


# Exhibit I

**Claim Chart for U.S. Patent No. 9,665,705 (“the ’705 Patent”)**


The Accused Instrumentalities include, but are not necessarily limited to, Apple iPhone and Apple iPad compatible with Yale Smart Locks, and any Apple product or device that is substantially or reasonably similar to the functionality set forth below. The Accused Instrumentalities infringe the claims of the ’705 Patent, as described below, either directly under 35 U.S.C. § 271(a), or indirectly under 35 U.S.C. §§ 271(b)–(c). The Accused Instrumentalities infringe the claims of the ’705 Patent literally and, to the extent not literally, under the doctrine of equivalents.


<b><u>Claim 1</u></b>	<b><u>Accused Instrumentalities</u></b>
<p>I. A system for providing secure access to a controlled item, the system comprising:</p>	<p><i>To the extent that the preamble is deemed to be a limitation, the Accused Instrumentalities are configured to use a system in accordance with this claim.</i></p> <p>More specifically, the controlled item is a locking mechanism of the door lock of the user’s home. The Accused Instrumentalities are configured to provide secure access to the user’s home via Yale Smart Locks when the user provides biometric signal to the Accused Instrumentalities via Touch ID or Face ID.</p> <p>“When the “Secure Remote Access” feature is turned on, the app will use your phone’s built-in authentication tools to prompt fingerprint or facial recognition before you can unlock or lock your home remotely (note: if your phone does not have these features, it will prompt you to use your PIN code). This further ensures that your door is only operated by the right people at the time you intend for it.”  <a href="https://us.yalehome.com/en/yale-news/blog/latest-blog-posts/introducing-biometric-verification-for-august-and-yale-locks/">(https://us.yalehome.com/en/yale-news/blog/latest-blog-posts/introducing-biometric-verification-for-august-and-yale-locks/)</a></p>

<u>Claim 1</u>	<u>Accused Instrumentalities</u>
	 <p>The screenshot shows a mobile application interface for Yale. At the top, there is a yellow circular logo with the word "Yale" in black. To the left of the logo is a hamburger menu icon and the word "Open". To the right is a magnifying glass search icon. Below the navigation bar, the text "Introducing Biometric Verification for August and Yale Locks" is displayed in a bold, black font. Underneath the text is a photograph of a person's hand holding a smartphone. The phone's screen displays a biometric verification interface with a red circular camera overlay and a black square in the center containing a white face icon. Below the photograph, the URL <a href="https://us.yalehome.com/en/yale-news/blog/latest-blog-posts/introducing-biometric-verification-for-august-and-yale-locks1/">(https://us.yalehome.com/en/yale-news/blog/latest-blog-posts/introducing-biometric-verification-for-august-and-yale-locks1/)</a> is provided.</p>

<u>Claim 1</u>	<u>Accused Instrumentalities</u>
	 <p>(<a href="https://www.apple.com/shop/product/HPAR2ZM/A/yale-assure-lock-sl-touchscreen-deadbolt-black">https://www.apple.com/shop/product/HPAR2ZM/A/yale-assure-lock-sl-touchscreen-deadbolt-black</a>)</p>

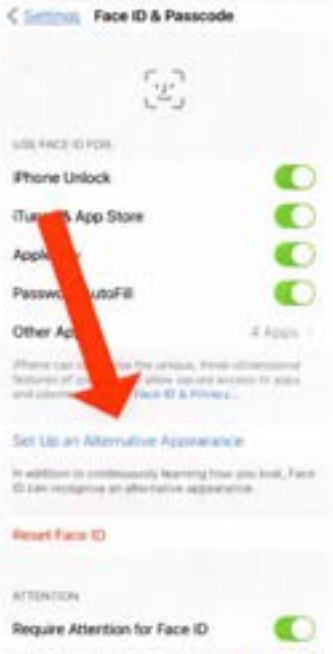
<b><u>Claim 1</u></b>	<b><u>Accused Instrumentalities</u></b>																																														
	<p>The Accused Instrumentalities compatible with Yale Smart Locks are shown below:</p> <p><b>Compatibility</b></p> <table border="0"> <thead> <tr> <th data-bbox="863 435 982 451">iPhone Models</th> <th data-bbox="1094 435 1192 451">iPad Models</th> </tr> </thead> <tbody> <tr><td data-bbox="863 459 982 475">iPhone 12 Pro</td><td data-bbox="1094 459 1234 505">iPad Pro 12.9-inch (5th generation)</td></tr> <tr><td data-bbox="863 488 1003 505">iPhone 12 Pro Max</td><td data-bbox="1094 513 1234 558">iPad Pro 12.9-inch (4th generation)</td></tr> <tr><td data-bbox="863 518 982 534">iPhone 12 mini</td><td data-bbox="1094 566 1234 612">iPad Pro 12.9-inch (3rd generation)</td></tr> <tr><td data-bbox="863 542 947 558">iPhone 12</td><td data-bbox="1094 620 1234 665">iPad Pro 12.9-inch (2nd generation)</td></tr> <tr><td data-bbox="863 574 982 591">iPhone 11 Pro</td><td data-bbox="1094 673 1234 719">iPad Pro 12.9-inch (1st generation)</td></tr> <tr><td data-bbox="863 607 1003 623">iPhone 11 Pro Max</td><td data-bbox="1094 727 1234 773">iPad Pro 11-inch (3rd generation)</td></tr> <tr><td data-bbox="863 639 947 656">iPhone 11</td><td data-bbox="1094 781 1234 826">iPad Pro 11-inch (2nd generation)</td></tr> <tr><td data-bbox="863 672 1073 688">iPhone SE (2nd generation)</td><td data-bbox="1094 834 1234 880">iPad Pro 11-inch (1st generation)</td></tr> <tr><td data-bbox="863 704 947 721">iPhone XS</td><td data-bbox="1094 888 1234 933">iPad Pro 11-inch (3rd generation)</td></tr> <tr><td data-bbox="863 737 982 753">iPhone XS Max</td><td data-bbox="1094 941 1234 987">iPad Pro 11-inch (2nd generation)</td></tr> <tr><td data-bbox="863 769 947 786">iPhone XR</td><td data-bbox="1094 995 1234 1040">iPad Pro 11-inch (1st generation)</td></tr> <tr><td data-bbox="863 802 947 818">iPhone X</td><td data-bbox="1094 1049 1234 1094">iPad Pro 10.5-inch</td></tr> <tr><td data-bbox="863 834 947 850">iPhone 8</td><td data-bbox="1094 1102 1234 1148">iPad Pro 9.7-inch</td></tr> <tr><td data-bbox="863 867 982 883">iPhone 8 Plus</td><td data-bbox="1094 1156 1276 1201">iPad Air (4th generation)</td></tr> <tr><td data-bbox="863 899 947 915">iPhone 7</td><td data-bbox="1094 1209 1276 1255">iPad Air (3rd generation)</td></tr> <tr><td data-bbox="863 932 982 948">iPhone 7 Plus</td><td data-bbox="1094 1263 1171 1279">iPad Air 2</td></tr> <tr><td data-bbox="863 964 947 980">iPhone 6s</td><td data-bbox="1094 1287 1255 1333">iPad (8th generation)</td></tr> <tr><td data-bbox="863 997 982 1013">iPhone 6s Plus</td><td data-bbox="1094 1341 1255 1386">iPad (7th generation)</td></tr> <tr><td data-bbox="863 1029 1066 1045">iPhone SE (1st generation)</td><td data-bbox="1094 1395 1255 1440">iPad (6th generation)</td></tr> <tr><td></td><td data-bbox="1094 1448 1255 1494">iPad (5th generation)</td></tr> <tr><td></td><td data-bbox="1094 1502 1283 1547">iPad mini (5th generation)</td></tr> <tr><td></td><td data-bbox="1094 1555 1178 1572">iPad mini 4</td></tr> </tbody> </table> <p><a href="https://www.apple.com/shop/product/HPAR2ZM/A/yale-assure-lock-sl-touchscreen-deadbolt-black">https://www.apple.com/shop/product/HPAR2ZM/A/yale-assure-lock-sl-touchscreen-deadbolt-black</a></p>	iPhone Models	iPad Models	iPhone 12 Pro	iPad Pro 12.9-inch (5th generation)	iPhone 12 Pro Max	iPad Pro 12.9-inch (4th generation)	iPhone 12 mini	iPad Pro 12.9-inch (3rd generation)	iPhone 12	iPad Pro 12.9-inch (2nd generation)	iPhone 11 Pro	iPad Pro 12.9-inch (1st generation)	iPhone 11 Pro Max	iPad Pro 11-inch (3rd generation)	iPhone 11	iPad Pro 11-inch (2nd generation)	iPhone SE (2nd generation)	iPad Pro 11-inch (1st generation)	iPhone XS	iPad Pro 11-inch (3rd generation)	iPhone XS Max	iPad Pro 11-inch (2nd generation)	iPhone XR	iPad Pro 11-inch (1st generation)	iPhone X	iPad Pro 10.5-inch	iPhone 8	iPad Pro 9.7-inch	iPhone 8 Plus	iPad Air (4th generation)	iPhone 7	iPad Air (3rd generation)	iPhone 7 Plus	iPad Air 2	iPhone 6s	iPad (8th generation)	iPhone 6s Plus	iPad (7th generation)	iPhone SE (1st generation)	iPad (6th generation)		iPad (5th generation)		iPad mini (5th generation)		iPad mini 4
iPhone Models	iPad Models																																														
iPhone 12 Pro	iPad Pro 12.9-inch (5th generation)																																														
iPhone 12 Pro Max	iPad Pro 12.9-inch (4th generation)																																														
iPhone 12 mini	iPad Pro 12.9-inch (3rd generation)																																														
iPhone 12	iPad Pro 12.9-inch (2nd generation)																																														
iPhone 11 Pro	iPad Pro 12.9-inch (1st generation)																																														
iPhone 11 Pro Max	iPad Pro 11-inch (3rd generation)																																														
iPhone 11	iPad Pro 11-inch (2nd generation)																																														
iPhone SE (2nd generation)	iPad Pro 11-inch (1st generation)																																														
iPhone XS	iPad Pro 11-inch (3rd generation)																																														
iPhone XS Max	iPad Pro 11-inch (2nd generation)																																														
iPhone XR	iPad Pro 11-inch (1st generation)																																														
iPhone X	iPad Pro 10.5-inch																																														
iPhone 8	iPad Pro 9.7-inch																																														
iPhone 8 Plus	iPad Air (4th generation)																																														
iPhone 7	iPad Air (3rd generation)																																														
iPhone 7 Plus	iPad Air 2																																														
iPhone 6s	iPad (8th generation)																																														
iPhone 6s Plus	iPad (7th generation)																																														
iPhone SE (1st generation)	iPad (6th generation)																																														
	iPad (5th generation)																																														
	iPad mini (5th generation)																																														
	iPad mini 4																																														
<p>1a. a memory comprising a database of biometric signatures;</p>	<p><b><i>The Accused Instrumentalities include a memory comprising a database of biometric signatures.</i></b></p>																																														

