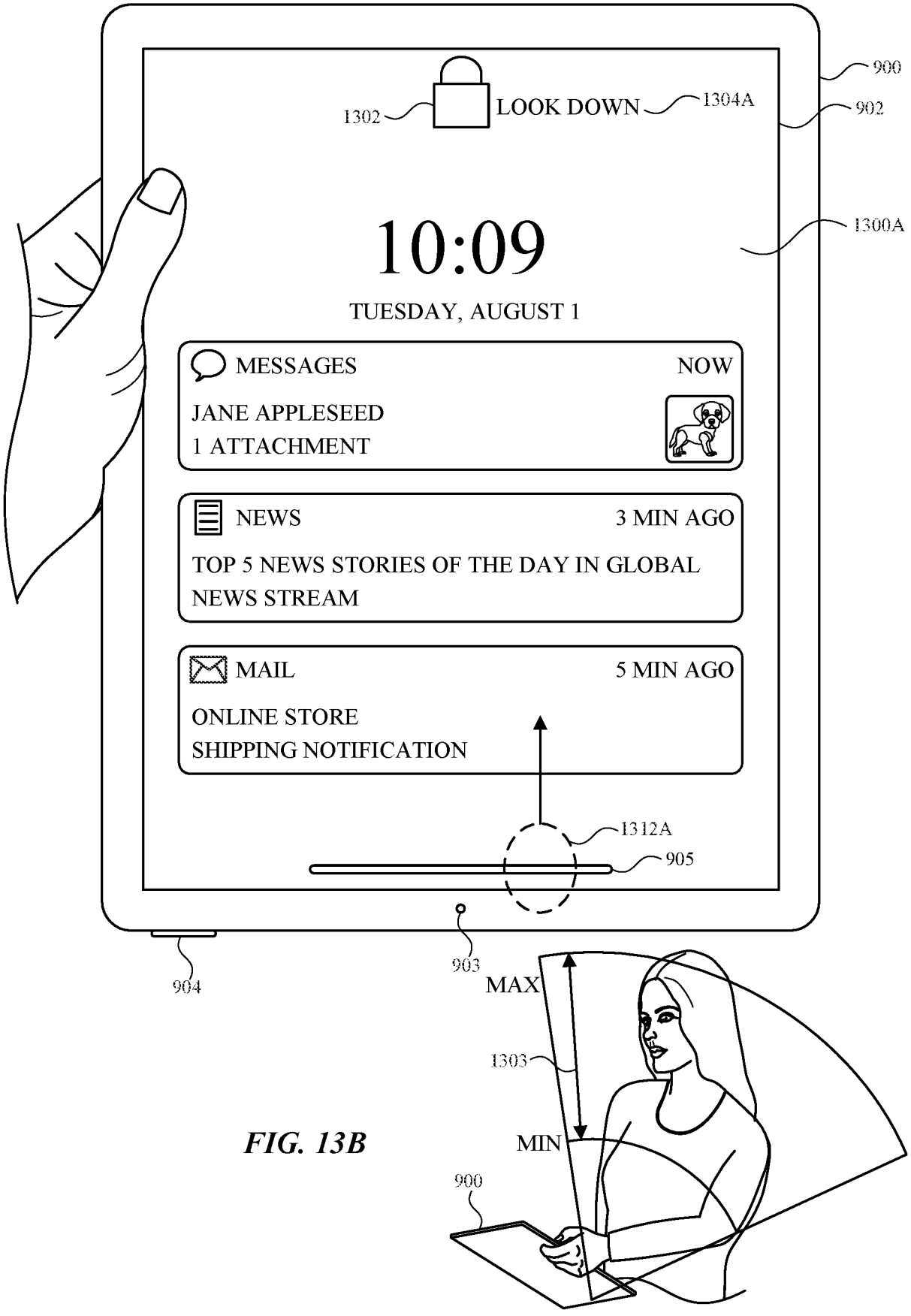


FIG. 13B

2022279466 30 Nov 2022

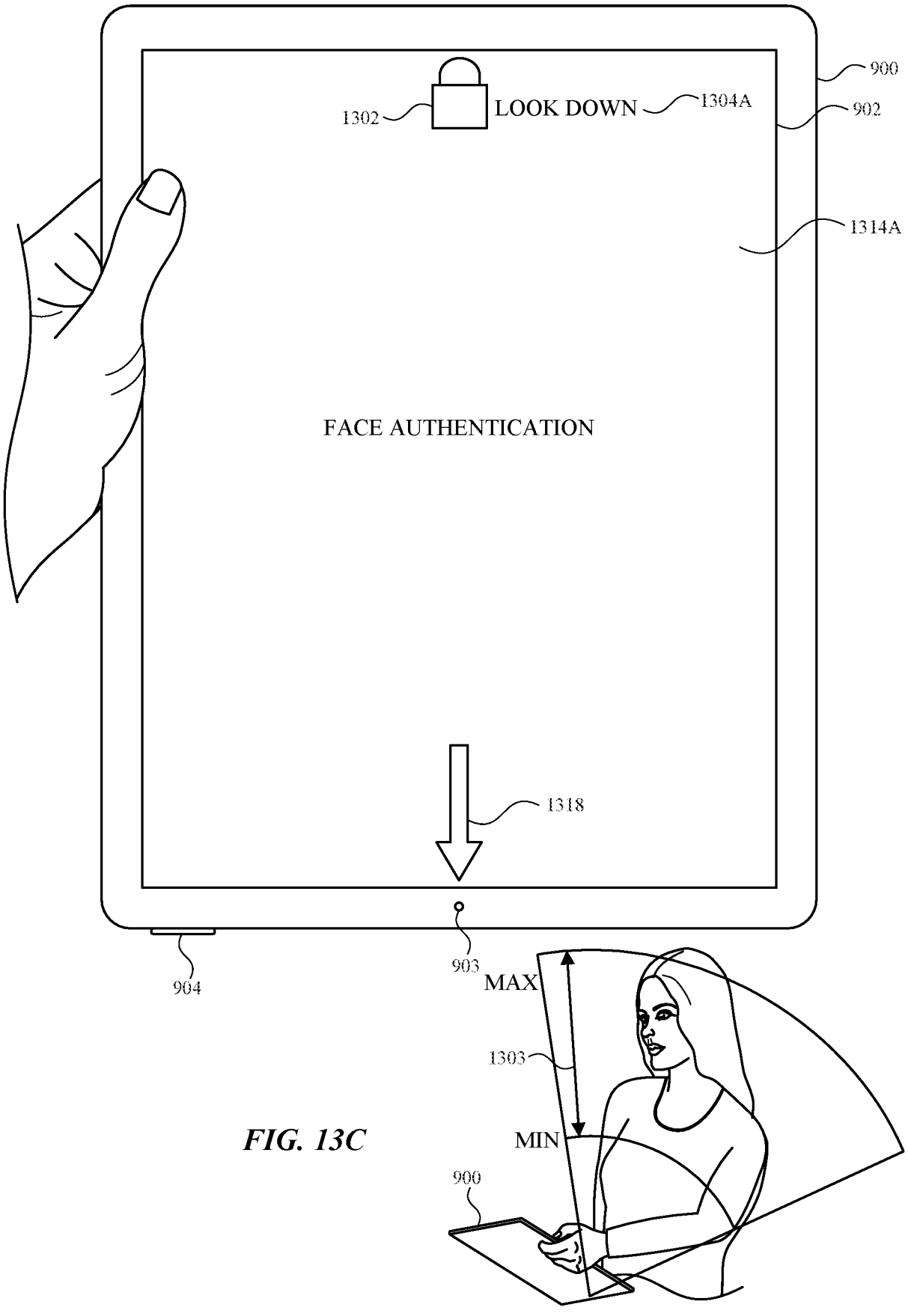


FIG. 13C

2022279466 30 Nov 2022

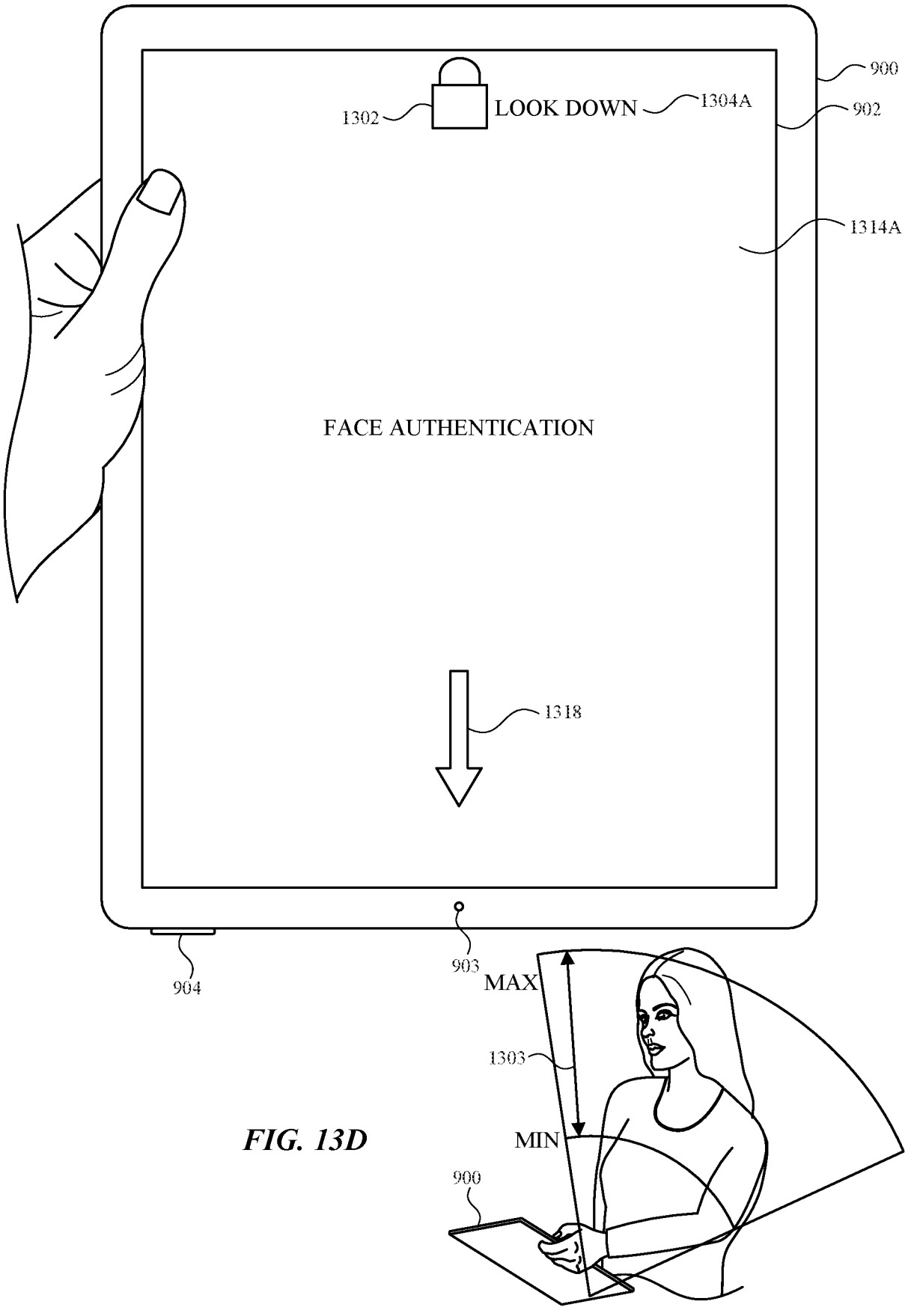


FIG. 13D

2022279466 30 Nov 2022

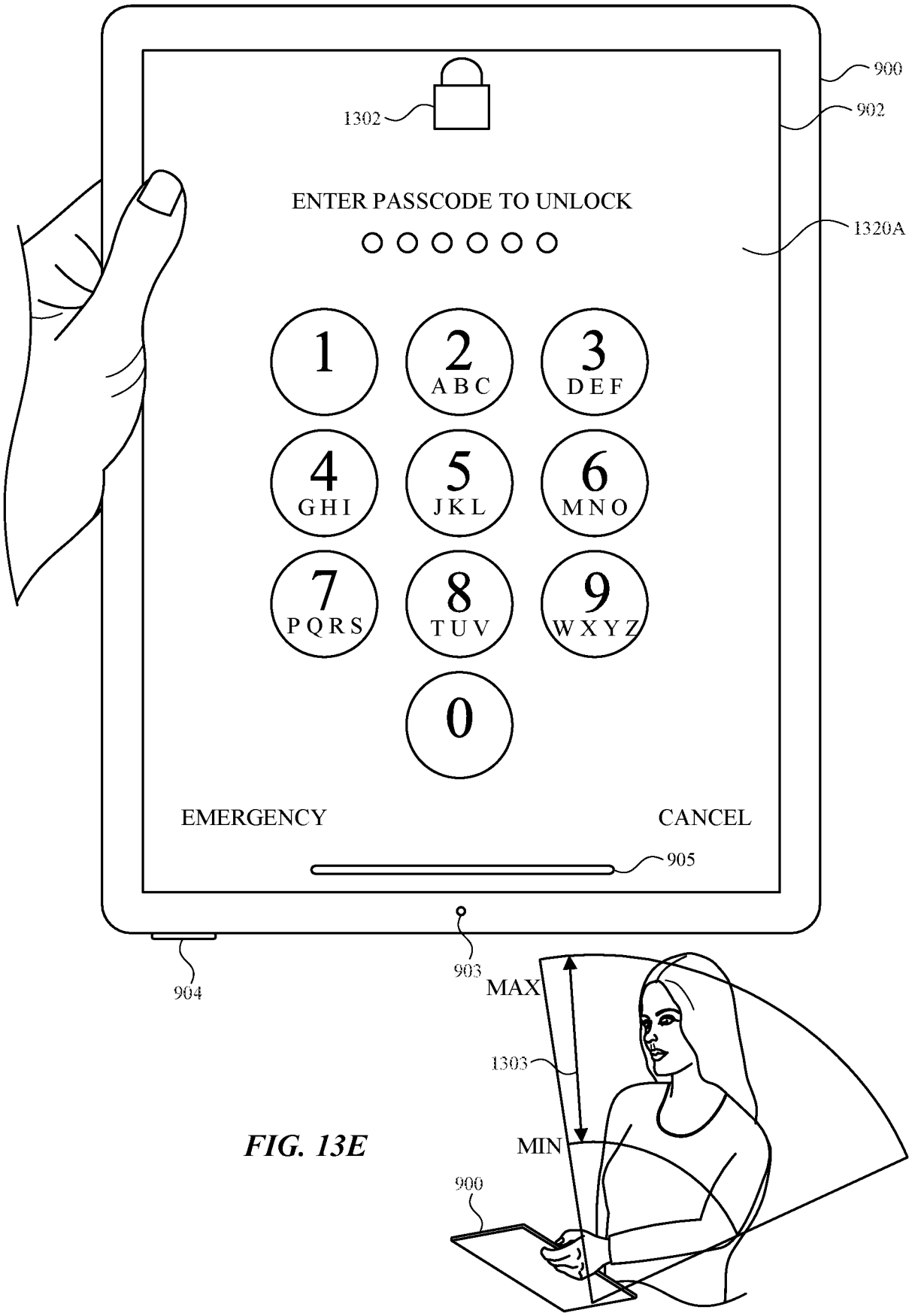