<u>Claim 1</u>	<u>Accused Instrumentalities</u>
	<p>More specifically, the iPhone allows multiple biometric signatures to be entered into a database on the iPhone:</p> <p><b>Touch ID</b></p> <p>The iPhone allows the registration of multiple fingerprints:</p>  <p>Fig. from <a href="https://support.apple.com/en-us/HT201371">https://support.apple.com/en-us/HT201371</a> under Manage Touch ID Settings. In the second bullet, it literally says:</p> <p>"Register up to five fingerprints."</p> <p>"Touch ID can read multiple fingerprints, and it can read fingerprints in 360-degrees of orientation. It then creates a mathematical representation of your fingerprint and compares this to your enrolled fingerprint data to identify a match and unlock your device. "</p>

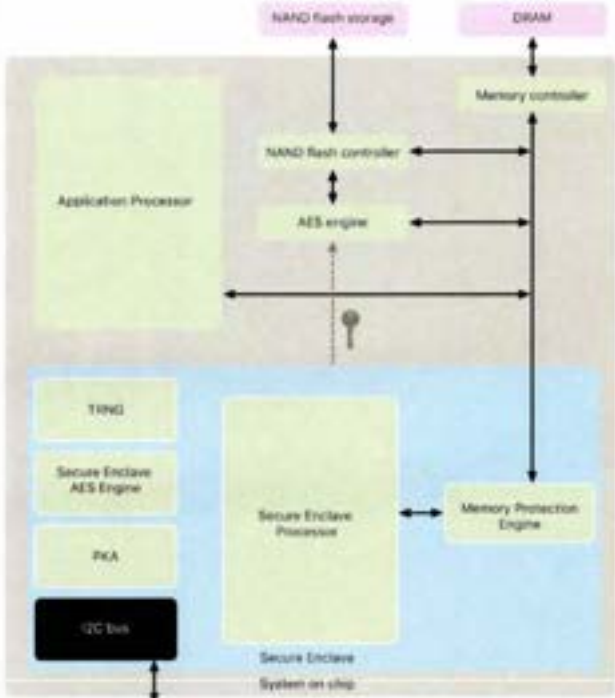
<u>Claim 1</u>	<u>Accused Instrumentalities</u>
	<p>(<a href="https://support.apple.com/en-us/HT204587">https://support.apple.com/en-us/HT204587</a>)</p> <p>"Touch ID can read multiple fingerprints and recognize fingerprints at any orientation of the finger. The system then creates a mathematical representation of your fingerprint and compares it to the registered fingerprint data to determine a match and unlock your device."                      (<a href="https://support.apple.com/en-us/HT204587">https://support.apple.com/en-us/HT204587</a>)</p> <p><b>Face ID</b></p> <p>The iPhone allows the registration of multiple faces:</p>  <p>To register a face, the iPhone takes a series of pictures of the user in different poses while circling his head. This is revealed in detail in <a href="https://support.apple.com/en-us/HT208109">https://support.apple.com/en-us/HT208109</a> in the second section "Configure Face ID", there also the figure shown above.</p>

<u>Claim 1</u>	<u>Accused Instrumentalities</u>
	<p>To register a second face, the iPhone offers a corresponding option in its settings. If the user selects the option "Set up an alternative appearance" as shown in the figure below (from How To Add A Second Face To Face ID - Macworld UK; <a href="https://www.macworld.co.uk/how-to/second-face-id-3803421/">https://www.macworld.co.uk/how-to/second-face-id-3803421/</a>), a second face is registered by the iPhone in the same way as the first face.</p> <p>"Set up Face ID or add another face.</p> <ul style="list-style-type: none"> <li>• Select "Settings" &gt; "Face ID &amp; Code" &gt; "Configure alternate appearance" if you want to configure another face to be recognized by Face ID."</li> </ul> <p>(<a href="https://support.apple.com/de-de/guide/iphone/iph6d162927a/ios">https://support.apple.com/de-de/guide/iphone/iph6d162927a/ios</a>)</p>



<u>Claim 1</u>	<u>Accused Instrumentalities</u>
	 <p>The page <a href="https://www.macworld.co.uk/how-to/second-face-id-3803421/">How To Add A Second Face To Face ID - Macworld UK</a> (<a href="https://www.macworld.co.uk/how-to/second-face-id-3803421/">https://www.macworld.co.uk/how-to/second-face-id-3803421/</a>) literally states:</p> <p>"Face ID is a fast and secure way to unlock your iPhone or iPad Pro, but you may not know that you can actually set up more than one face to use the feature.</p> <p>This second face could belong to a loved one, enabling your partner or child to access your phone without requiring your smiling mug to unlock it."</p> <p>To store the biometric signatures ("template data") from the received biometric signals, the iPhone has a System on Chip (SOC) called a Secure Enclave. A Secure Enclave Processor provides the Secure Enclave with computing power:</p>

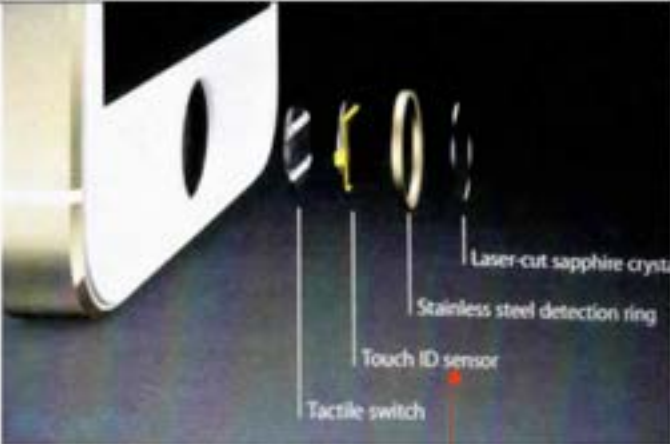
<u>Claim 1</u>	<u>Accused Instrumentalities</u>
	<p>"The <i>Secure Enclave</i> is a system on chip (SoC) that is included on all recent iPhone, ... devices" (Ex. A, Apple Platform Security, at 7.)</p> <p>"The Secure Enclave is a dedicated secure subsystem integrated into Apple systems on chip (SoCs)." (<i>Id.</i>, at 9.)</p> <p>The Secure Enclave Processor provides the main computing power for the Secure Enclave." (<i>Id.</i>, at 10.)</p> <p>"During enrollment, the Secure Enclave processes, encrypts, and <b>stores</b> the corresponding Touch ID and Face ID template data." (<i>Id.</i>, at 19.)</p> <p>The Secure Enclave has access to a memory assigned to it and accessible only to it:</p> <p><b>Secure nonvolatile storage</b> "The Secure Enclave is equipped with a dedicated secure nonvolatile storage device. The secure nonvolatile storage is connected to the Secure Enclave using a dedicated I2C bus, so that it can only be accessed by the Secure Enclave." (<i>Id.</i>, at 15.)</p> <p>This memory serves as a database for storing the biometric signatures:</p> <p>"The secure nonvolatile storage is used for all anti-replay services in the Secure Enclave. Anti-replay services on the Secure Enclave are used for revocation of data over events that mark anti-replay boundaries including, but not limited to, the following:</p> <ul style="list-style-type: none"> <li>• ...</li> <li>• Adding or removing a Touch ID fingerprint or Face ID face".</li> </ul> <p>(<i>Id.</i>, at 16.)</p>

<u>Claim 1</u>	<u>Accused Instrumentalities</u>
	<p>This database is shown in the figure from Apple Platform Security reproduced below:</p>  <p>The diagram illustrates the hardware components and their interconnections. At the top, NAND flash storage and DRAM are connected to the NAND flash controller and Memory controller, respectively. The Application Processor contains the NAND flash controller, AES engine, and Memory controller. The Secure Enclave contains the TMMG, Secure Enclave AES Engine, PCA, Secure Enclave Processor, Memory Protection Engine, and Secure Nonvolatile Storage. A key symbol indicates a secure connection between the AES engine and the Secure Enclave Processor. The entire system is labeled 'System on chip'.</p> <p>Secure Nonvolatile Storage The Secure Enclave components.</p> <p>Database 105 (Ex. A, Apple Platform Security, at 9.)</p>

<u>Claim 1</u>	<u>Accused Instrumentalities</u>
<p>1b. a transmitter sub-system comprising:</p>	<p><i>As set forth in elements 1b1, 1b2, and 1b3 below, the Accused Instrumentalities include a transmitter sub-system.</i></p> <p>The iPhone's Secure Enclave is a transmitter sub-system. It sends ephemerally re-encrypted file keys to the application processor with its file system driver ("Application Processor file-system driver") to read the files in the NAND Flash Storage.</p> <p>The Secure Enclave components. (Ex. A, Apple Platform Security, at 9.)</p>

<u>Claim 1</u>	<u>Accused Instrumentalities</u>
	<p>"sepOS can then use the ephemeral wrapping key to wrap file keys for use by the Application Processor file-system driver. When the file-system driver reads or writes a file, it sends the wrapped key to the AES Engine." <i>(Id.</i>, at 14.)</p> <p>"All wrapped file key handling occurs in the Secure Enclave; the file key is never directly exposed to the Application Processor. [...] When the Secure Enclave unwraps a file's keys, they're rewrapped with the ephemeral key and sent back to the Application Processor." <i>(Id.</i>, at 85.)</p> <p>The file system driver of the application processor is an NVME driver:</p> <div data-bbox="604 667 1766 1325" style="background-color: black; color: white; padding: 10px;"> <h3 style="text-align: center;">Filesystem Data Protection</h3> <pre> graph TD     subgraph User         U[User]     end     subgraph Kernel         HFS[HFS]         NVME[NVME Driver]     end     subgraph SEP         KS[Key Store]         AE[AES Engine]     end     subgraph Hardware         NAND[NAND]         SC[Storage Controller]     end      U -- "open('foo.txt', ...)" --&gt; HFS     HFS -- "1. Fetch wrapped file_key from metadata" --&gt; NVME     NVME -- "4. Send IO command with ephemerally wrapped file_key" --&gt; SC     SC -- "Cipher Text" --&gt; NAND     SC -- "Ephemeral Key established on boot" --&gt; AE     AE -- "3. Wrap file_key using ephemeral_key, return ephemerally wrapped file_key to kernel" --&gt; NVME     KS -- "2. Unwrap file_key using keybag key" --&gt; AE     </pre> </div> <p>(Ex. B, Behind the Scenes with iOS Security, at 30.)</p>

<u>Claim 1</u>	<u>Accused Instrumentalities</u>
<p>1b1. a biometric sensor configured to receive a biometric signal;</p>	<p><b><i>The Accused Instrumentalities include a biometric sensor configured to receive a biometric signal.</i></b></p> <p>More specifically, the iPhone has at least one biometric sensor for capturing a fingerprint or a face (Touch ID and/or Face ID), namely a Touch ID sensor and a camera system with image sensor, respectively.</p> <p><b>Touch ID</b></p> <p>"Apple devices with a Touch ID sensor can be unlocked using a fingerprint." (Ex. A, Apple Platform Security, at 19.)</p> <p>"Touch ID is the fingerprint sensing system that makes secure access to supported Apple devices faster and easier. This technology reads fingerprint data from any angle and learns more about a user's fingerprint over time, with the <b>sensor</b> continuing to expand the fingerprint map as additional overlapping nodes are identified with each use." (<i>Id.</i>)</p> <p>"When the fingerprint sensor detects the touch of a finger, it triggers the advanced imaging array to scan the finger and sends the scan to the Secure Enclave." (<i>Id.</i>)</p> <p>The biometric sensor for Touch ID is located below the home button:</p> <p>"The Home button is a stack of different materials, capped with a sapphire crystal lens. The surrounding stainless-steel ring works as a ground and detects the user's finger. This action activates a capacitive touch sensor installed underneath the cover: A CMOS chip with small capacitors." (<a href="https://appleinsider.com/inside/touch-id">https://appleinsider.com/inside/touch-id</a>)</p>

<u>Claim 1</u>	<u>Accused Instrumentalities</u>
	 <p data-bbox="892 797 1157 829">Biometric sensor 121</p> <p data-bbox="604 870 1108 902">"Where is the Touch ID sensor located?"</p> <p data-bbox="604 930 1829 995">The Touch ID sensor is located either in the home button or - on the iPad Air (4th generation) - in the top button.</p> <p data-bbox="604 1027 1129 1060"><a href="https://support.apple.com/en-us/HT201371">https://support.apple.com/en-us/HT201371</a>)</p> <p data-bbox="604 1097 1419 1130">The image sensor captures an 88-by-88-pixel, 500 PPI raster scan:</p> <p data-bbox="604 1170 1871 1375">"The 88-by-88-pixel, 500-ppi raster scan is temporarily stored in encrypted memory within the Secure Enclave while being vectorized for analysis, and then it's discarded. The analysis utilizes subdermal ridge flow angle mapping, which is a lossy process that discards minutia data that would be required to reconstruct the user's actual fingerprint. The resulting map of nodes is stored without any identity information in an encrypted format that can only be read by the Secure Enclave, and is never sent to Apple or backed up to iCloud or iTunes."</p>

<u>Claim 1</u>	<u>Accused Instrumentalities</u>
	<p>(Ex. C, iOS Security white paper, at 8.)</p> <p><b>Face ID</b></p> <p>The biometric sensor for facial biometrics is a camera system ("<b>TrueDepth camera system</b>") with an image sensor.</p> <p>"With a simple glance, Face ID securely unlocks supported Apple devices. It provides intuitive and secure authentication enabled by the TrueDepth camera system, which uses advanced technologies to accurately map the geometry of a user's face. "</p> <p>(Ex. A, Apple Platform Security, at 20.)</p> <p>To receive a biometric signal, the camera system with image sensor reads over 30,000 infrared points to capture depth information along with a two-dimensional infrared image.</p> <p>"After the TrueDepth camera confirms the presence of an attentive face, it projects and <b>reads over 30,000 infrared dots to form a depth map of the face along with a 2D infrared image</b>. This data is used to <b>create a sequence of 2D images and depth maps</b>, which are digitally signed and sent to the Secure Enclave. To counter both digital and physical spoofs, the TrueDepth camera randomizes the sequence of 2D images and depth map captures, and projects a device-specific random pattern. A portion of the Secure Neural Engine-protected within the Secure Enclave-transforms this data into a mathematical representation and compares that representation to the enrolled facial data. This enrolled facial data is itself a mathematical representation of the user's face captured across a variety of poses." (<i>Id.</i>)</p> <p>The camera system includes a biometric image sensor, namely a "CMOS image" sensor from Sony, to perform facial biometrics:</p>

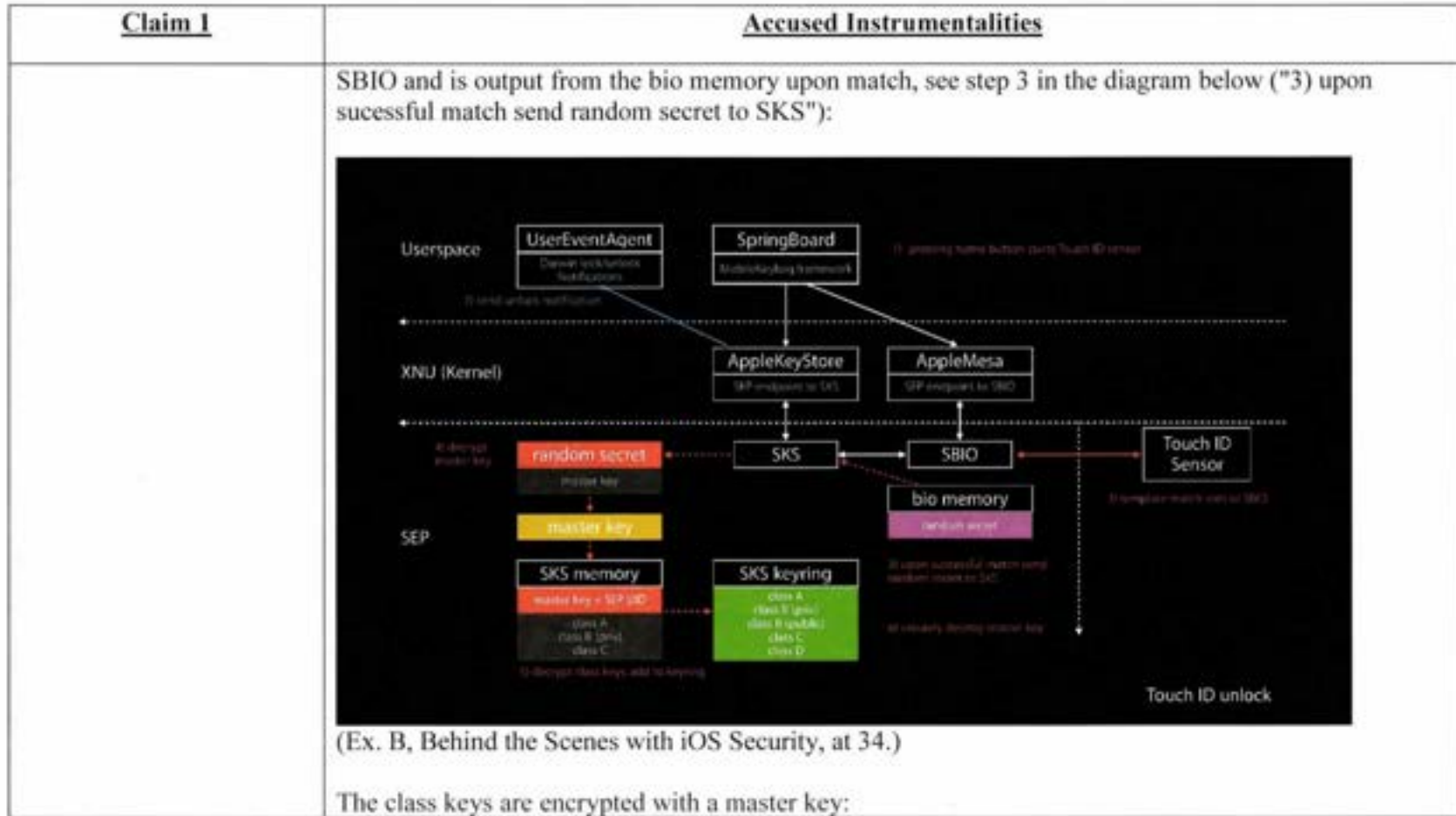


Claim 1	Accused Instrumentalities
	<p>(<a href="https://appleinsider.com/articles/17/09/09/inner-workings-of-apples-face-id-camera-detailed-in-report">https://appleinsider.com/articles/17/09/09/inner-workings-of-apples-face-id-camera-detailed-in-report</a>)</p>
<p>1b2. a transmitter sub-system controller configured to match the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute; and</p>	<p><i>The Accused Instrumentalities include a transmitter controller configured to emit a secure access signal conveying information dependent upon said accessibility attribute.</i></p> <p>More specifically, the iPhone's System on Chip (SOC), i.e. the Secure Enclave with its Secure Enclave Processor (SEP) or a Secure Neural Engine contained therein, is a means (103) to check a match of the biometric signal with elements of the biometric signature database.</p> <p>"The <i>Secure Enclave</i> is a system on chip (SoC) that is included on all recent iPhone, ... devices" (Ex. A, Apple Platform Security, at 7.)</p>

<u>Claim 1</u>	<u>Accused Instrumentalities</u>
	<p>"During <b>matching</b>, the Secure Enclave <b>compares</b> incoming data from the biometric sensor against the stored templates <b>to determine whether to unlock the device</b> or respond that a match is valid (for Apple Pay, in-app, and other uses of Touch ID and Face ID). "  <i>(Id.</i>, at 19.)</p> <p>The biometric signal received from the biometric sensor ("incoming data from the biometric sensor") is thus checked by the Secure Enclave and its SEP with the elements of the database of biometric signatures 105, i.e. the "stored templates", for the presence of a match.</p> <p>For Touch ID, the Secure Enclave match verification is performed as follows:</p> <p>"The Secure Enclave is responsible for processing fingerprint data from the Touch ID sensor, determining if there is a match against registered fingerprints, and then enabling access or purchases on behalf of the user ..."                  (Ex. C, iOS Security white paper, at 7.)</p> <p>"During enrollment, the resulting map of nodes is stored in an encrypted format that can be read only by the Secure Enclave as a template to compare against for future matches...."                  (Ex. A, Apple Platform Security, at 19.)</p> <p>"Touch ID can read multiple fingerprints, and it can read fingerprints in 360-degrees of orientation. It then creates a mathematical representation of your fingerprint and compares this to your enrolled fingerprint data to identify a match and unlock your device. "                  (<a href="https://support.apple.com/en-us/HT204587">https://support.apple.com/en-us/HT204587</a>)</p> <p>"Touch ID can read multiple fingerprints and recognize fingerprints at any orientation of the finger. The system then creates a mathematical representation of your fingerprint and compares it to the registered fingerprint data to determine a match and unlock your device."                  (<a href="https://support.apple.com/de-de/HT204587">https://support.apple.com/de-de/HT204587</a>)</p>

<u>Claim 1</u>	<u>Accused Instrumentalities</u>
	<p>For <b>Face ID</b>, the Secure Enclave has a neural network protected by it, i.e., a Secure Neural Engine, which is used to verify the match:</p> <p>"Face ID uses neural networks for determining attention, <b>matching</b>, and antispoofing, so a user can unlock their phone with a glance." (Ex. A, Apple Platform Security, at 20.)</p> <p>"A portion of the Secure Neural Engine-protected within the Secure Enclave-transforms this data into a mathematical representation and compares that representation to the enrolled facial data. This enrolled facial data is itself a mathematical representation of the user's face captured across a variety of poses." (<i>Id.</i>).</p> <p>"Facial matching security</p> <p>Facial matching is performed within the Secure Enclave using neural networks trained specifically for that purpose... Face ID data, including mathematical representations of a user's face, is encrypted and available only to the Secure Enclave. This data never leaves the device." (<i>Id.</i> at 23.)</p> <p>When the Secure Enclave, or more precisely the Touch ID or Face ID subsystem within the Secure Enclave, has determined that a match exists, an accessibility attribute is issued by the corresponding Touch ID or Face ID subsystem. This Touch ID or Face ID subsystem is also referred to as the SBIO. The accessibility attribute confirms that there is a match and that the iPhone is to be unlocked ("... determine whether to unlock the device ...").</p> <p>This confirmation of the match is signaled by the SBIO by issuing a random secret to which only the Touch ID or Face ID subsystem within the Secure Enclave has access:</p> <p>"During matching, the Secure Enclave compares incoming data from the biometric sensor against the stored templates to determine whether to unlock the device [...]." (<i>Id.</i> at 19.)</p>