FIG. 13E

2022279466 30 Nov 2022

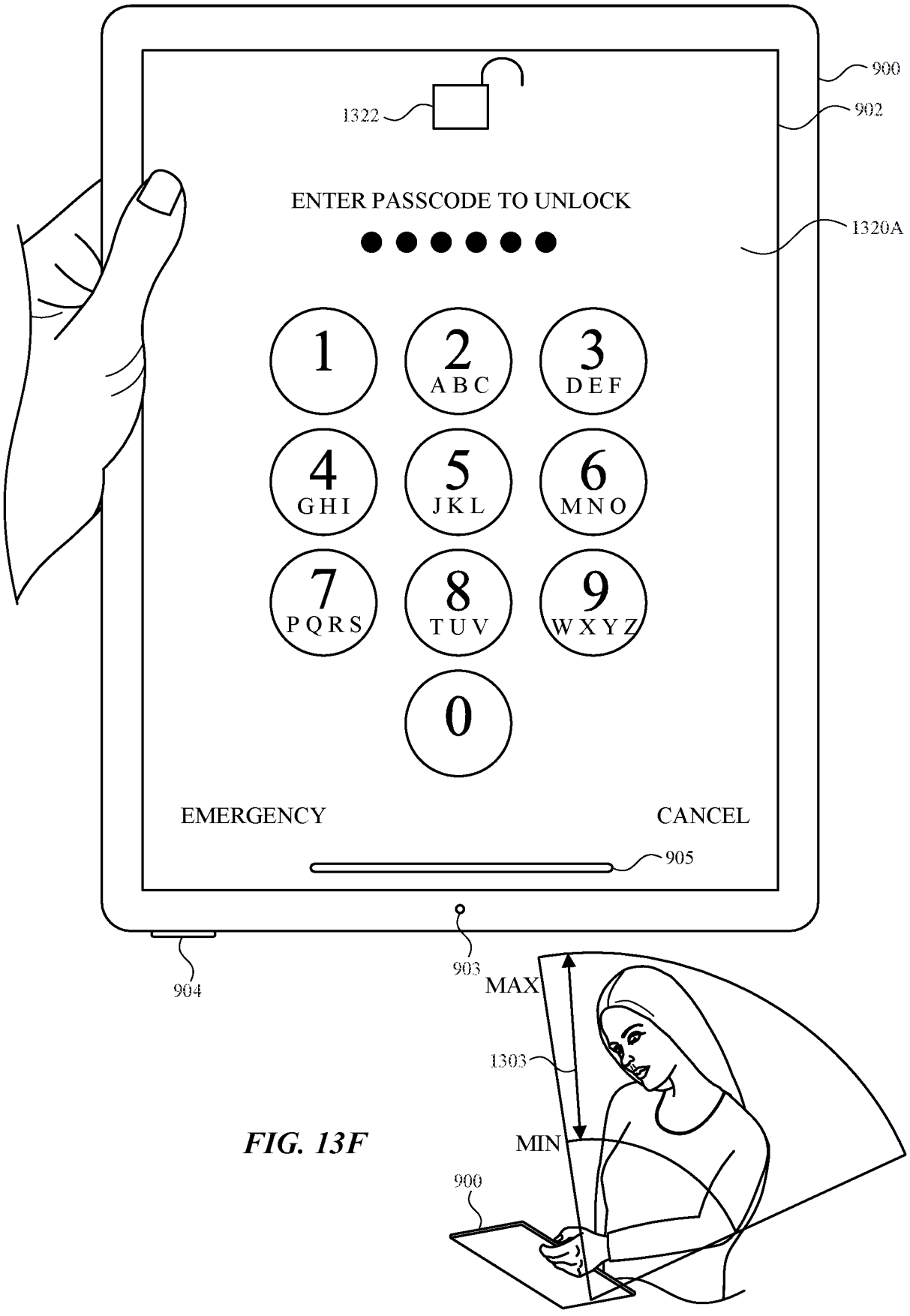


FIG. 13F

2022279466 30 Nov 2022

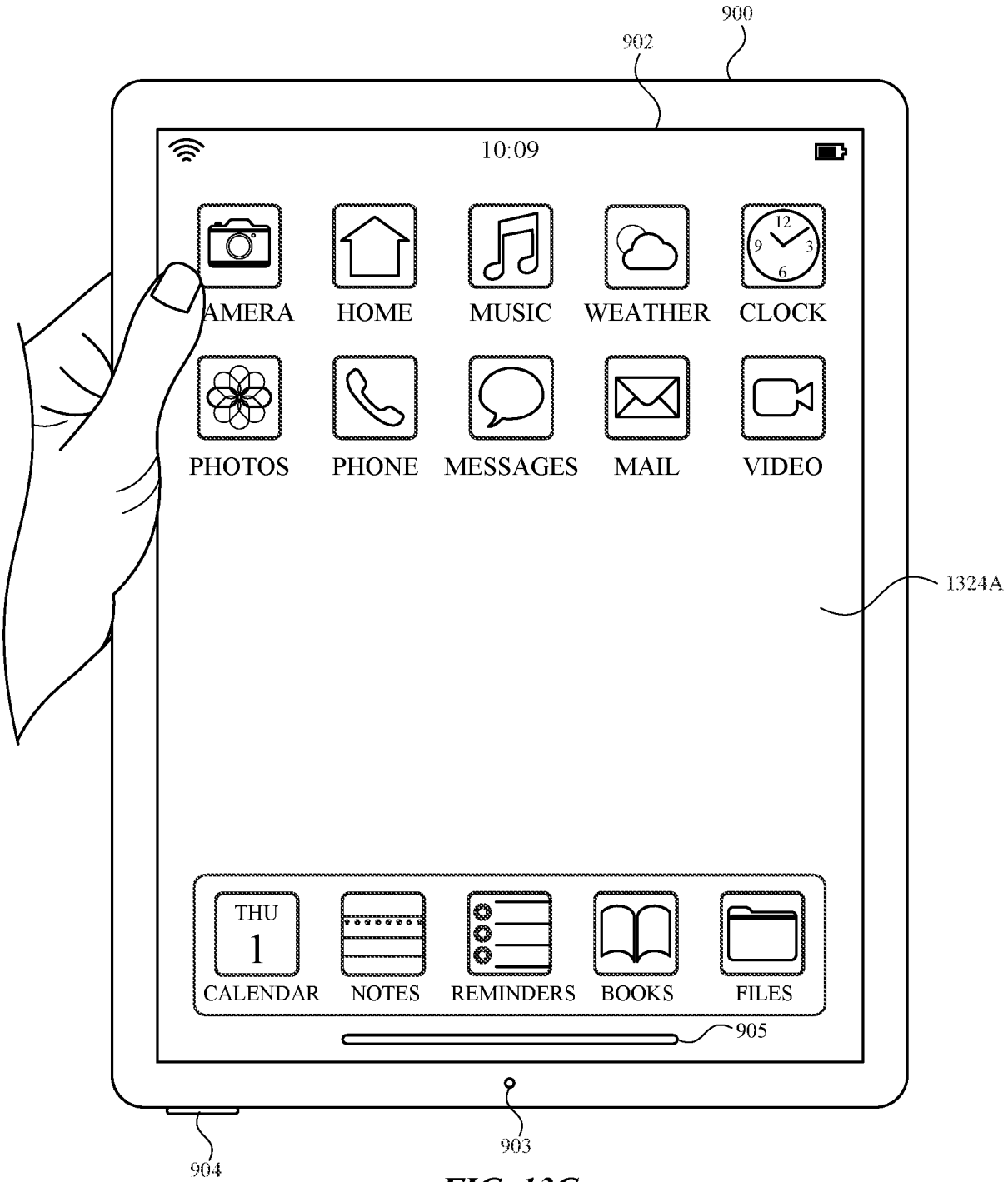


FIG. 13G

2022279466 30 Nov 2022

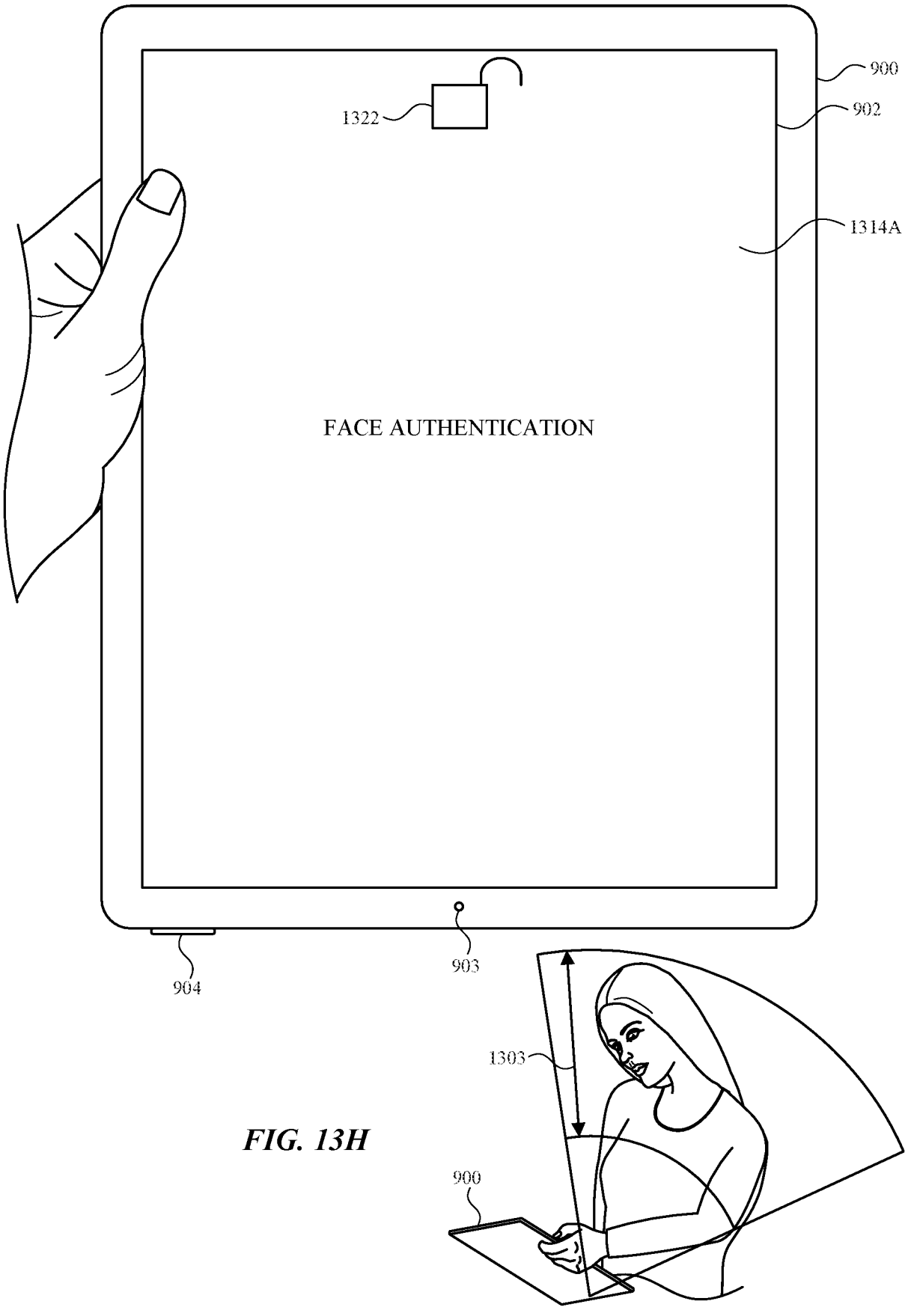
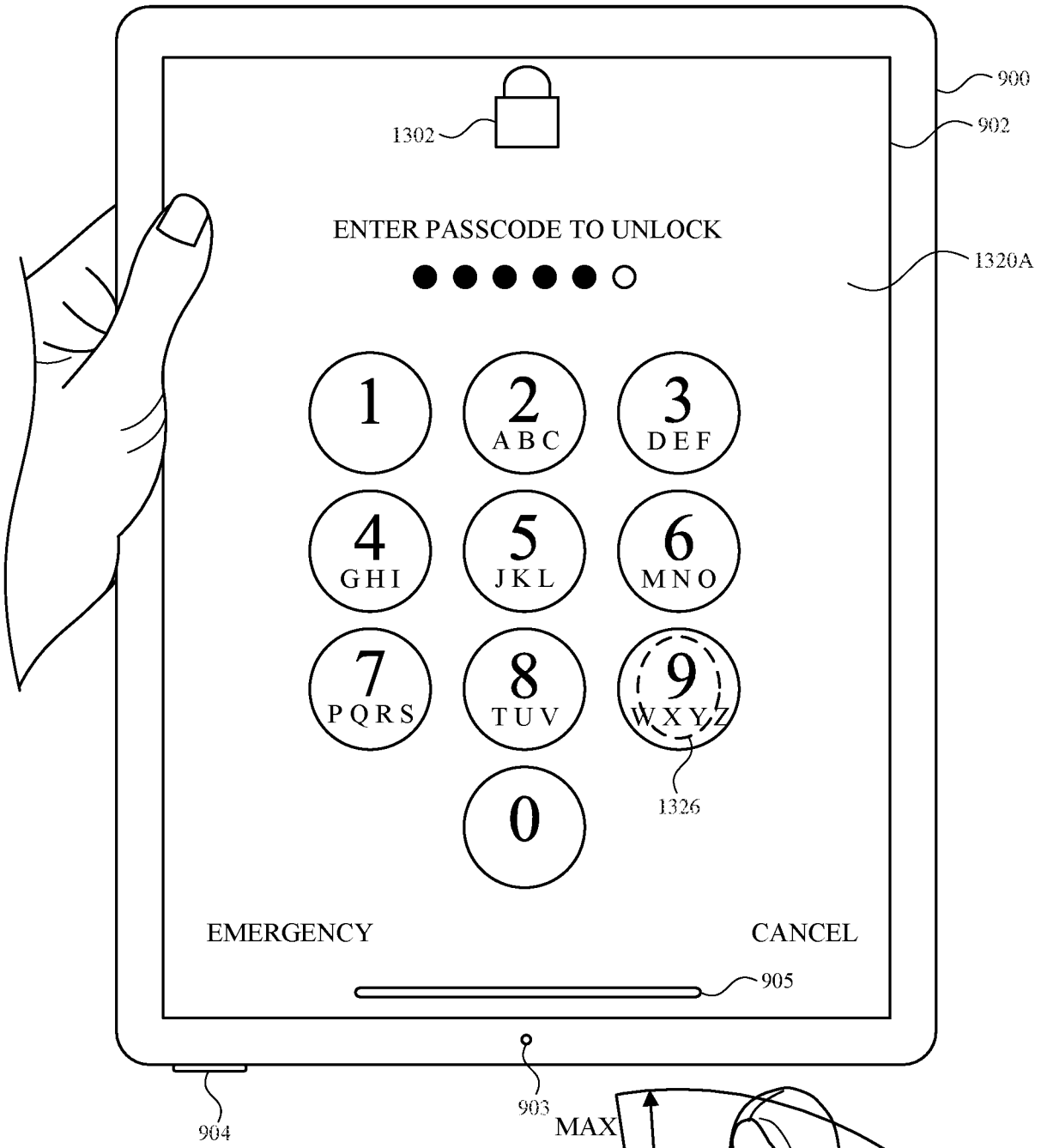


FIG. 13H

2022279466 30 Nov 2022



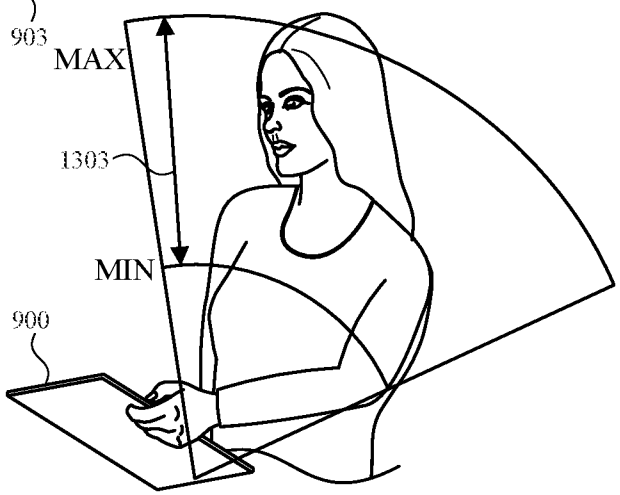


FIG. 131

2022279466 30 Nov 2022

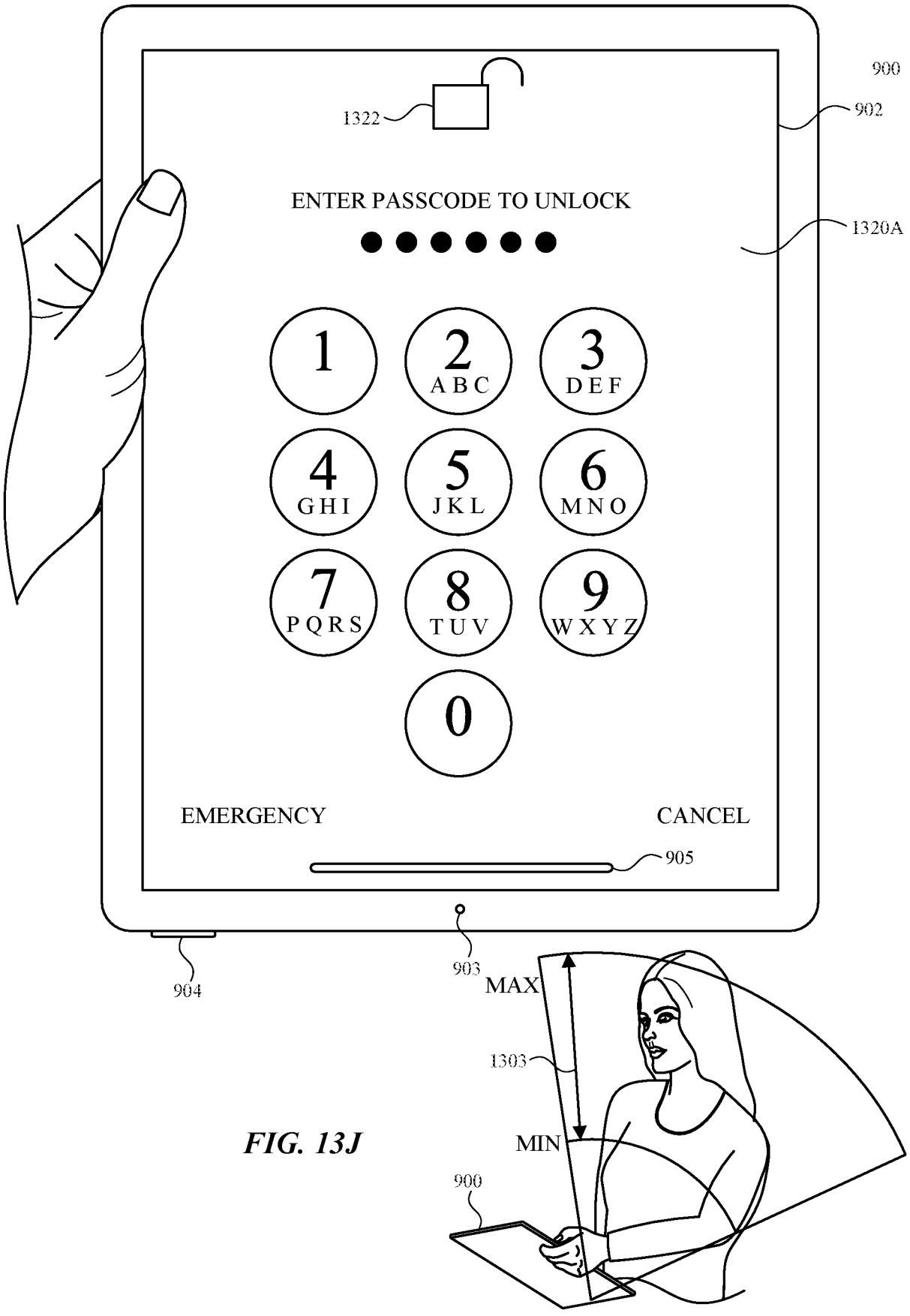


FIG. 13J

2022279466 30 Nov 2022

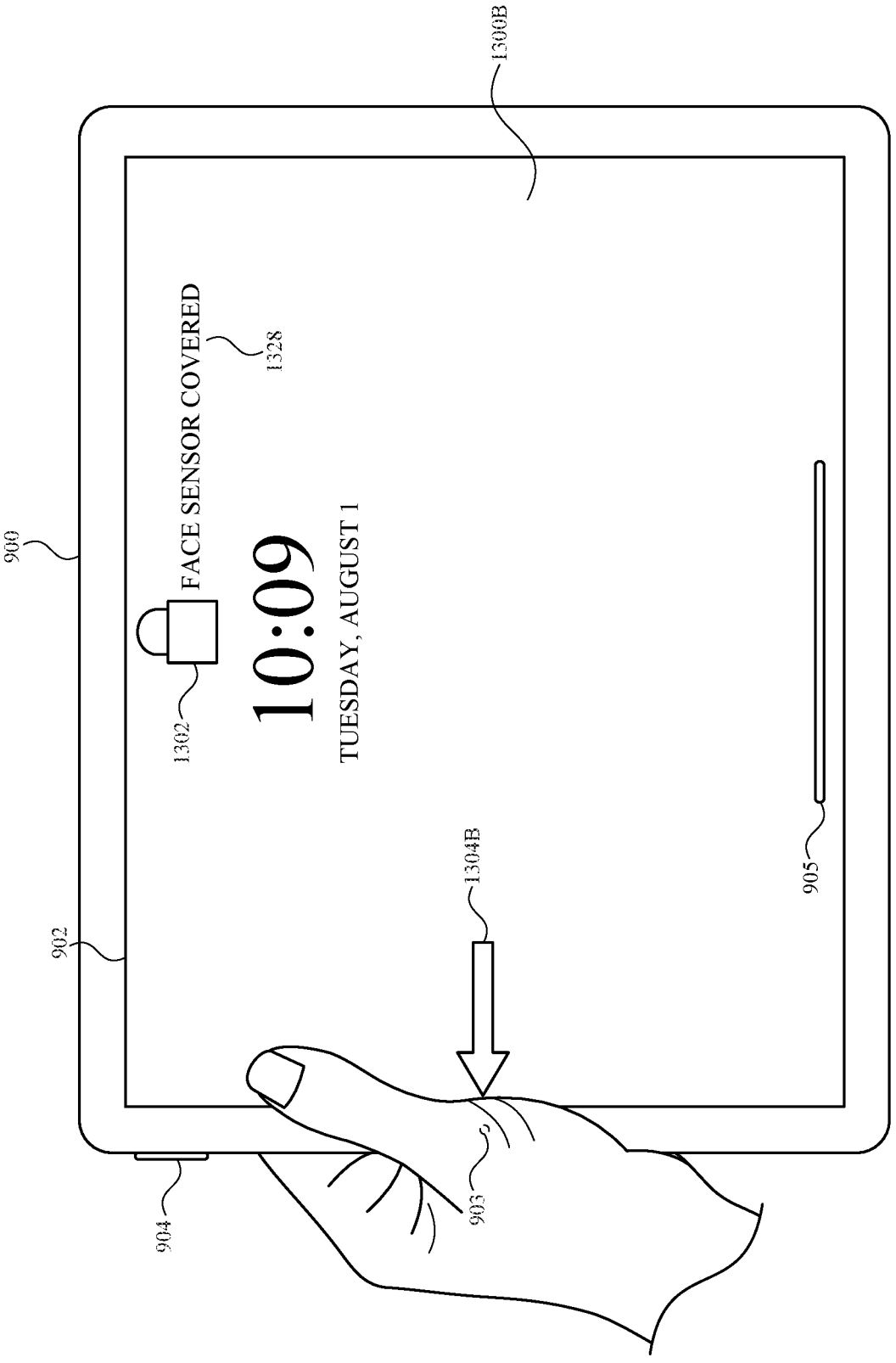