<u>Claim 1</u>	<u>Accused Instrumentalities</u>
	<p>"Uses for Touch ID and Face ID</p> <p><b>Unlocking a device or user account</b></p> <p>[...] <b>keys for the highest class of Data Protection-which are held in the Secure Enclave [...].</b></p> <p>With Touch ID or Face ID enabled, the keys aren't discarded when the device or account locks; instead, <b>they're wrapped with a key that's given to the Touch ID or Face ID subsystem inside the Secure Enclave.</b> When a user attempts to unlock the device or account, <b>if the device detects a successful match, it provides the key for unwrapping the Data Protection keys,</b> and the device or account is unlocked. This process provides additional protection by requiring cooperation between the Data Protection and Touch ID or Face ID subsystems to unlock the device."</p> <p>(<i>Id.</i> at 24.)</p> <p>"The class key is protected with the hardware UID and, for some classes, the user's passcode." (<i>Id.</i> at 85.)</p> <p><b>"Complete Protection</b></p> <p>(<i>NSFileProtectionComplete</i>): The class key is protected with a key derived from the user passcode or password and the device UID. Shortly after the user locks a device (10 seconds, if the Require Password setting is Immediately), the decrypted class key is discarded, <b>rendering all data in this class inaccessible until the user enters the passcode again or unlocks (logs in to) the device using Touch ID or Face ID.</b>"</p> <p>(<i>Id.</i> at 86.)</p> <p>The Touch ID or Face ID subsystem within the Secure Enclave is the SBIO shown below. SBIO is an application that runs within the Secure Enclave on the SEP and is responsible for checking the match of biometric features. SBIO receives the corresponding biometric data from a biometric sensor, such as the Touch ID sensor. The random secret is stored in a memory ("bio memory") associated with the</p>



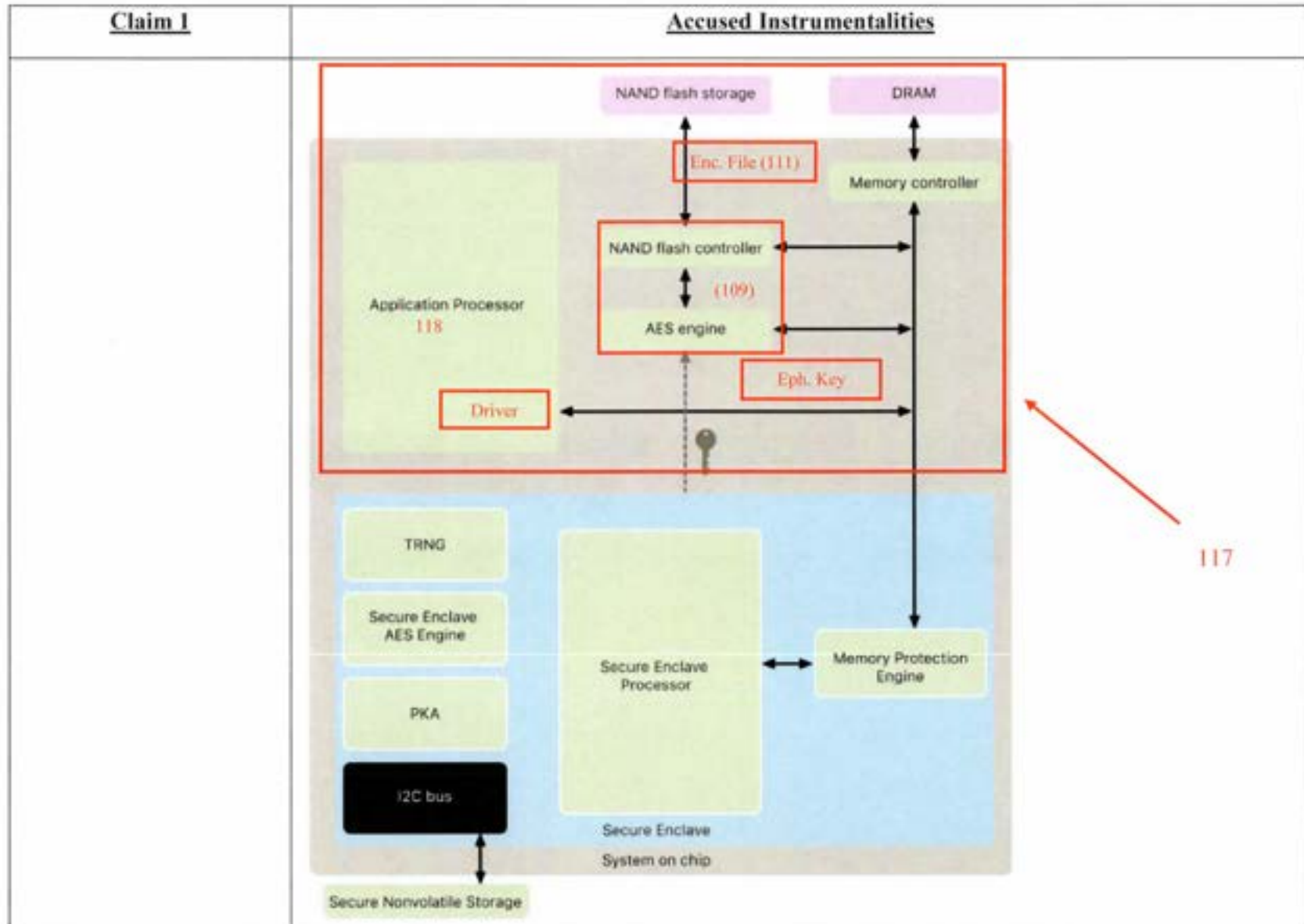
<u>Claim 1</u>	<u>Accused Instrumentalities</u>
	<p data-bbox="619 293 1044 370"><b>User Keybags</b></p> <p data-bbox="619 391 910 444">Background</p> <p data-bbox="619 500 1613 540">Sets of keys generated for each user to protect their data at rest</p> <p data-bbox="619 565 1710 605">Keys wrapped by master key derived from user passcode and SEP UID</p> <p data-bbox="619 630 1817 670">After 10 incorrect passcode entries, SEP will not process any further attempts</p> <p data-bbox="619 695 1696 735">Different policy associated with each keybag key—Usage, availability</p> <p data-bbox="612 760 757 792"><i>(Id., at 25.)</i></p> <p data-bbox="612 867 1889 1076">The random secret is issued to SKS. SKS is a Secure Key Service application which is located within the Secure Enclave on the SEP and is responsible for decrypting class keys. The random secret provided by SBIO is used to decrypt a master key ("4) decrypt master key"). The master key is concatenated with the UID of the SEP and thus class keys are decrypted and added to the SKS keyring ("5) decrypt class keys, add to keyring") for further use by the Secure Enclave. The decrypted class keys include, for example, the class key of class A.</p>
<p data-bbox="246 1117 591 1326">1b3. a transmitter configured to emit a secure access signal conveying information dependent upon said accessibility attribute; and</p>	<p data-bbox="612 1117 1817 1187"><i>The Accused Instrumentalities include a transmitter configured to emit a secure access signal conveying information dependent upon said accessibility attribute.</i></p> <p data-bbox="612 1222 1715 1255">For example, the Secure Enclave emits a signal with ephemerally re-encrypted file keys:</p> <p data-bbox="612 1295 1859 1395">"sepOS can then use the ephemeral wrapping key to wrap file keys for use by the Application Processor file-system driver. When the file-system driver reads or writes a file, it sends the wrapped key to the AES Engine."</p>

<u>Claim 1</u>	<u>Accused Instrumentalities</u>
	<p>(Ex. A, Apple Platform Security, at 14.)</p> <p>"All wrapped file key handling occurs in the Secure Enclave; the file key is never directly exposed to the Application Processor. [...] When the Secure Enclave unwraps a file's keys, they're rewrapped with the ephemeral key and sent back to the Application Processor." (<i>Id.</i> at 85.)</p> <p>The signal with the ephemerally re-encrypted file keys is a secure signal because it comes from the Secure Enclave and thus from a secure environment. Furthermore, the signal is secure because the transmitted information is encrypted. The emitted file keys are encrypted with the ephemeral key:</p> <p>"All wrapped file key handling occurs in the Secure Enclave; the file key is never directly exposed to the Application Processor. At startup, the Secure Enclave negotiates an ephemeral key with the AES Engine. When the Secure Enclave unwraps a file's keys, they're rewrapped with the ephemeral key and sent back to the Application Processor." (<i>Id.</i>)</p> <div data-bbox="604 878 1885 1377" style="background-color: black; color: white; padding: 10px;"> <h2 style="margin: 0;">Filesystem Data Protection</h2> <h3 style="margin: 0;">Overview</h3> <p style="margin: 0;">File blocks are encrypted using AES-XTS with 128-bit keys</p> <p style="margin: 0;">Each file on the user partition is encrypted using a unique random key chosen by SEP</p> <p style="margin: 0;">Raw file keys are never exposed to the AP</p> <ul style="list-style-type: none"> <li style="margin: 0;">• Wrapped with a key from the user keybag for long-term storage</li> <li style="margin: 0;">• Wrapped with an ephemeral key while in use, bound to boot session</li> </ul> </div>

<u>Claim 1</u>	<u>Accused Instrumentalities</u>
	<p>(Ex. B, Behind the Scenes with iOS Security, at 29.)</p> <div data-bbox="604 347 1766 1003" style="background-color: black; color: white; padding: 10px;"> <h3 style="text-align: center;">Filesystem Data Protection</h3> <pre> graph TD     subgraph User         U[User]     end     subgraph Kernel         HFS[HFS]         NVME[NVME Driver]     end     subgraph SEP         KS[Key Store]         AE[AES Engine]     end     subgraph Hardware         NAND[NAND]         SC[Storage Controller]     end     U -- "open('foo.txt') ..." --&gt; HFS     HFS -- "1. Fetch wrapped file_key from metadata" --&gt; NVME     NVME -- "4. Send ID command with ephemeral wrapped file_key" --&gt; SC     SC -- "Clear Text" --&gt; NVME     SC -- "Cipher Text" --&gt; NAND     AE -- "1. Wrap file_key using ephemeral_key, return ephemeral wrapped file_key to kernel" --&gt; KS     KS -- "2. Unwrap file_key using keybag key" --&gt; HFS     subgraph SEP_Boot [SEP]         EK[Ephemeral Key established on boot]     end     EK --&gt; AE             </pre> </div> <p>(<i>Id.</i>, at 30.)</p> <p>The information transmitted by the emitted signal, i.e., the ephemeral re-encrypted file keys, is dependent on the availability attribute, i.e., the confirmation that a biometric "template match" exists. This confirmation is signaled by the issuance of the random secret (cf. step 3): Only if there is a confirmation of the match and the random secret is issued by the Touch ID or Face ID subsystem within the Secure Enclave, i.e. SBIO, the class key is available for re-encrypting the file keys.</p> <p>The re-encrypted file keys are therefore information which is emitted depending on the fact that the availability attribute has been emitted.</p>