FIG. 13K

2022279466 30 Nov 2022

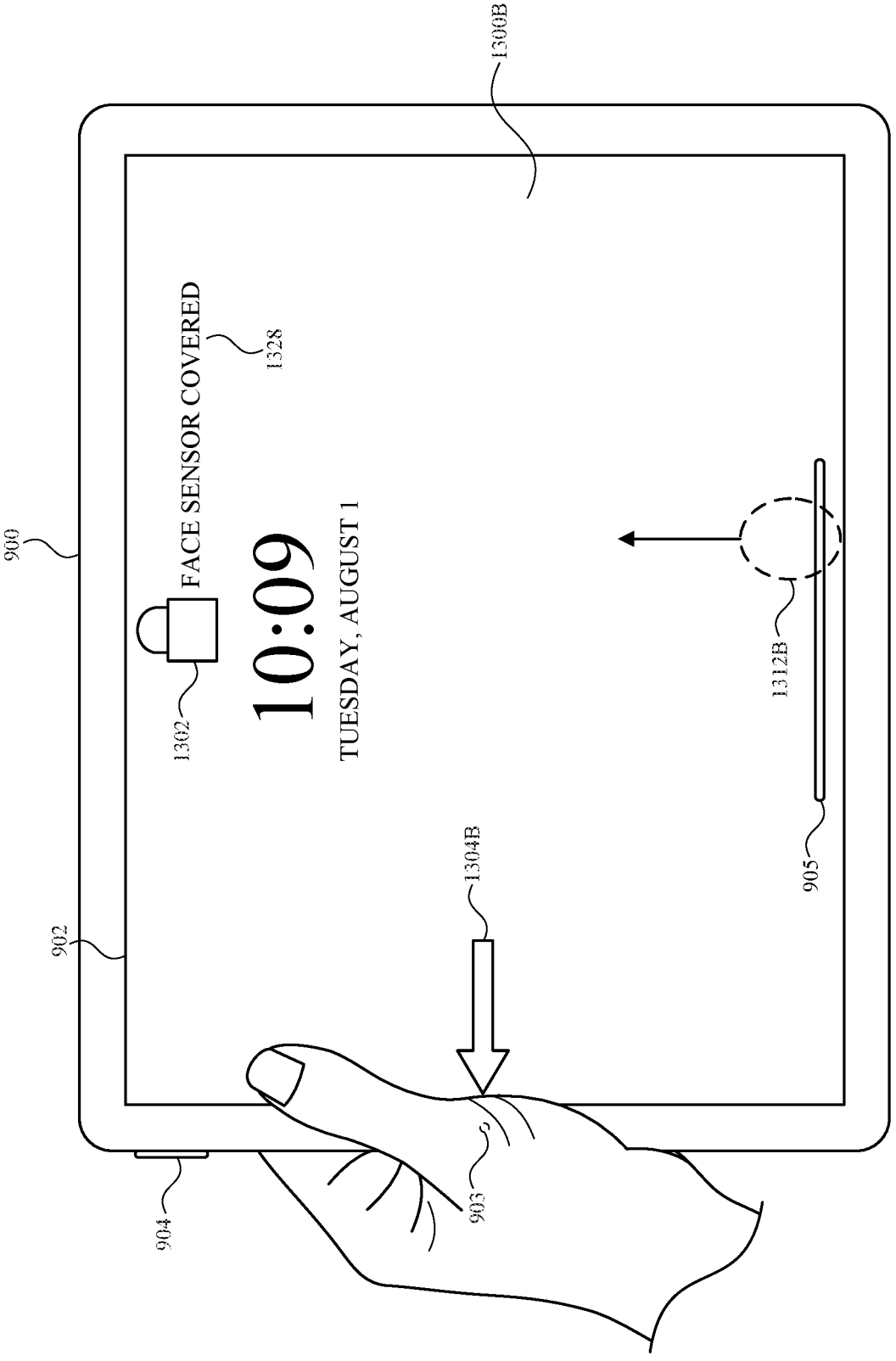


FIG. 13L

2022279466 30 Nov 2022

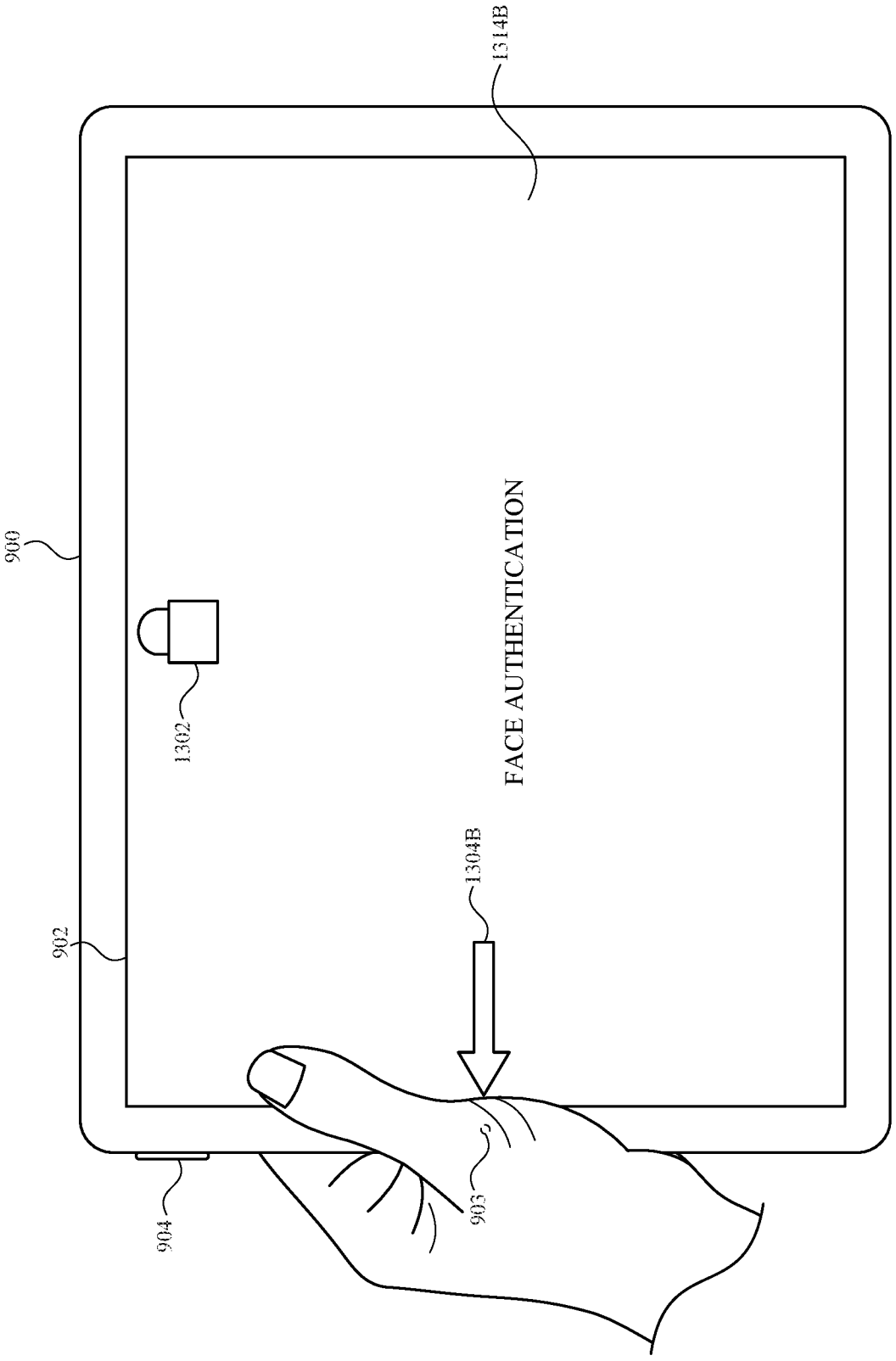


FIG. 13M

2022279466 30 Nov 2022

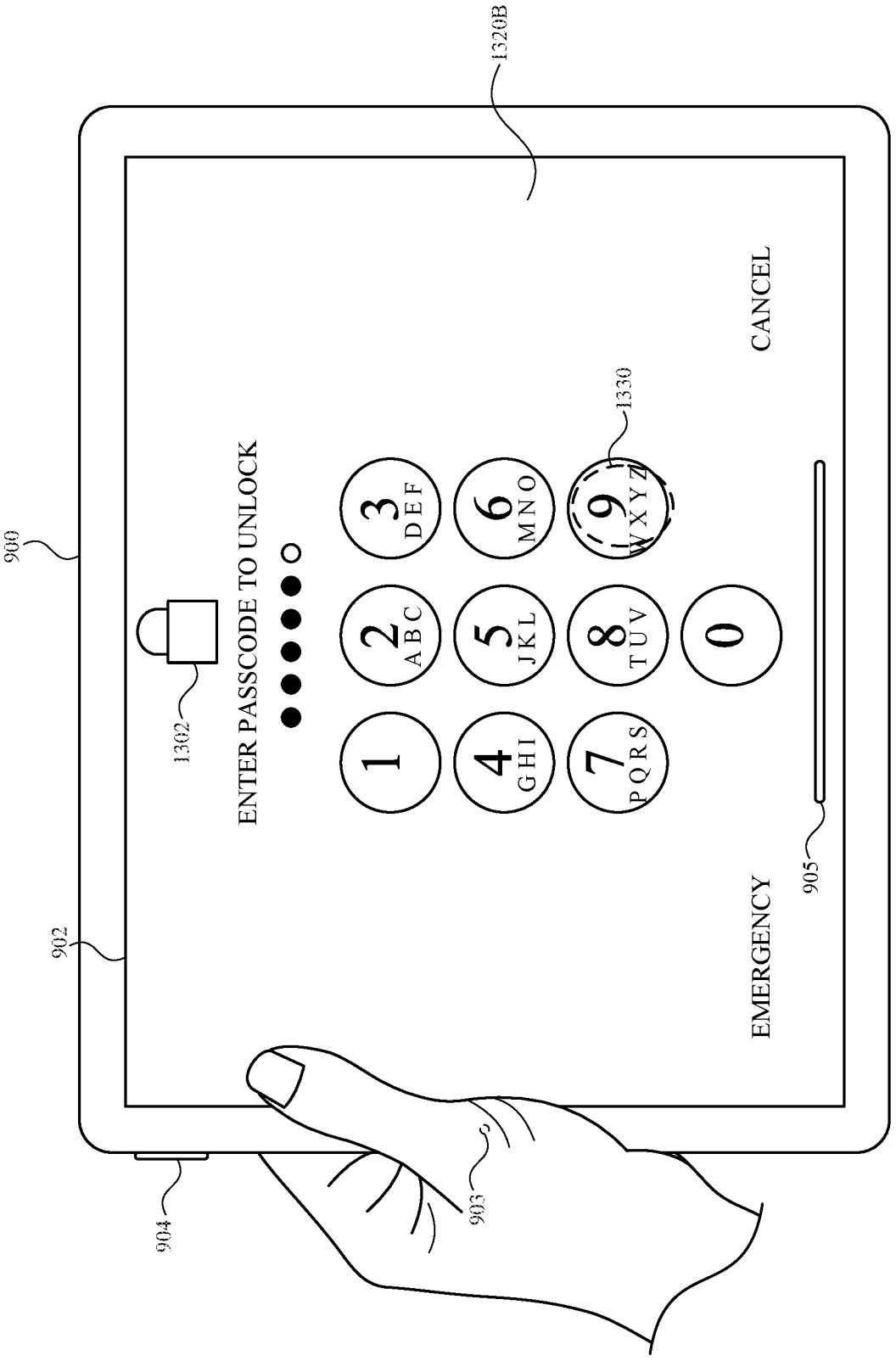


FIG. 13N

2022279466 30 Nov 2022

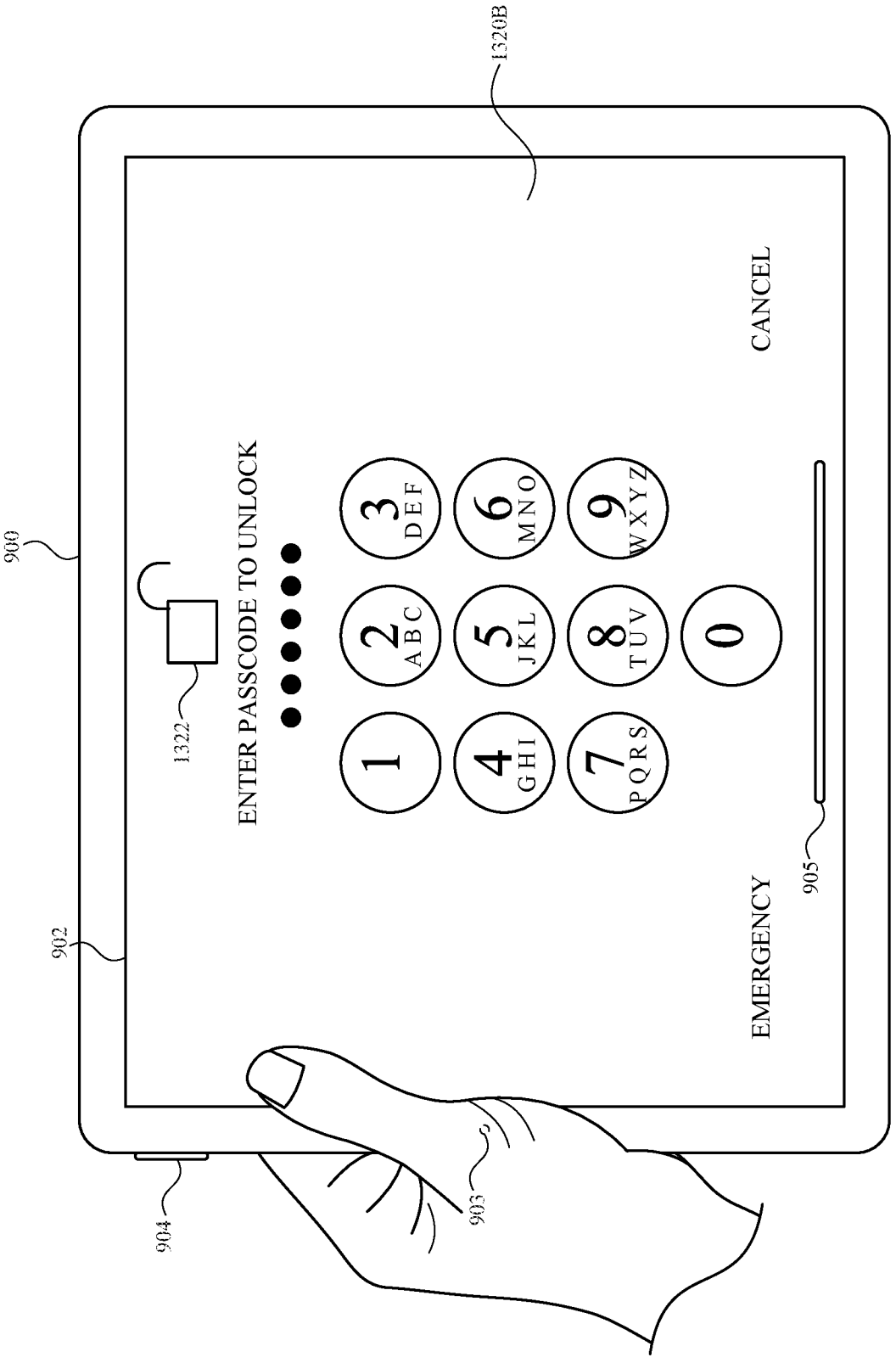


FIG. 13O

2022279466 30 Nov 2022

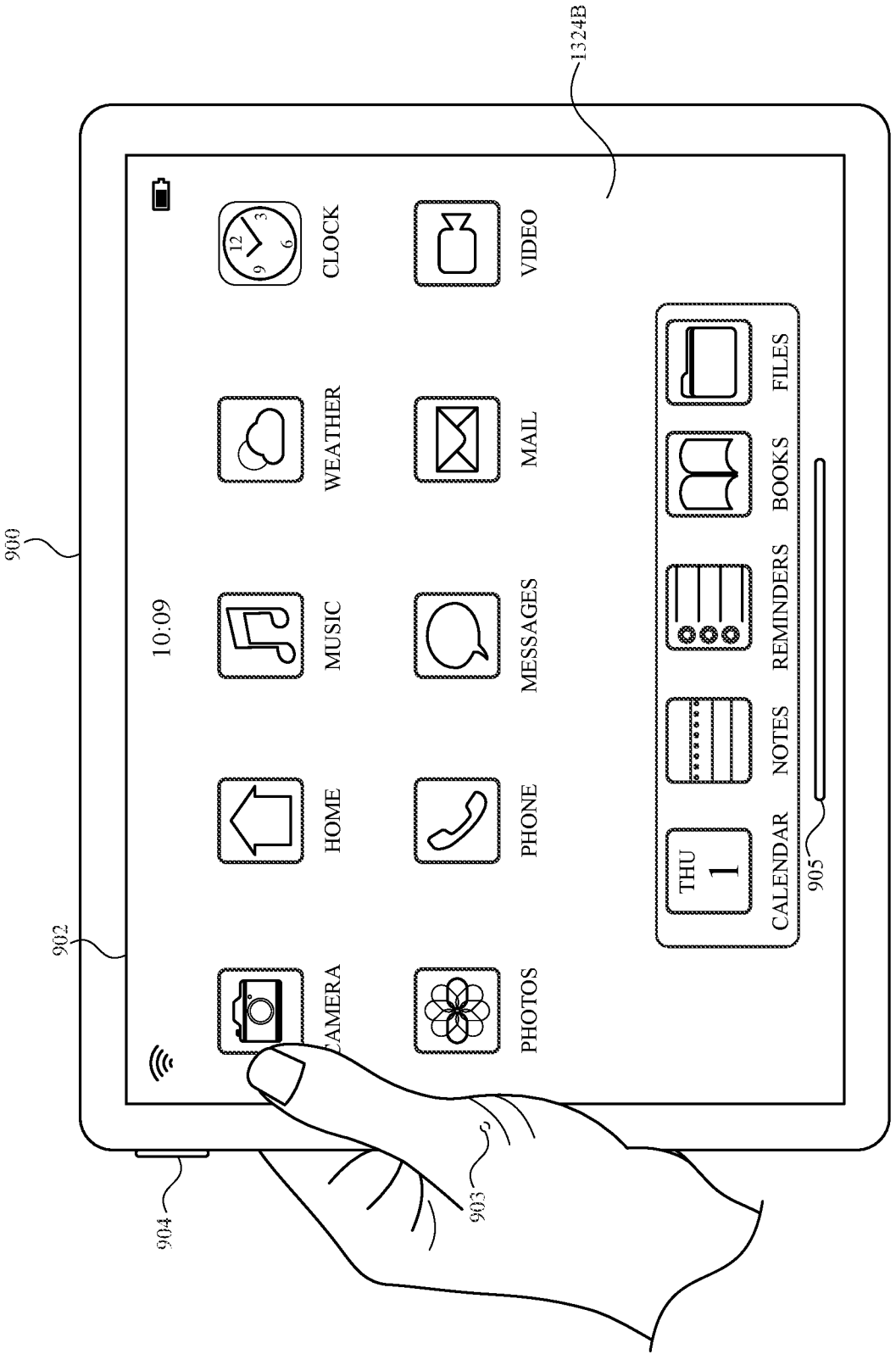
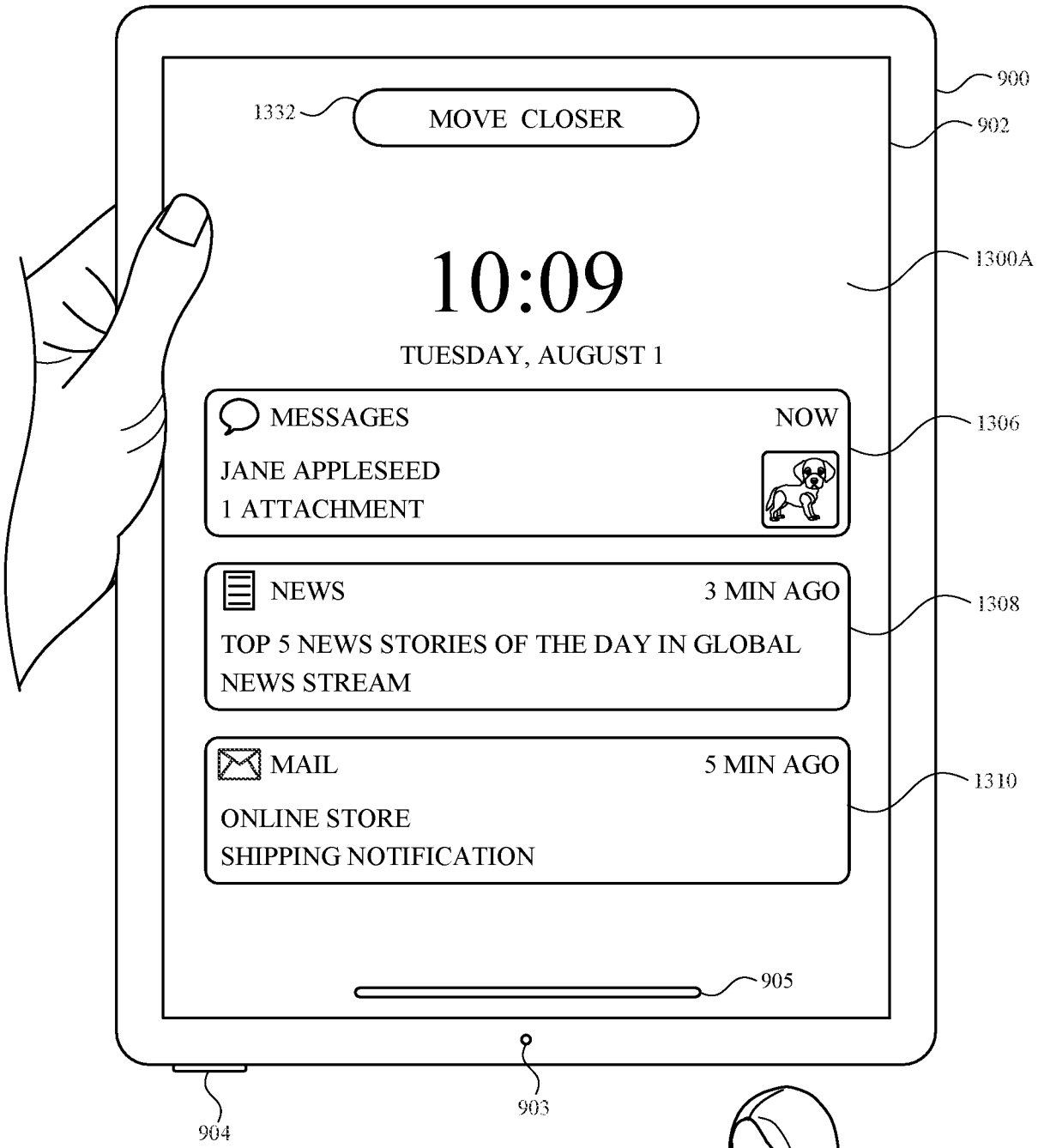