<u>Claim 1</u>	<u>Accused Instrumentalities</u>
1c. a receiver sub-system comprising:	<p data-bbox="612 285 1847 350"><i>As set forth in elements 1c1 and 1c2 below, the Accused Instrumentalities include a receiver sub-system.</i></p> <p data-bbox="612 391 1885 492">The receiver subsystem is the part of the system outside the Secure Enclave that is responsible for reading encrypted files from the NAND Flash Storage and receives ephemerally re-encrypted file keys from the Secure Enclave for this purpose:</p>




<u>Claim 1</u>	<u>Accused Instrumentalities</u>
	(Ex. A, Apple Platform Security, at 9.)
<p>1c1. a receiver sub-system controller configured to: receive the transmitted secure access signal; and</p>	<p><i>The Accused Instrumentalities include a receiver sub-system controller configured to: receive the transmitted secure access signal.</i></p> <p>An application processor (118) with file system driver, which receives the ephemerally re-encrypted file key. To read files from the NAND Flash storage, the application processor processes the received signal by creating a read command with the ephemerally wrapped file key ("IO command with ephemerally wrapped file_key") and sends it to the storage controller (109) (NAND Flash controller with AES engine). This read command provides the storage controller with all the information required to read and decrypt the encrypted file from the NAND flash storage:</p> <div data-bbox="612 704 1789 1360" data-label="Diagram"> <p>The diagram, titled "Filesystem Data Protection", illustrates the interaction between different system layers during a file read operation:</p> <ul style="list-style-type: none"> <li><b>User Layer:</b> Initiates the process with the command <code>open("foo.txt") ...</code>.</li> <li><b>Kernel Layer:</b> <ul style="list-style-type: none"> <li>1. Fetches the wrapped file key from metadata in the <b>HFS</b> (Hierarchical File System).</li> <li>4. Sends an IO command with the ephemerally wrapped file_key to the <b>NVME Driver</b>.</li> </ul> </li> <li><b>SEP (Secure Execution Platform) Layer:</b> <ul style="list-style-type: none"> <li>2. Unwraps the file_key using a keybag key from the <b>Key Store</b>.</li> <li>3. Wraps the file_key using an ephemeral_key from the <b>AES Engine</b> and returns the ephemerally wrapped file_key to the kernel.</li> </ul> </li> <li><b>Hardware Layer:</b> <ul style="list-style-type: none"> <li>The <b>Storage Controller</b> (containing an AES engine) receives the <b>IO command</b> and <b>Clear Text</b> from the NVME Driver.</li> <li>The <b>Storage Controller</b> sends <b>Cipher Text</b> to the <b>NAND</b> memory.</li> <li>An <b>Ephemeral Key</b> is established on boot and used by the Storage Controller.</li> </ul> </li> </ul> </div> <p>(Ex. B, Behind the Scenes with iOS Security, at 30.)</p>

<u>Claim 1</u>	<u>Accused Instrumentalities</u>
	<p>"sepOS can then use the ephemeral wrapping key to wrap file keys <b>for use by the Application Processor file-system driver. When the file-system driver reads or writes a file, it sends the wrapped key to the AES Engine.</b> "</p> <p>(Ex. A, Apple Platform Security, at 14.)</p> <p>"All wrapped file key handling occurs in the Secure Enclave; the file key is never directly exposed to the Application Processor. [...] When the Secure Enclave unwraps a file's keys, they're rewrapped with the ephemeral key and <b>sent back to the Application Processor.</b>"</p> <p>(<i>Id.</i>, at 85.)</p>
<p>1c2. provide conditional access to the controlled item dependent upon said information;</p>	<p><i>The Accused Instrumentalities include a receiver sub-system configured to provide conditional access to the controlled item dependent upon said information.</i></p> <p>More specifically, the controlled item is a locking mechanism of the door lock of the user's home. The Accused Instrumentalities are configured to provide secure access to the user's home via Yale Smart Locks when the user provides biometric signal to the Accused Instrumentalities via Touch ID or Face ID.</p> <p>"When the "Secure Remote Access" feature is turned on, the app will use your phone's built-in authentication tools to prompt fingerprint or facial recognition before you can unlock or lock your home remotely (note: if your phone does not have these features, it will prompt you to use your PIN code). This further ensures that your door is only operated by the right people at the time you intend for it."</p> <p>(<a href="https://us.yalehome.com/en/yale-news/blog/latest-blog-posts/introducing-biometric-verification-for-august-and-yale-locks1/">https://us.yalehome.com/en/yale-news/blog/latest-blog-posts/introducing-biometric-verification-for-august-and-yale-locks1/</a>)</p>

<u>Claim 1</u>	<u>Accused Instrumentalities</u>
	 <p>The screenshot shows a mobile application interface for Yale. At the top, there is a yellow circular logo with the word "Yale" in black. To the left of the logo is a hamburger menu icon and the word "Open". To the right is a magnifying glass search icon. Below the navigation bar, the text "Introducing Biometric Verification for August and Yale Locks" is displayed in a bold, black font. Underneath the text is a photograph of a hand holding a smartphone. The phone's screen displays a biometric verification interface with a large red circle containing a white "1-G" logo. The background of the photo is a blurred outdoor scene with green foliage.</p> <p>(<a href="https://us.yalehome.com/en/yale-news/blog/latest-blog-posts/introducing-biometric-verification-for-august-and-yale-locks1/">https://us.yalehome.com/en/yale-news/blog/latest-blog-posts/introducing-biometric-verification-for-august-and-yale-locks1/</a>)</p>

<u>Claim 1</u>	<u>Accused Instrumentalities</u>
	 <p>(<a href="https://www.apple.com/shop/product/HPAR2ZM/A/yale-assure-lock-sl-touchscreen-deadbolt-black">https://www.apple.com/shop/product/HPAR2ZM/A/yale-assure-lock-sl-touchscreen-deadbolt-black</a>)</p>


<u>Claim 1</u>	<u>Accused Instrumentalities</u>
<p>1d. wherein the transmitter sub-system controller is further configured to:</p>	<p><i>The Accused Instrumentalities include a transmitter sub-system controller that is configured to be used as set forth in elements 1d1, 1d2, and 1d3 below.</i></p>
<p>1d1. receive a series of entries of the biometric signal, said series being characterized according to at least one of the number of said entries and a duration of each said entry;</p>	<p><i>The Accused Instrumentalities include a transmitter sub-system controller configured to receive a series of entries of the biometric signal, said series being characterized according to at least one of the number of said entries and a duration of each said entry.</i></p> <p>More specifically, the Secure Enclave of the iPhone with the Secure Enclave Processor forms the means for receiving a series of entries of the biometric signal.</p> <p>"Apple's biometric security architecture relies on a strict separation of responsibilities between the biometric sensor and the Secure Enclave, and a secure connection between the two. The sensor captures the biometric image and securely transmits it to the Secure Enclave." (Ex. A, Apple Platform Security, at 19.)</p> <p><b>Touch ID</b></p> <p>When a finger is placed on the biometric sensor, the finger is scanned and the corresponding biometric signal entry is received by the Secure Enclave.</p> <p>"When the fingerprint sensor detects the touch of a finger, it triggers the advanced imaging array to scan the finger and sends the scan to the Secure Enclave." (<i>Id.</i>)</p> <p>To enroll a fingerprint in the database, the iPhone's fingerprint sensor records an entry of a biometric signal when the user places his finger on the sensor. This is done multiple times, resulting in a series of entries of such biometric signals.</p> <p>Receiving a series of entries of the biometric signal by repeatedly placing a finger on the Touch ID sensor will use Touch ID on iPhone.</p>

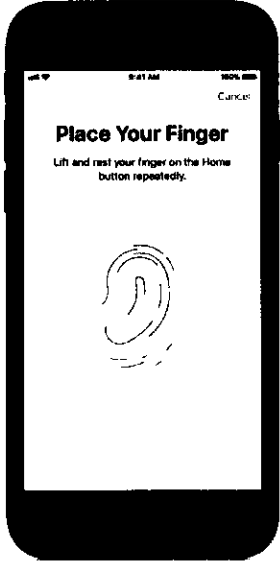
<u>Claim 1</u>	<u>Accused Instrumentalities</u>
	<p><b>Set up Touch ID</b></p> <p>Before you can set up Touch ID, you must first create a <a href="#">code</a> for your device,* then follow these steps:</p> <ol style="list-style-type: none"> <li>1. Make sure the Touch ID sensor and your finger are clean and dry.</li> <li>2. Tap Settings &gt; Touch ID &amp; Code, and then enter your code.</li> <li>3. Tap "Add fingerprint" and hold the device as you normally would when touching the Touch ID sensor.</li> <li>4. Touch the Touch ID sensor with one finger, but do not press. Keep your finger on the button until you feel a quick vibration or are prompted to lift your finger.</li> </ol>  <ol style="list-style-type: none"> <li>5. Continue by raising and slowly lowering your finger over and over again, changing the position of your finger just a tiny bit at a time.</li> </ol>

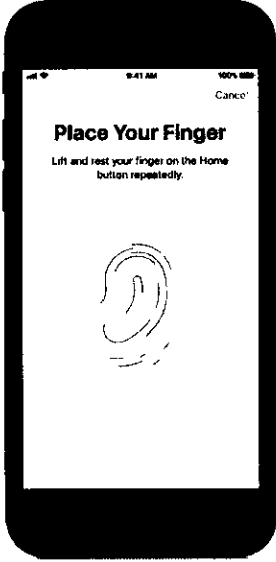



<u>Claim 1</u>	<u>Accused Instrumentalities</u>
	<p>6. The next screen will ask you to change your finger position. Hold your device as you normally would when unlocking it. Touch the Touch ID sensor with the outer edges of your fingertip instead of the middle part as you would during the first scan.”</p> <p>(<a href="https://support.apple.com/en-us/HT201371">https://support.apple.com/en-us/HT201371</a>)</p> <p>Accordingly, the user is prompted to place his finger on the sensor several times, in particular in accordance with step 5. Each time the finger is placed on the sensor, a corresponding biometric entry is generated, i.e. a series of such entries. All these entries, which result from placing the same finger on the sensor, form a series.</p> <p><b>Face ID</b></p> <p>The means for receiving a series of entries of the biometric signal includes a Secure Neural Engine, which is protected by the Secure Enclave. The Secure Neural Engine transforms the series of entries of the biometric signal received by the Secure Enclave into a biometric signature ("mathematical representation").</p> <p>"After the TrueDepth camera confirms the presence of an attentive face, it projects and reads over 30,000 infrared dots to form a depth map of the face along with a 2D infrared image. This data is used to create <b>a sequence of 2D images and depth maps</b>, which are digitally signed and <b>sent to the Secure Enclave</b>. To counter both digital and physical spoofs, the TrueDepth camera randomizes the sequence of 2D images and depth map captures, and projects a device-specific random pattern. A portion of the <b>Secure Neural Engine-protected</b> within the Secure Enclave-transforms this data into a mathematical representation and compares that representation to the enrolled facial data. This enrolled facial data is itself a mathematical representation of the user's face captured across a variety of poses." (Ex. A, Apple Platform Security, at 20.)</p> <p>Each entry of the biometric signal thus contains a two-dimensional infrared image with 30,000 infrared points for capturing depth information. By continuously capturing such infrared images into a Face ID scan while the user moves his head into different poses, a series of entries of the biometric signal</p>