FIG. 13P

2022279466 30 Nov 2022



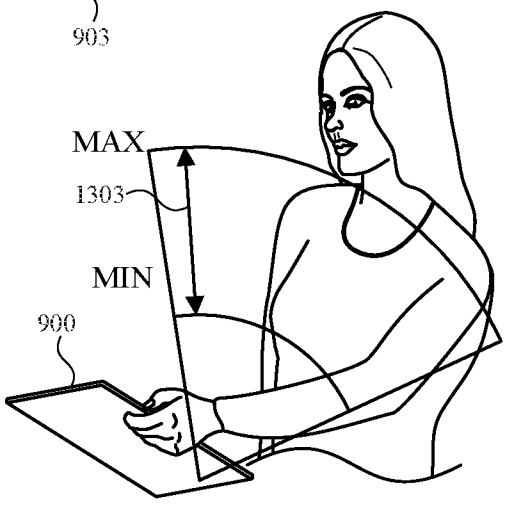


FIG. 13Q

20222794666 30 Nov 2022

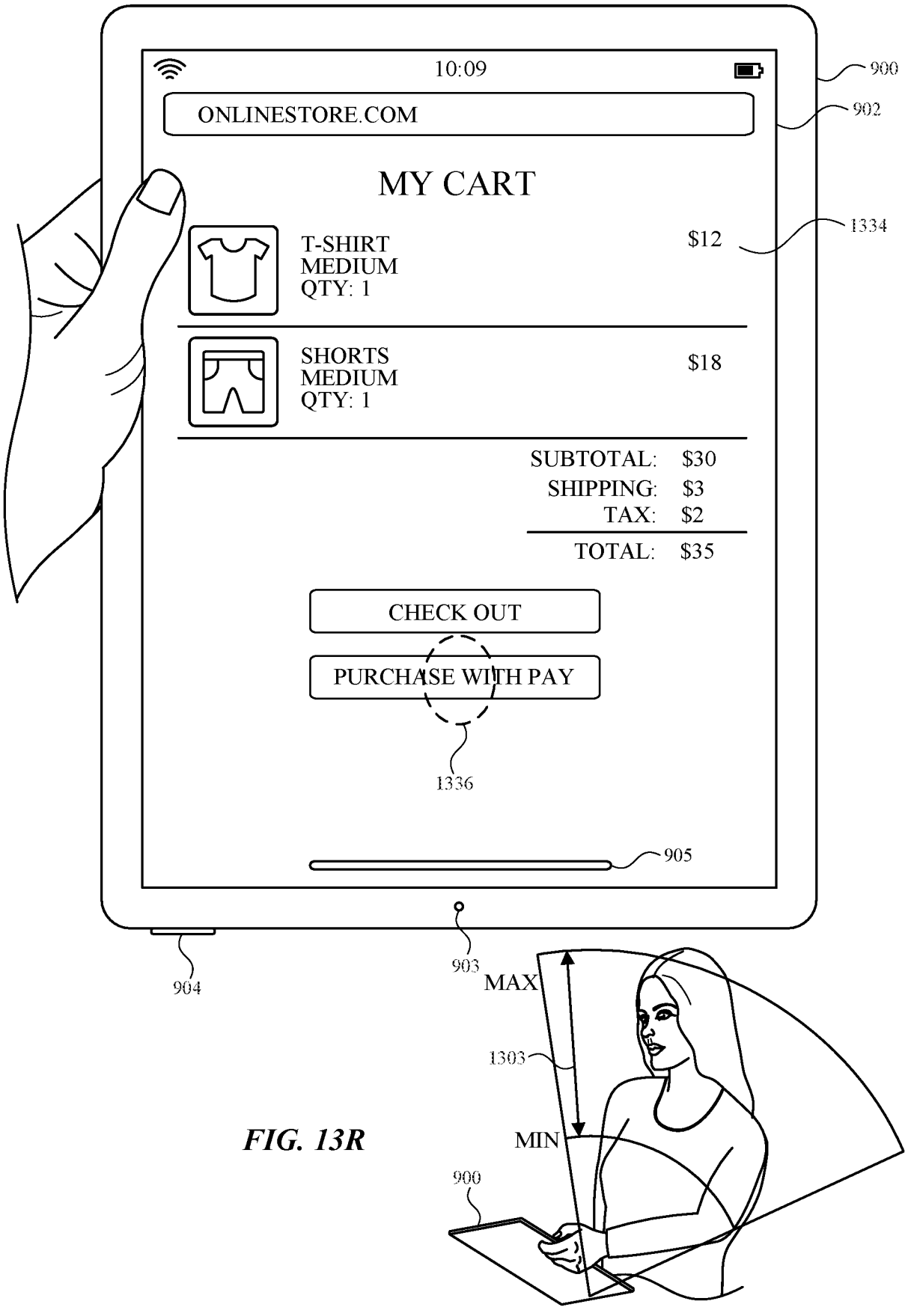


FIG. 13R

20222794666 30 Nov 2022

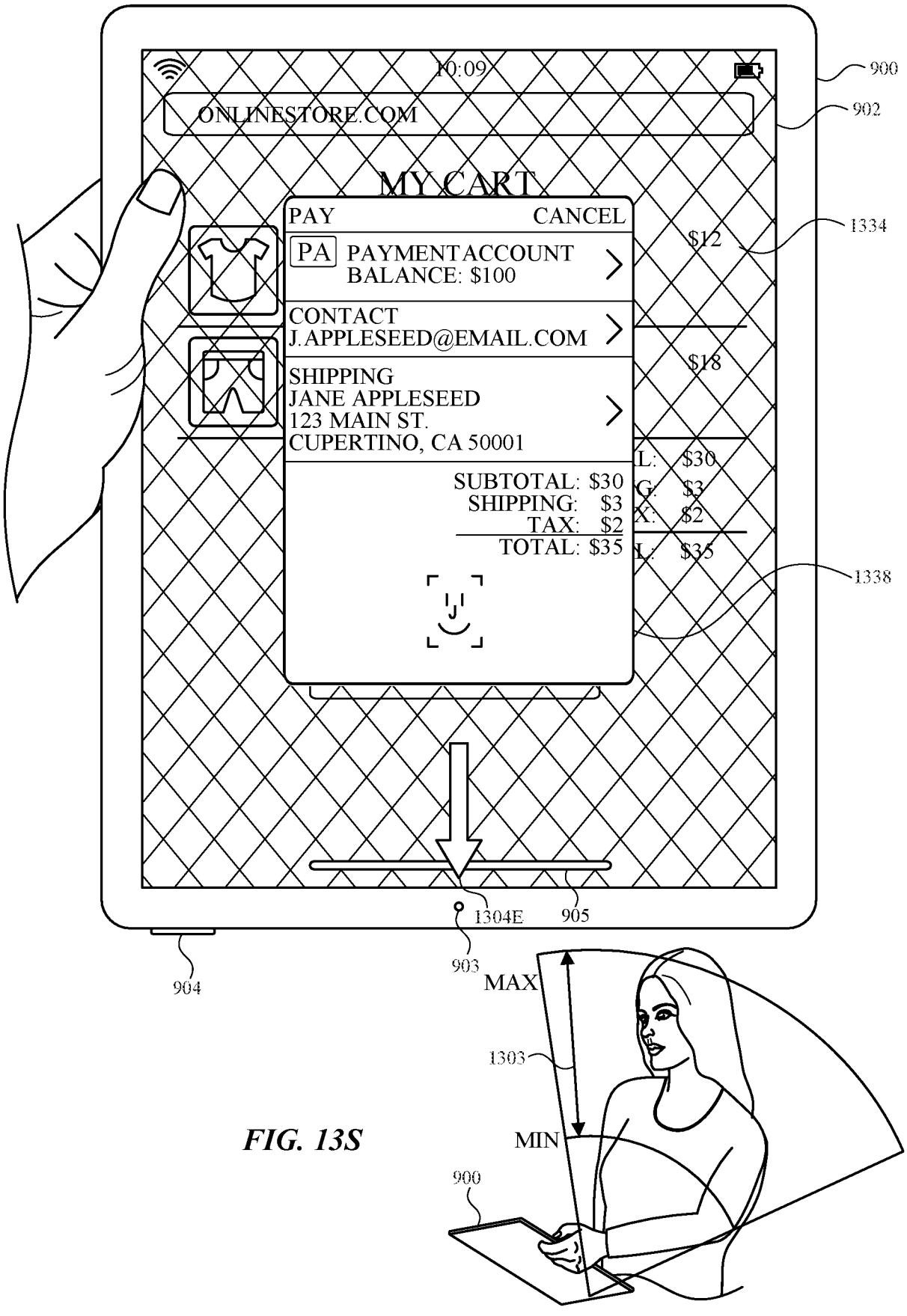


FIG. 13S

20222794666 30 Nov 2022

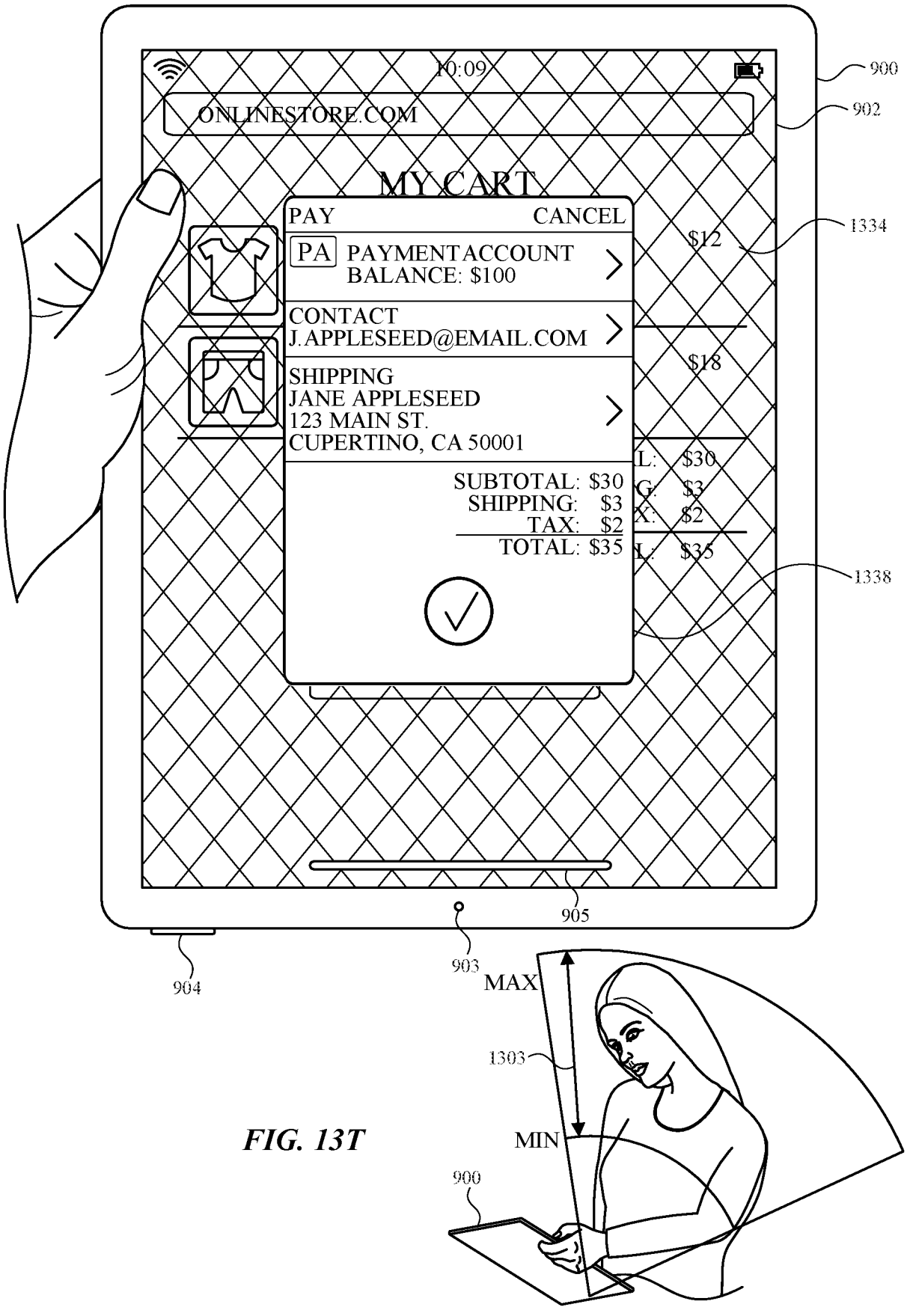