<u>Claim 1</u>	<u>Accused Instrumentalities</u>
	<p>results. Two such Face ID scans are required to generate a biometric signature of a single face, so that two series of entries of the biometric signal are received accordingly.</p> <p>Using Face ID on iPhone</p> <ol style="list-style-type: none"> <li>1. Tap Settings &gt; Face ID &amp; Code. Enter your code when prompted.</li> <li>2. Tap on "Configure Face ID".</li> <li>3. Hold the device in portrait mode in front of your face and tap "Let's go".</li> <li>4. Make sure your face is inside the frame and slowly move your head until the circle shown is completed. If you can't move your head, tap on "Options for operating aids".</li> <li>5. After performing the first Face ID scan, tap "Next".</li> <li>6. Again, slowly describe a circle with your head until it is completed.</li> <li>7. Tap "Done."</li> </ol> <p>(<a href="https://support.apple.com/en-us/HT208109">https://support.apple.com/en-us/HT208109</a>)</p> <p>The biometric signature of a single face is thus determined by two successive Face ID scans, each of which receives a series of entries of the biometric signal (compare steps 4. and 6. above).</p> <p>To register a second face, the iPhone offers a corresponding option in its settings. If the user selects the option "Set up an alternative appearance" as shown in the figure below on <a href="https://www.macworld.co.uk/how-to/second-face-id-3803421/">https://www.macworld.co.uk/how-to/second-face-id-3803421/</a>, a second face is registered by the iPhone in the same way as the first face.</p>

<u>Claim 1</u>	<u>Accused Instrumentalities</u>
	 <p>The series of entries of the biometric signal is identified on the iPhone by both the number and duration of each such entry.</p> <p><b>Touch ID</b></p> <p>According to step 5 of the instructions <a href="https://support.apple.com/en-us/HT201371">https://support.apple.com/en-us/HT201371</a>, for the enrollment of a single finger, the user has to repeatedly place the respective finger on the sensor and thus a number of entries in a row predetermined via the user guidance are captured by the iPhone. Each one of the entries must also be of a predetermined duration given to the user via the iPhone display, i.e. the user's finger must remain on the sensor for a predetermined duration for each entry of the biometric signal in order to capture the biometric signal during this time.</p>

<u>Claim 1</u>	<u>Accused Instrumentalities</u>
	<p>Receiving a series of entries of the biometric signal by repeatedly placing a finger on the Touch ID sensor will use Touch ID on iPhone and iPad.</p> <p><b>Set up Touch ID</b></p> <p>...</p> <p>4. Touch the Touch ID sensor with one finger, but do not press. Keep your finger on the button until you feel a quick vibration or are prompted to lift your finger.</p>  <p>5. Continue by raising and slowly lowering your finger over and over again, changing the position of your finger just a tiny bit at a time.</p> <p>6. The next screen will ask you to change your finger position. Hold your device as you normally would when unlocking it. Touch the Touch ID sensor with the outer edges of your fingertip instead of the middle part as you did during the first scan.</p> <p>(<a href="https://support.apple.com/en-us/HT201371">https://support.apple.com/en-us/HT201371</a>)</p>

<u>Claim 1</u>	<u>Accused Instrumentalities</u>
	<p>After placing a finger on the home button, a fingerprint appears on the display with red progress bars spreading along some of the papillary bars until the capture of the biometric entry in question is complete:</p>  <p>When the required duration is reached, the iPhone vibrates after an entry of the biometric signal is received or it issues a prompt to the user to lift the finger. The user then lifts the finger in question and replaces the same finger so that the iPhone receives a series of biometric signal entries of sufficient duration for that finger. The process is repeated for the same finger for as long as required according to the iPhone's user guidance.</p> <p>This is shown in the Apple You Tube video (32) How to set up Touch ID on your iPhone or iPad - Apple Support - YouTube (<a href="https://www.youtube.com/watch?v=xTZ2LALWZlg">https://www.youtube.com/watch?v=xTZ2LALWZlg</a>):</p>

<u>Claim 1</u>	<u>Accused Instrumentalities</u>
	 <p>Both the number of entries, i.e. the number of repetitions for placing the finger on the screen, and their respective duration are specified by the iPhone via the user guidance.</p>

<u>Claim 1</u>	<u>Accused Instrumentalities</u>
	<p><b>Face ID</b></p> <p>The user moves his face in front of the camera to strike different poses, and the camera system with image sensor continuously captures a large number of biometric entries, i.e. here the 2D images with depth information, in a row.</p> <p>"This enrolled facial data is itself a mathematical representation of the user's face captured across a variety of poses." (Ex. A, Apple Platform Security, at 20.)</p> <p>The sufficient duration of an entry for a pose, i.e. an angular position of the head specified via the user interface of the iPhone, is indicated to the user by the transformation of a gray line into a green line:</p>  <p>(Individual images taken from: <a href="https://support.apple.com/en-us/HT208109">https://support.apple.com/en-us/HT208109</a>)</p>


<u>Claim 1</u>	<u>Accused Instrumentalities</u>
<p>1d2. map said series into an instruction; and</p>	<p><i>The Accused Instrumentalities include a transmitter sub-system controller configured to map said series into an instruction.</i></p> <p>More specifically, the Secure Enclave of the iPhone contains means to assign the received row to an instruction: The Secure Enclave, after receiving the full set of entries of the biometric signal, assigns this set to an instruction for processing, encrypting and storing the biometric signature ("Touch ID and Face ID template data").</p> <p>"The sensor captures the biometric image and securely transmits it to the Secure Enclave. During enrollment, the Secure Enclave processes, encrypts, and stores the corresponding Touch ID and Face ID template data." (Ex. A, Apple Platform Security, at 19.)</p> <p>To carry out this instruction, the Secure Enclave has its own processor: "The Secure Enclave Processor provides the main computing power for the Secure Enclave." (<i>Id.</i>, at 10.)</p> <p><b>Touch ID</b></p> <p>The instruction here involves the processing of under-the-skin fingerprint characteristics and their encrypted storage.</p> <p>"The analysis uses subdermal ridge flow angle mapping, a lossy process that discards "finger minutiae data" that would be required to reconstruct the user's actual fingerprint. During enrollment, the resulting map of nodes is stored in an encrypted format that can be read only by the Secure Enclave as a template to compare against for future matches, but without any identity information." (<i>Id.</i>, at 19.)</p> <p><b>Face ID</b></p>



<u>Claim 1</u>	<u>Accused Instrumentalities</u>
	<p>The instruction involves the transformation of the set of entries of the biometric signal captured via the Face ID scans into a mathematical representation, i.e. the biometric signature of the face in question by the Secure Neural Engine of the Secure Enclave, as well as its encryption and storage.</p> <p>"A portion of the Secure Neural Engine-protected within the Secure Enclave-transforms this data into a mathematical representation and compares that representation to the enrolled facial data. This enrolled facial data is itself a mathematical representation of the user's face captured across a variety of poses. " (<i>Id.</i>, at 20.)</p> <p>"Face ID data, including mathematical representations of a user's face, is encrypted and available only to the Secure Enclave. This data never leaves the device. It's not sent to Apple, nor is it included in device backups. The following Face ID data is saved, encrypted only for use by the Secure Enclave, during normal operation:</p> <ul style="list-style-type: none"> <li>• The mathematical representations of a user's face calculated during enrollment</li> <li>• ..."</li> </ul> <p>(<i>Id.</i>, at 23.)</p>

<u>Claim 1</u>	<u>Accused Instrumentalities</u>
<p>1d3. populate the database according to the instruction,</p>	<p><b><i>The Accused Instrumentalities include a transmitter sub-system controller configured to populate the database according to the instruction.</i></b></p> <p>More specifically, the Secure Enclave stores the biometric signature, i.e. the encrypted mathematical representation of the fingerprint or face, in the database 105, i.e. the "secure nonvolatile storage":</p> <p>"The secure nonvolatile storage is used for all anti-replay services in the Secure Enclave. Anti-replay services on the Secure Enclave are used for revocation of data over events that mark anti-replay boundaries including, but not limited to, the following:</p> <ul style="list-style-type: none"> <li>• ...</li> <li>• ...</li> <li>• Adding or removing a Touch ID fingerprint or Face ID face".</li> </ul> <p>(Ex. A, Apple Platform Security, at 16.)</p> <p>"During enrollment, the Secure Enclave processes, encrypts, and stores the corresponding Touch ID and Face ID template data." (<i>Id.</i>, at 19.)</p> <p><b>Touch ID</b></p> <p>"During enrollment, the resulting map of nodes is stored in an encrypted format that can be read only by the Secure Enclave as a template to compare against for future matches...." (<i>Id.</i>)</p> <p><b>Face ID</b></p> <p>The following Face ID data is saved, encrypted only for use by the Secure Enclave, during normal operation:</p> <ul style="list-style-type: none"> <li>• The mathematical representations of a user's face calculated during enrollment".</li> </ul> <p>(<i>Id.</i>, at 23.)</p>

<u>Claim 1</u>	<u>Accused Instrumentalities</u>
<p>wherein the controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing device.</p>	<p><i>The Accused Instrumentalities are configured to provide access to the controlled item, wherein the controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing device.</i></p> <p>More specifically, the controlled item is a locking mechanism of the door lock of the user's home. The Accused Instrumentalities are configured to provide secure access to the user's home via Yale Smart Locks when the user provides biometric signal to the Accused Instrumentalities via Touch ID or Face ID.</p> <p>"When the "Secure Remote Access" feature is turned on, the app will use your phone's built-in authentication tools to prompt fingerprint or facial recognition before you can unlock or lock your home remotely (note: if your phone does not have these features, it will prompt you to use your PIN code). This further ensures that your door is only operated by the right people at the time you intend for it."</p> <p>(<a href="https://us.yalehome.com/en/yale-news/blog/latest-blog-posts/introducing-biometric-verification-for-august-and-yale-locks1/">https://us.yalehome.com/en/yale-news/blog/latest-blog-posts/introducing-biometric-verification-for-august-and-yale-locks1/</a>)</p>

<u>Claim 1</u>	<u>Accused Instrumentalities</u>
	 <p>The screenshot shows a mobile application interface for Yale. At the top, there is a yellow circular logo with the word "Yale" in black. To the left of the logo is a hamburger menu icon and the word "Open". To the right is a magnifying glass search icon. Below the navigation bar, the text "Introducing Biometric Verification for August and Yale Locks" is displayed in a bold, black font. Underneath the text is a photograph of a hand holding a smartphone. The phone's screen displays a biometric verification interface with a red circular camera viewfinder and a black square in the center containing a white face icon. Below the photograph, the URL <a href="https://us.yalehome.com/en/yale-news/blog/latest-blog-posts/introducing-biometric-verification-for-august-and-yale-locks1/">(https://us.yalehome.com/en/yale-news/blog/latest-blog-posts/introducing-biometric-verification-for-august-and-yale-locks1/)</a> is provided.</p>

<u>Claim 1</u>	<u>Accused Instrumentalities</u>
	 <p data-bbox="612 1078 1874 1110">(https://www.apple.com/shop/product/HPAR2ZM/A/yale-assure-lock-sl-touchscreen-deadbolt-black)</p>