FIG. 13T

2022279466 30 Nov 2022

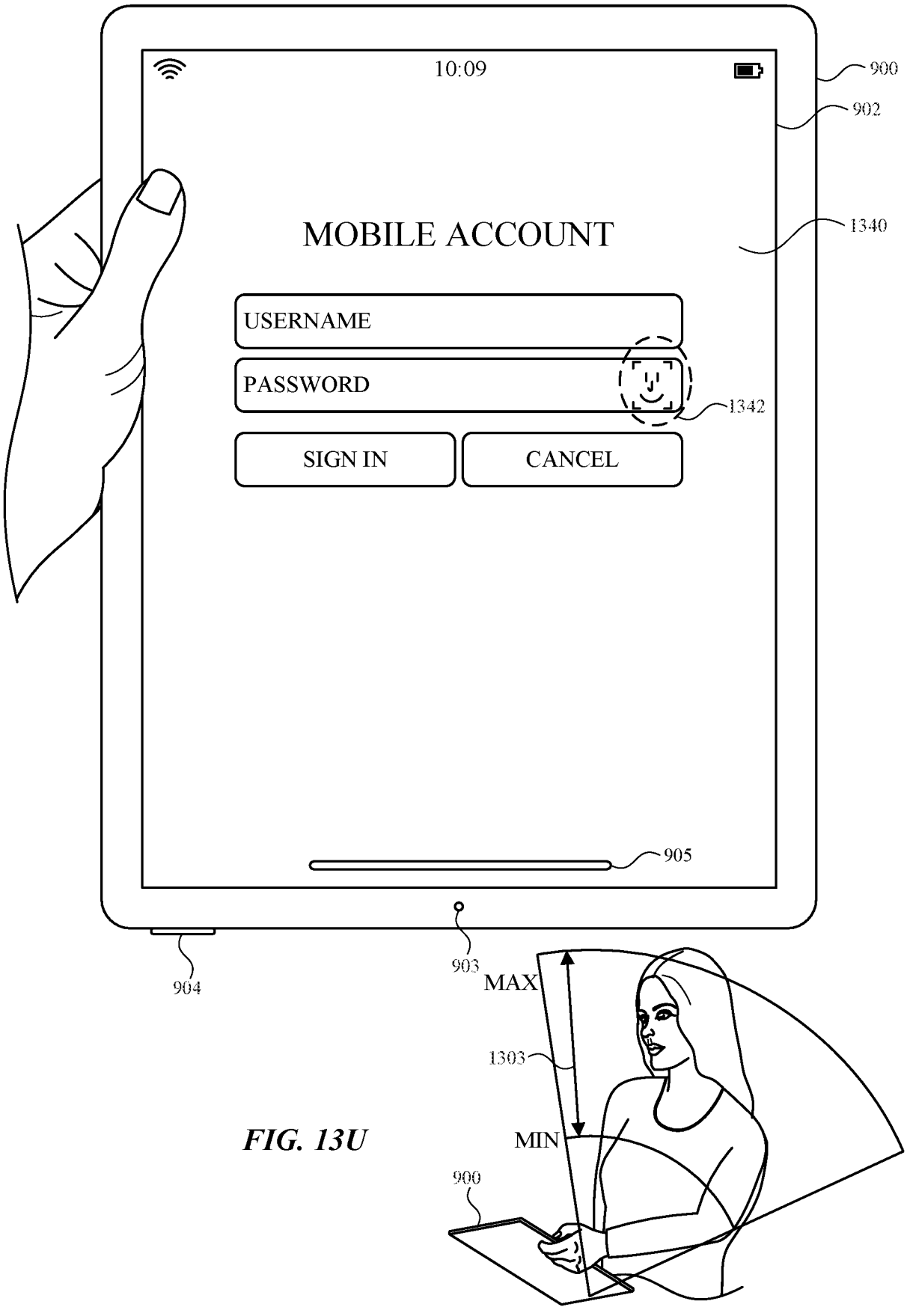


FIG. 13U

20222794666 30 Nov 2022

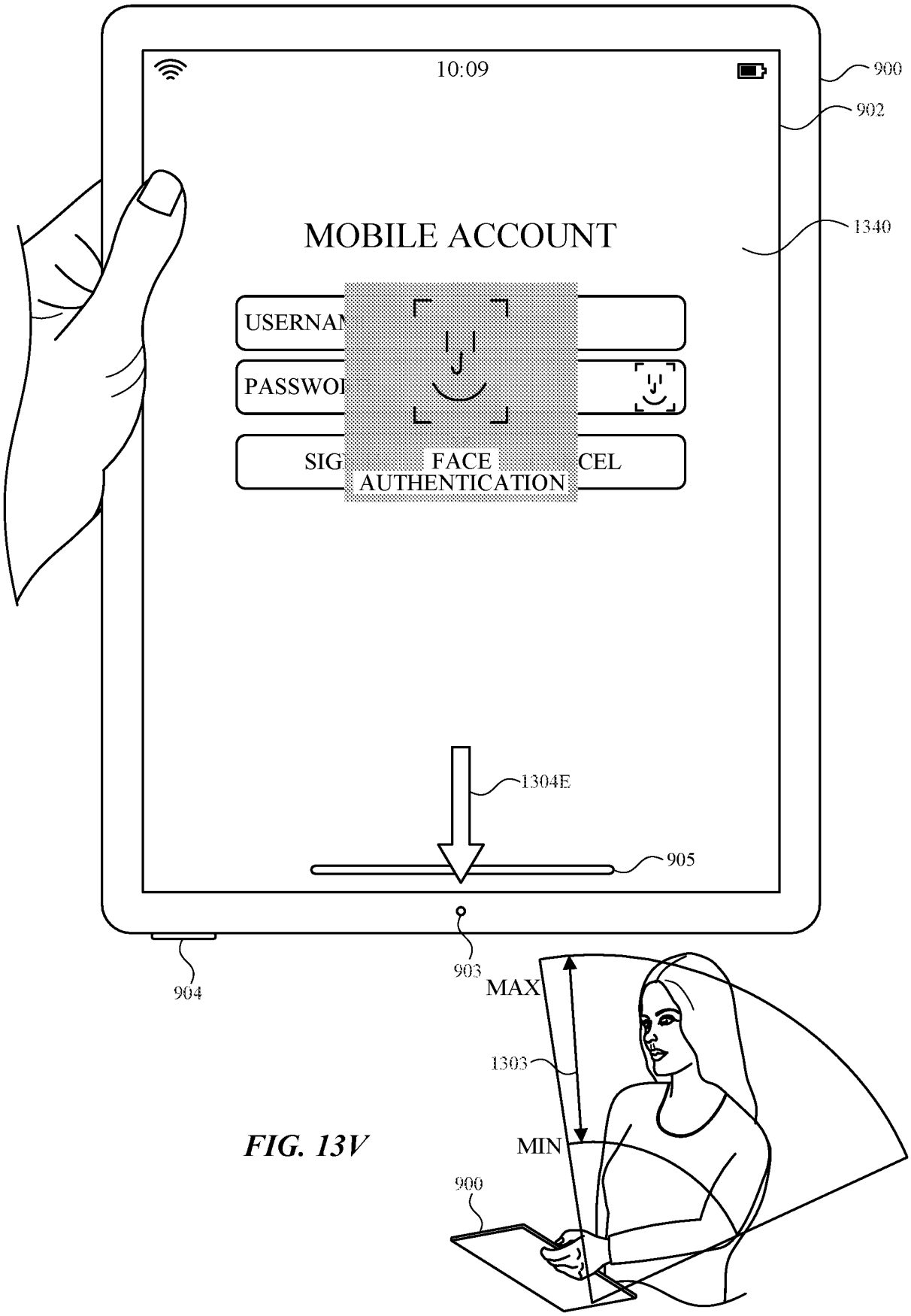


FIG. 13V

20222279466 30 Nov 2022

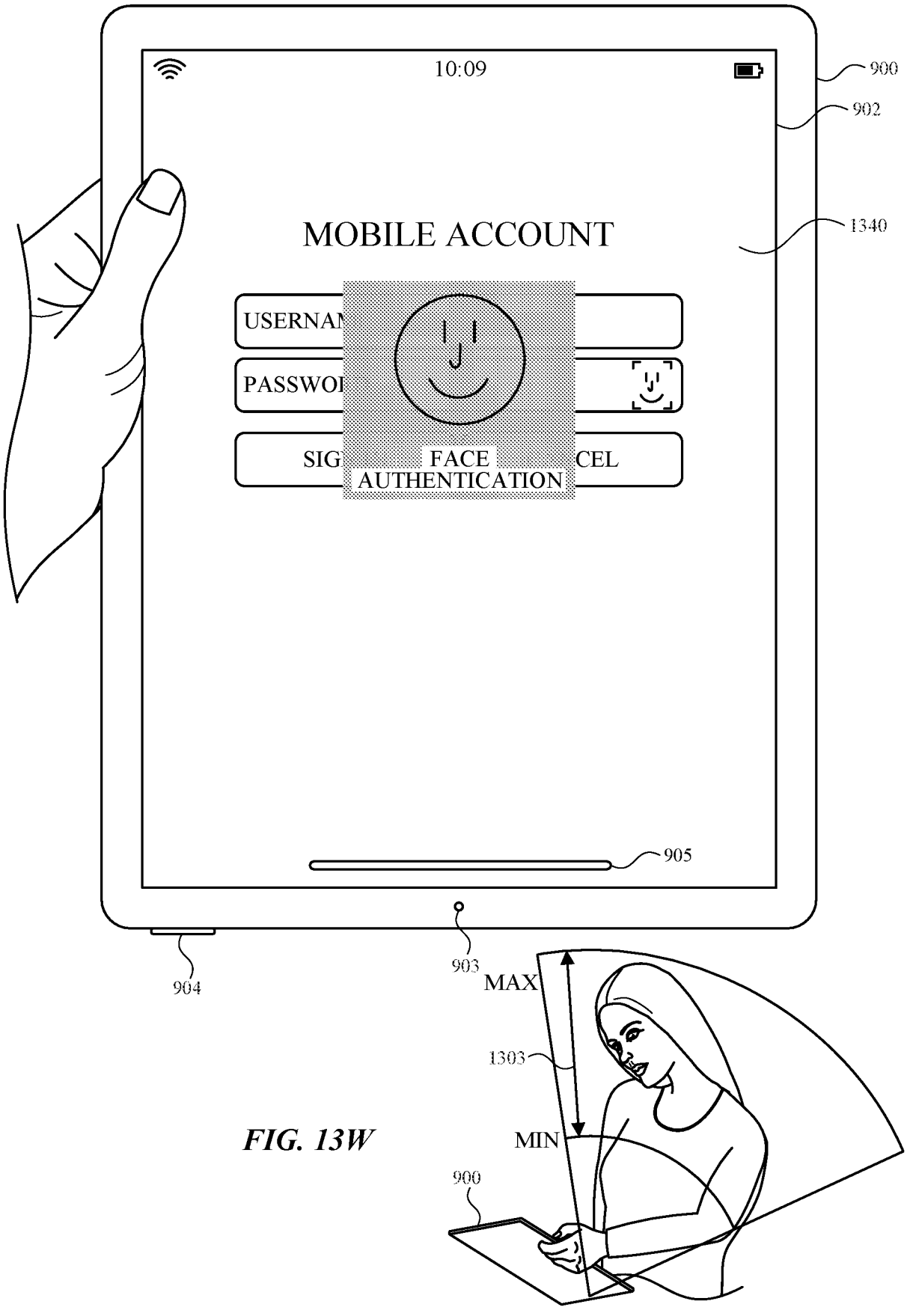


FIG. 13W

2022279466 30 Nov 2022

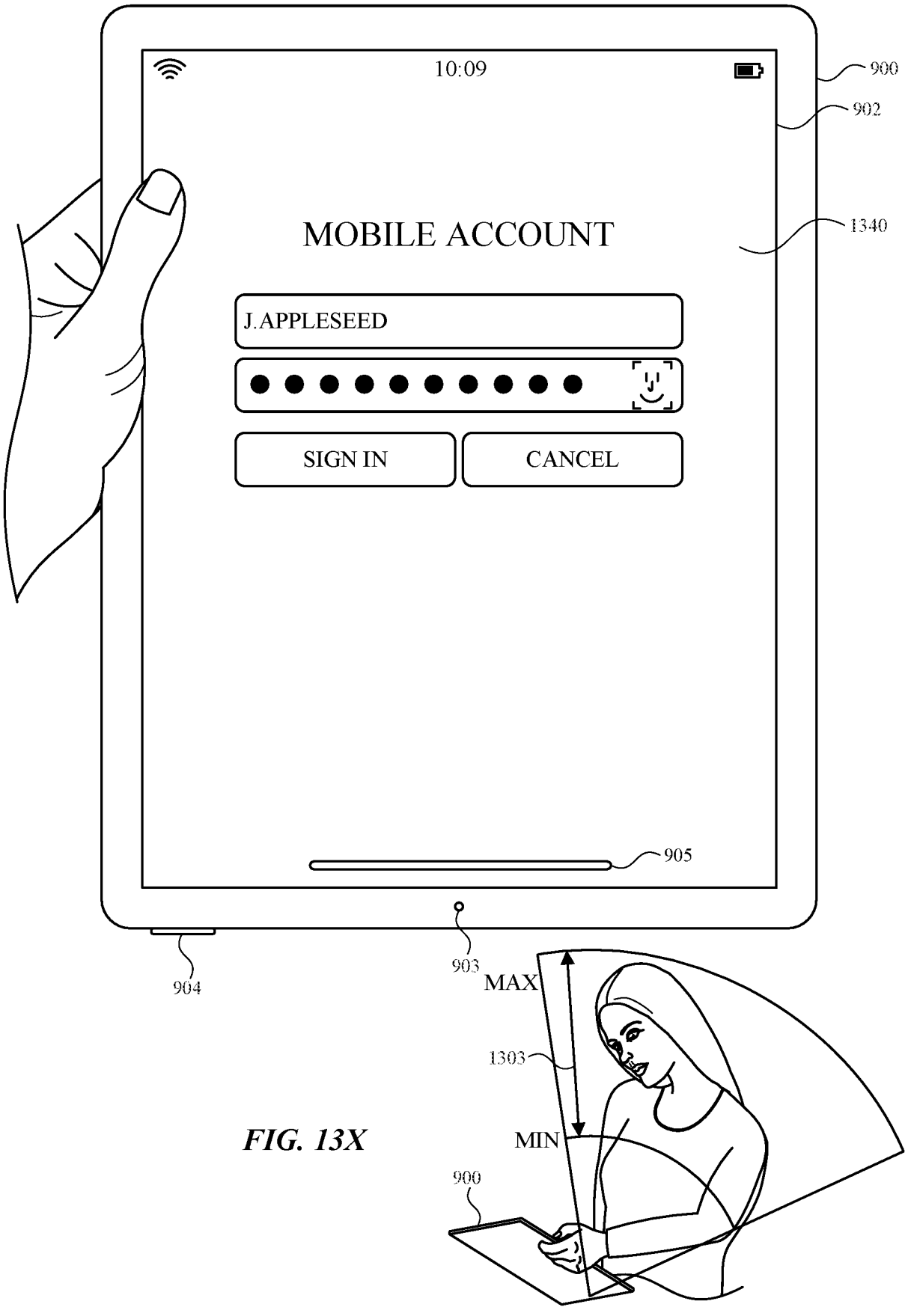