<u>Claim 2</u>	<u>Accused Instrumentalities</u>
2. The system according to claim 1, wherein the transmitter sub-system	<i>Upon information and belief, the Accused Instrumentalities include the transmitter sub-system controller that is configured to be used as set forth in elements 2a, 2b, and 2c below.</i>


<u>Claim 2</u>	<u>Accused Instrumentalities</u>
controller is further configured to:	
2a. provide a signal for directing input of the series of entries of the biometric signal;	<p><b><i>Upon information and belief, the Accused Instrumentalities are configured to provide a signal for directing input of the series of entries of the biometric signal.</i></b></p> <p>More specifically, the Accused Instrumentalities provide instructions for the user to input a series of fingerprint or face images via Touch ID and Face ID.</p> <p>Touch ID: Register a fingerprint for Apple Touch ID by the user tapping a finger several times on the home button to record the fingerprint data. (<a href="https://video.search.yahoo.com/yhs/search?fr=yhs-pty-pty_converter&amp;hsimp=yhs-pty_converter&amp;hspart=pty&amp;p=registering+fingerprint+apple+touch+id+on+screen+instructions#id=1&amp;vid=156de65ae06ca453643009fc0ea9cf79&amp;action=click.">https://video.search.yahoo.com/yhs/search?fr=yhs-pty-pty_converter&amp;hsimp=yhs-pty_converter&amp;hspart=pty&amp;p=registering+fingerprint+apple+touch+id+on+screen+instructions#id=1&amp;vid=156de65ae06ca453643009fc0ea9cf79&amp;action=click.</a>)</p> <p>Touch ID: The user's finger must remain on the home button long enough for the data to be recorded. "Touch the Touch ID sensor with your finger, but don't press it. Hold it there until you feel a quick vibration, or until you're asked to lift your finger." "Continue to lift and rest your finger slowly, making small adjustments to the position of your finger each time." (<a href="https://support.apple.com/en-au/HT201371">https://support.apple.com/en-au/HT201371</a>)</p> <p>Touch ID: "you shouldn't tap too quickly or move your finger around" (<a href="https://support.apple.com/en-us/HT207537">https://support.apple.com/en-us/HT207537</a>)</p> <p>Face ID: Setting up Face ID requires two scans of the user's face. Each scan asks users to move their head slowly in a circle to register different angles of the user's face. (<a href="https://www.imore.com/how-set-face-id-iphone">https://www.imore.com/how-set-face-id-iphone</a>)</p>

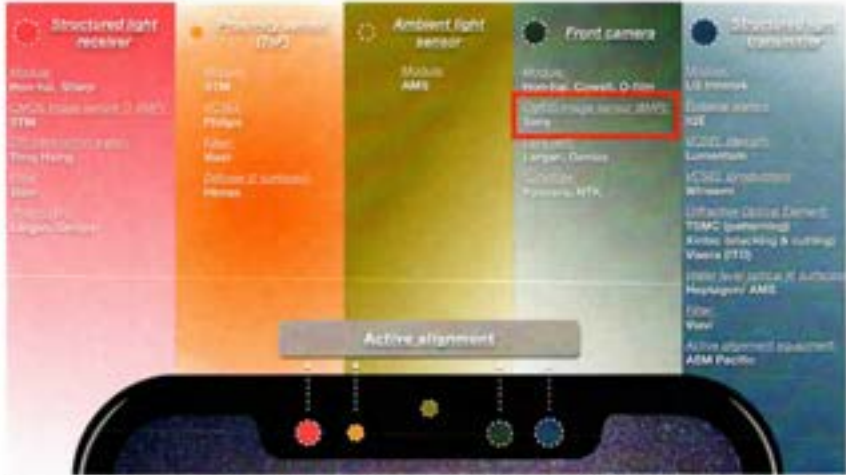
<u>Claim 2</u>	<u>Accused Instrumentalities</u>
	 <p>(<a href="https://support.apple.com/en-us/HT201371">https://support.apple.com/en-us/HT201371</a>)</p>

<u>Claim 2</u>	<u>Accused Instrumentalities</u>
	 <p>(<a href="https://support.apple.com/en-us/HT208109">https://support.apple.com/en-us/HT208109</a>)</p>
<p>2b. incorporate into the secure access signal an identification field identifying the biometric signal if the signal matches a member of the database; and</p>	<p><i>Upon information and belief, the Accused Instrumentalities are configured to incorporate into the secure access signal an identification field identifying the biometric signal if the signal matches a member of the database.</i></p> <p>More specifically, upon information and belief, the Accused Instrumentalities are configured to provide secure access signal when the fingerprint or face image received via Touch ID and Face ID matches the fingerprint and face data stored in the Secure Nonvolatile Storage.</p> <p>“During matching, the Secure Enclave compares incoming data from the biometric sensor against the stored templates to determine whether to unlock the device or respond that a match is valid (for Apple Pay, in-app, and other uses of Touch ID and Face ID). The architecture supports devices that include both the sensor and Secure Enclave (such as iPhone, iPad, and many Mac systems), as well as the ability to physically separate the sensor into a peripheral that is then securely paired to the Secure Enclave in a Mac with Apple silicon.”</p> <p>(<a href="https://support.apple.com/ko-kr/guide/security/sec067eb0c9e/1/web/1">https://support.apple.com/ko-kr/guide/security/sec067eb0c9e/1/web/1</a>)</p>



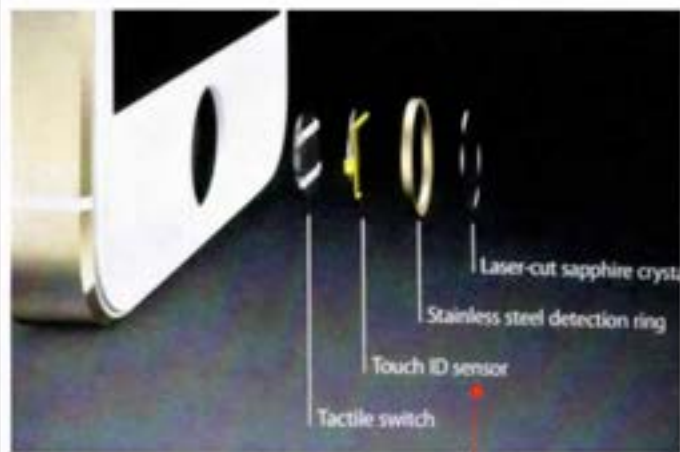
<u>Claim 2</u>	<u>Accused Instrumentalities</u>
	<p>With Touch ID and Face ID, the keys for the highest class of Data Protection are held in the Secure Enclave, “[w]hen a user attempts to unlock the device or account, if the device detects a successful match, it provides the key for unwrapping the Data Protection keys, and the device or account is unlocked.” (Ex. A, Apple Platform Security, at 24.)</p>
<p>2c. construct an audit trail of biometric signals provided to the biometric sensor in order to access the controlled item.</p>	<p><i>Upon information and belief, the Accused Instrumentalities are configure to construct an audit trail of biometric signals provided to the biometric sensor in order to access the controlled item.</i></p> <p>More specifically, upon information and belief, the Accused Instrumentalities are configured to construct an audit trail of the enrolled fingerprint and face data to continually improve matching accuracy.</p> <p>“Touch ID will incrementally update the mathematical representation of enrolled fingerprints over time to improve matching accuracy.” (<a href="https://support.apple.com/en-us/HT204587">https://support.apple.com/en-us/HT204587</a>)</p> <p>“Face ID data - including mathematical representations of your face - is encrypted and protected by the Secure Enclave. This data will be refined and updated as you use Face ID to improve your experience, including when you successfully authenticate. Face ID will also update this data when it detects a close match but a passcode is subsequently entered to unlock the device.” (<a href="https://support.apple.com/en-us/HT208108">https://support.apple.com/en-us/HT208108</a>)</p> <p>In an alternative read, upon information and belief, every time a user uses Touch ID or Face ID to access an iPhone, the iPhone keeps a record of fingerprint and face unlocking, or some kind record for subsequent auditing.</p>

<u>Claim 4</u>	<u>Accused Instrumentalities</u>
<p>4. The system according to claim 1, wherein the biometric sensor is responsive to one of voice, retinal pattern, iris pattern, face pattern, and palm configuration, and/or the database of biometric signatures is located in at least one of the transmitter sub-system and the receiver sub-system.</p>	<p><i>The Accused Instrumentalities includes a biometric sensor that is responsive to one of voice, retinal pattern, iris pattern, face pattern, and palm configuration, and/or the database of biometric signatures is located in at least one of the transmitter sub-system and the receiver sub-system.</i></p> <p>More specifically, the Accused Instrumentalities include a CMOS image sensor in the front camera of the iPhones that is responsive to face pattern of the user. Upon information and belief, the Secure Nonvolatile Storage is a memory including a database of the face data.</p> <p><b>Face ID</b>  The biometric sensor for facial biometrics is a camera system ("TrueDepth camera system") with an image sensor.  "With a simple glance, Face ID securely unlocks supported Apple devices. It provides intuitive and secure authentication enabled by the TrueDepth camera system, which uses advanced technologies to accurately map the geometry of a user's face."  (Ex. A, Apple Platform Security, at 20.)</p>  <p>(<a href="https://appleinsider.com/articles/17/09/09/inner-workings-of-apples-face-id-camera-detailed-in-report">https://appleinsider.com/articles/17/09/09/inner-workings-of-apples-face-id-camera-detailed-in-report</a>)</p>

<u>Claim 6</u>	<u>Accused Instrumentalities</u>
<p>6. The system as claimed in claim 1, wherein the biometric sensor is further configured to authenticate the identity of a user;</p>	<p><i>The Accused Instrumentalities includes a biometric sensor that is further configured to authenticate the identity of a user.</i></p> <p>More specifically, the iPhones uses Face ID and Touch ID to authenticate the user's identity.</p> <p><b>Face ID</b> The biometric sensor for facial biometrics is a camera system ("TrueDepth camera system") with an image sensor.</p> <p>"With a simple glance, Face ID securely unlocks supported Apple devices. It provides intuitive and secure authentication enabled by the TrueDepth camera system, which uses advanced technologies to accurately map the geometry of a user's face." (Ex. A, Apple Platform Security, at 20.)</p>  <p>(<a href="https://appleinsider.com/articles/17/09/09/inner-workings-of-apples-face-id-camera-detailed-in-report">https://appleinsider.com/articles/17/09/09/inner-workings-of-apples-face-id-camera-detailed-in-report</a>)</p> <p><b>Touch ID</b></p>

"Apple devices with a Touch ID sensor can be unlocked using a fingerprint."  
(Ex. A, Apple Platform Security, at 9.)

"Touch ID is the fingerprint sensing system that makes secure access to supported Apple devices faster and easier. This technology reads fingerprint data from any angle and learns more about a user's fingerprint over time, with the sensor continuing to expand the fingerprint map as additional overlapping nodes are identified with each use."  
(*Id.* at 19.)