FIG. 13X

2022279466 30 Nov 2022

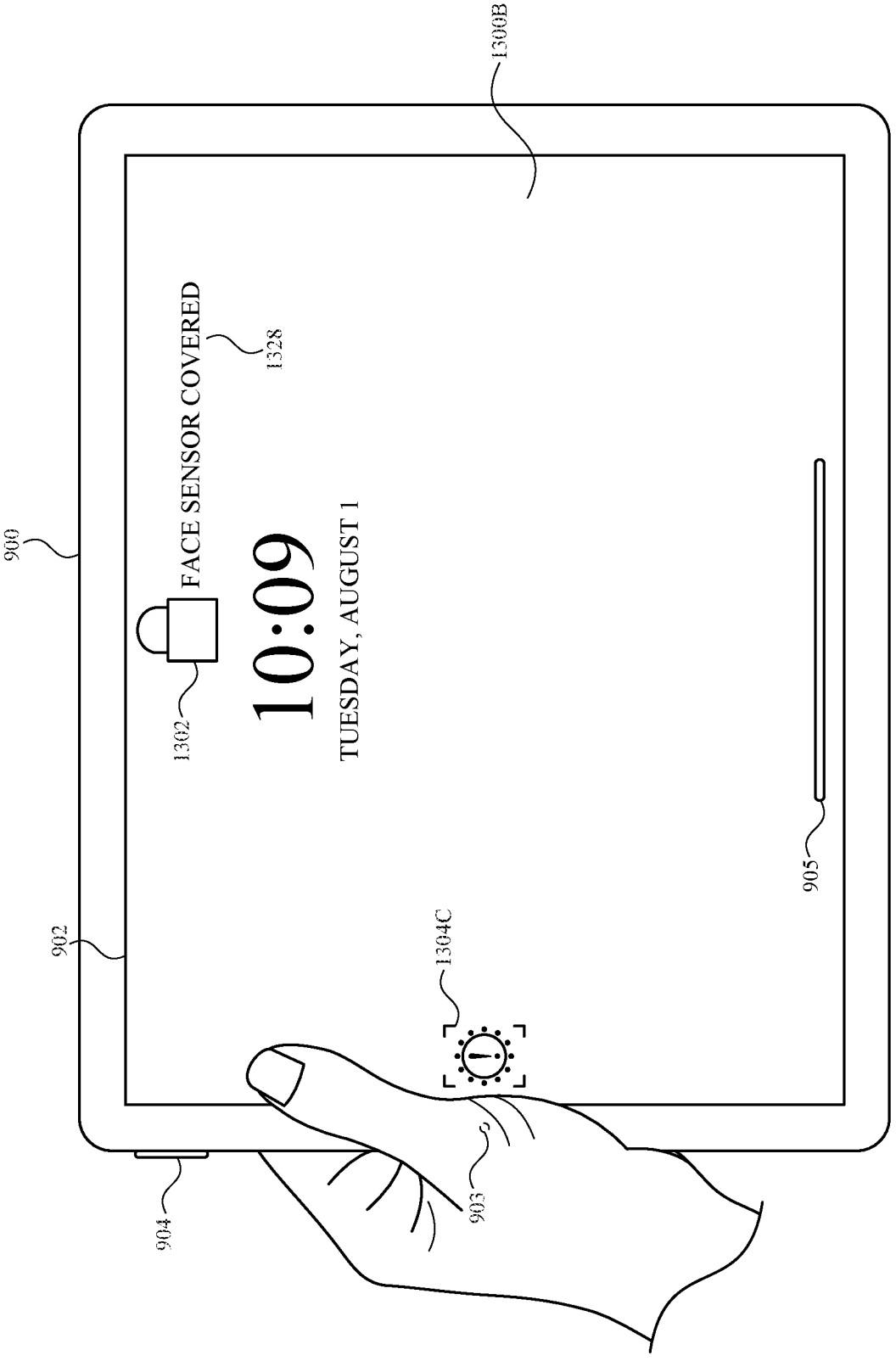


FIG. 13Y

2022279466 30 Nov 2022

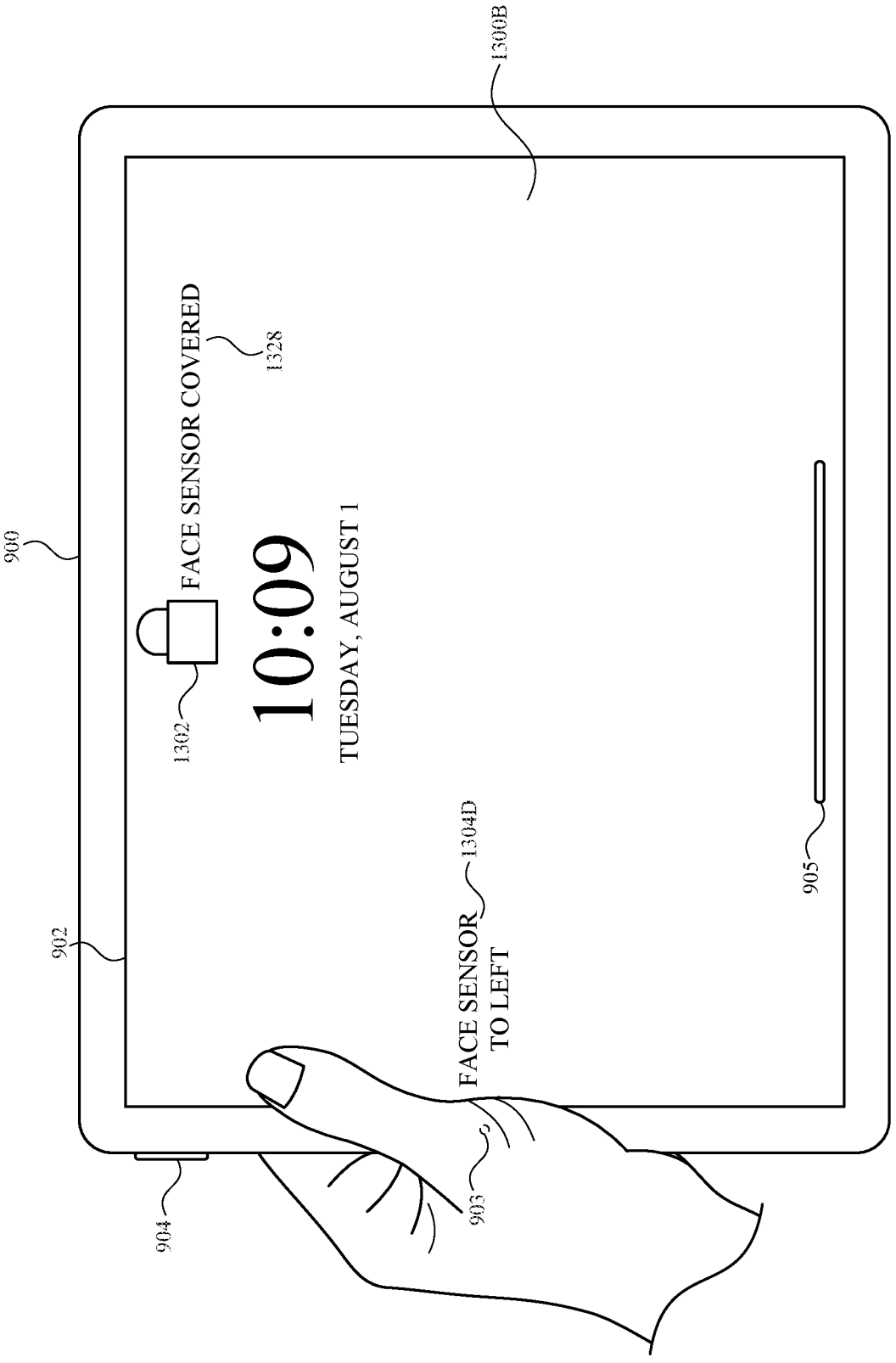


FIG. 13Z

2022279466 30 Nov 2022

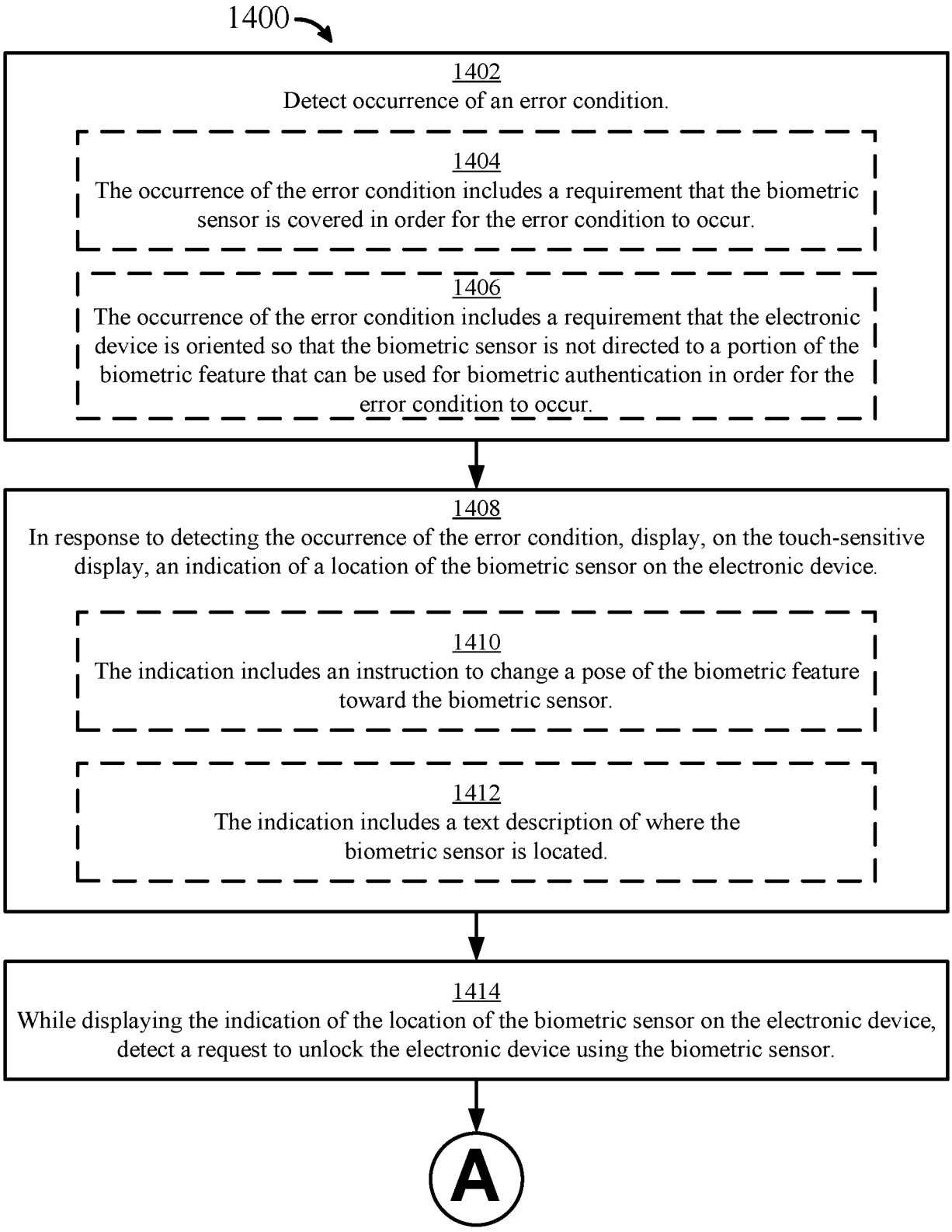


FIG. 14A

2022279466 30 Nov 2022

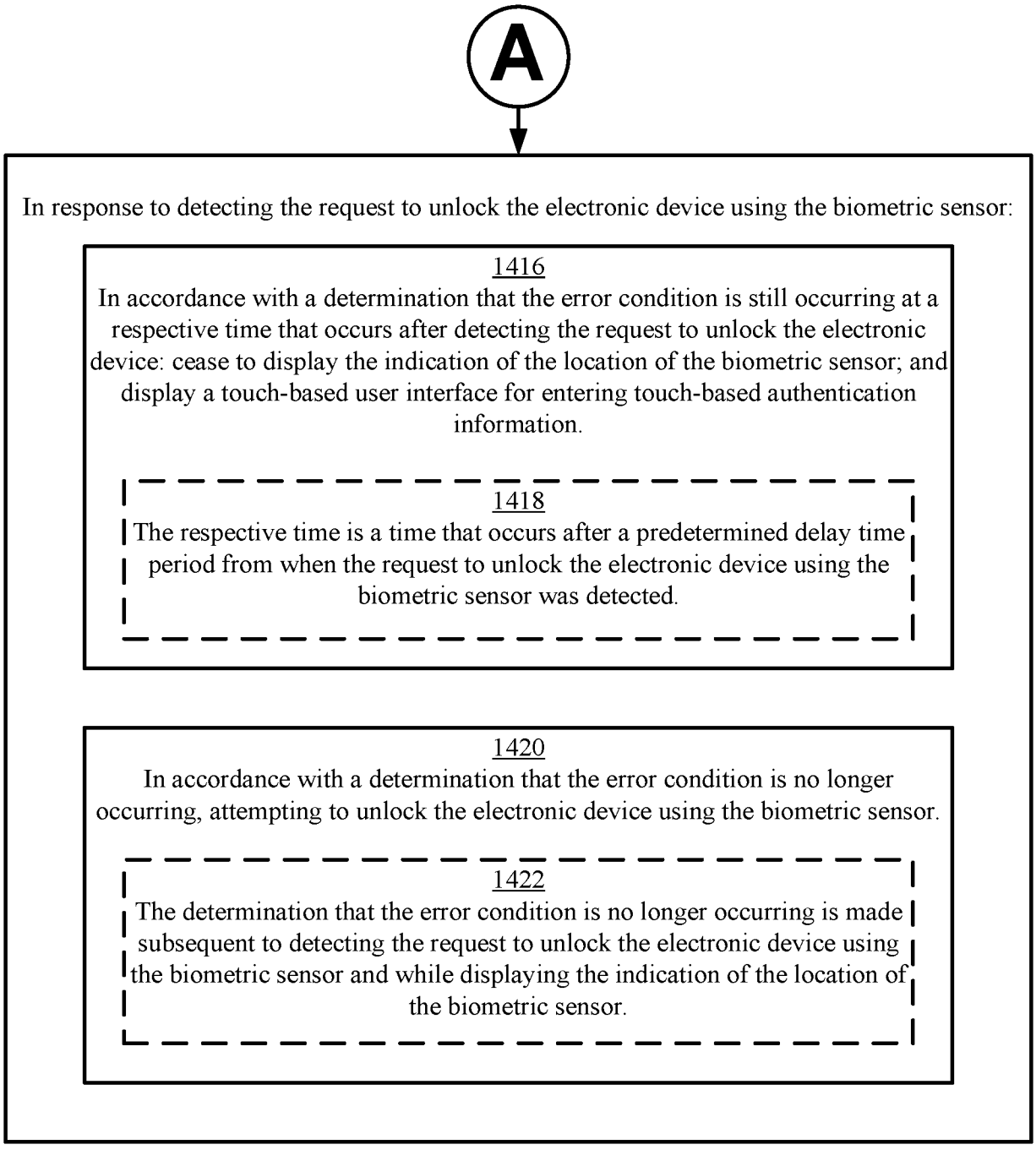


FIG. 14B