Biometric sensor 121

<p>6a. wherein the transmitter is further configured to transmit information capable of granting access to the controlled item using a secure wireless signal dependent upon a request from the user and the authentication of the user identity; and</p>	<p><b><i>The Accused Instrumentalities includes a transmitter configured to transmit information capable of granting access to the controlled item using a secure wireless signal dependent upon a request from the user and the authentication of the user identity.</i></b></p> <p>Upon information and belief, the Secure Enclave of the iPhone is configured to grant access to the controlled item (e.g., a locking mechanism of the door lock) via Wi-Fi, mobile data or Bluetooth dependent upon the user’s request to unlock and the user’s authentication via Touch ID or Face ID.</p> <p>“When the ‘Secure Remote Access’ feature is turned on, the app will use your phone’s built-in authentication tools to prompt fingerprint or facial recognition before you can unlock or lock your home remotely (note: if your phone does not have these features, it will prompt you to use your PIN code). This further ensures that your door is only operated by the right people at the time you intend for it.” “The feature applies to operations done via Wi-Fi, mobile data or Bluetooth. You’ll be able to opt in to this security feature, and it will not be enacted when checking your lock status in order to preserve a seamless app experience.”</p> <p>(<a href="https://us.yalehome.com/en/yale-news/blog/latest-blog-posts/introducing-biometric-verification-for-august-and-yale-locks1/">https://us.yalehome.com/en/yale-news/blog/latest-blog-posts/introducing-biometric-verification-for-august-and-yale-locks1/</a>)</p>
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

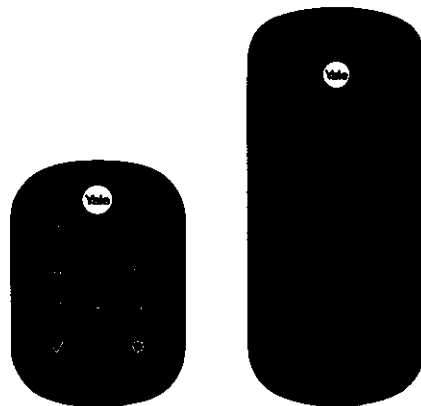
6b. the system further comprising a control panel configured to receive the information and provide the secure access requested.

*The Accused Instrumentalities includes a control panel configured to receive the information and provide the secure access requested.*

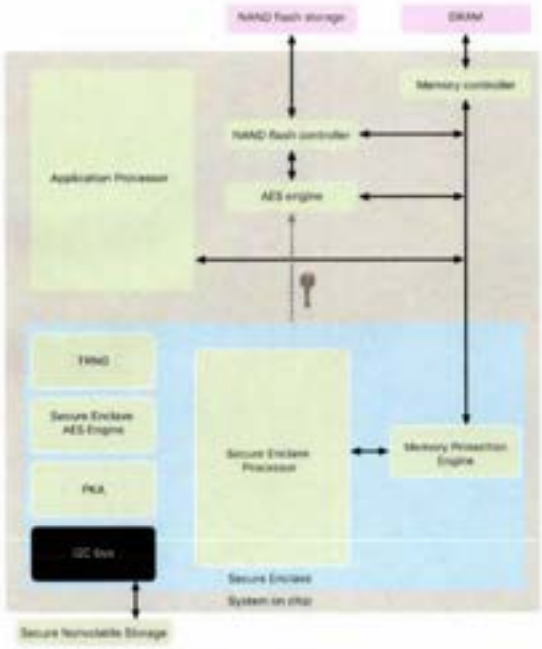
More specifically, upon information and belief, the Yale Home Smart Lock is configured to receive information allowing its unlocking from the Secure Enclave of the iPhone.

“Upgrade your door with the Assure Lock SL, a touchscreen deadbolt for key-free entry. The lock is HomeKit-enabled so it allows you to lock or unlock and share access all from your Yale Secure app.”

(<https://www.apple.com/shop/product/HPAR2ZM/A/yale-assure-lock-sl-touchscreen-deadbolt-black>)

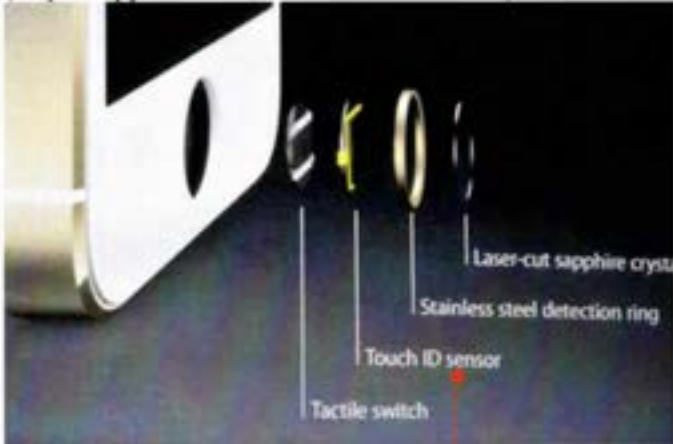


(<https://www.apple.com/shop/product/HPAR2ZM/A/yale-assure-lock-sl-touchscreen-deadbolt-black>)


<u>Claim 9</u>	<u>Accused Instrumentalities</u>
<p>9. The system according to claim 1, wherein: the transmitter sub-system and the receiver sub-system are collocated in the electronic computing device.</p>	<p><i>The transmitter sub-system and the receiver sub-system are collocated in the Accused Instrumentalities.</i></p> <p>More specifically, the iPhone is a computing device that includes the transmitter sub-system and the receiver sub-system.</p>  <p>The Secure Enclave components</p> <p>(Ex. A, Apple Platform Security, at 9.)</p>

<u>Claim 10</u>	<u>Accused Instrumentalities</u>
10. A transmitter sub-system for operating in a system for providing secure access to a controlled item, wherein the transmitter sub-system comprises:	<i>To the extent that the preamble is deemed to be a limitation, the Accused Instrumentalities are configured to use a system in accordance with this claim.</i>
10a. a biometric sensor configured to receiving a biometric signal;	<p><i>The Accused Instrumentalities include a biometric sensor configured to receive a biometric signal.</i></p> <p>More specifically, the iPhone has at least one biometric sensor for capturing a fingerprint or a face (Touch ID and/or Face ID), namely a Touch ID sensor and a camera system with image sensor, respectively.</p> <p><b>Touch ID</b></p> <p>"Apple devices with a Touch ID sensor can be unlocked using a fingerprint." (Ex. A, Apple Platform Security, at 19.)</p> <p>"Touch ID is the fingerprint sensing system that makes secure access to supported Apple devices faster and easier. This technology reads fingerprint data from any angle and learns more about a user's fingerprint over time, with the <b>sensor</b> continuing to expand the fingerprint map as additional overlapping nodes are identified with each use." (<i>Id.</i>)</p> <p>"When the fingerprint sensor detects the touch of a finger, it triggers the advanced imaging array to scan the finger and sends the scan to the Secure Enclave." (<i>Id.</i>)</p>



<u>Claim 10</u>	<u>Accused Instrumentalities</u>
	<p>The biometric sensor for Touch ID is located below the home button:</p> <p>"The Home button is a stack of different materials, capped with a sapphire crystal lens. The surrounding stainless-steel ring works as a ground and detects the user's finger. This action activates a capacitive touch sensor installed underneath the cover: A CMOS chip with small capacitors."                      (https://appleinsider.com/inside/touch-id)</p>  <p style="text-align: center;">Biometric sensor 121</p> <p>"Where is the Touch ID sensor located?</p> <p>The Touch ID sensor is located either in the home button or - on the iPad Air (4th generation) - in the top button.</p> <p>(https://support.apple.com/en-us/HT201371)</p> <p>The image sensor captures an 88-by-88-pixel, 500 PPI raster scan:</p>

<u>Claim 10</u>	<u>Accused Instrumentalities</u>
	<p>"The 88-by-88-pixel, 500-ppi raster scan is temporarily stored in encrypted memory within the Secure Enclave while being vectorized for analysis, and then it's discarded. The analysis utilizes subdermal ridge flow angle mapping, which is a lossy process that discards minutia data that would be required to reconstruct the user's actual fingerprint. The resulting map of nodes is stored without any identity information in an encrypted format that can only be read by the Secure Enclave, and is never sent to Apple or backed up to iCloud or iTunes." (Ex. C, iOS Security white paper, at 8.)</p> <p><b>Face ID</b></p> <p>The biometric sensor for facial biometrics is a camera system ("<b>TrueDepth camera system</b>") with an image sensor.</p> <p>"With a simple glance, Face ID securely unlocks supported Apple devices. It provides intuitive and secure authentication enabled by the TrueDepth camera system, which uses advanced technologies to accurately map the geometry of a user's face." (Ex. A, Apple Platform Security, at 20.)</p> <p>To receive a biometric signal, the camera system with image sensor reads over 30,000 infrared points to capture depth information along with a two-dimensional infrared image.</p> <p>"After the TrueDepth camera confirms the presence of an attentive face, it projects and <b>reads over 30,000 infrared dots to form a depth map of the face along with a 2D infrared image</b>. This data is used to <b>create a sequence of 2D images and depth maps</b>, which are digitally signed and sent to the Secure Enclave. To counter both digital and physical spoofs, the TrueDepth camera randomizes the sequence of 2D images and depth map captures, and projects a device-specific random pattern. A portion of the Secure Neural Engine-protected within the Secure Enclave-transforms this data into a mathematical representation and compares that representation to the enrolled facial data. This enrolled facial data is itself a mathematical representation of the user's face captured across a variety of poses." (<i>Id.</i>)</p>

<u>Claim 10</u>	<u>Accused Instrumentalities</u>
	<p>The camera system includes a biometric image sensor, namely a "CMOS image" sensor from Sony, to perform facial biometrics:</p>  <p>(<a href="https://appleinsider.com/articles/17/09/09/inner-workings-of-apples-face-id-camera-detailed-in-report">https://appleinsider.com/articles/17/09/09/inner-workings-of-apples-face-id-camera-detailed-in-report</a>)</p>
<p>10b. a controller configured to match the biometric signal against members of a database of biometric signatures to</p>	<p><i>The Accused Instrumentalities include a transmitter controller configured to emit a secure access signal conveying information dependent upon said accessibility attribute.</i></p>

<u>Claim 10</u>	<u>Accused Instrumentalities</u>
thereby output an accessibility attribute; and	<p>More specifically, the iPhone's System on Chip (SOC), i.e. the Secure Enclave with its Secure Enclave Processor (SEP) or a Secure Neural Engine contained therein, is a means (103) to check a match of the biometric signal with elements of the biometric signature database.</p> <p>"The <i>Secure Enclave</i> is a system on chip (SoC) that is included on all recent iPhone, ... devices" (Ex. A, Apple Platform Security, at 7.)</p> <p>"During <b>matching</b>, the Secure Enclave <b>compares</b> incoming data from the biometric sensor against the stored templates <b>to determine whether to unlock the device</b> or respond that a match is valid (for Apple Pay, in-app, and other uses of Touch ID and Face ID). " (<i>Id.</i>, at 19.)</p> <p>The biometric signal received from the biometric sensor ("incoming data from the biometric sensor") is thus checked by the Secure Enclave and its SEP with the elements of the database of biometric signatures 105, i.e. the "stored templates", for the presence of a match.</p> <p>For Touch ID, the Secure Enclave match verification is performed as follows:</p> <p>"The Secure Enclave is responsible for processing fingerprint data from the Touch ID sensor, determining if there is a match against registered fingerprints, and then enabling access or purchases on behalf of the user ..." (Ex. C, iOS Security white paper, at 7.)</p> <p>"During enrollment, the resulting map of nodes is stored in an encrypted format that can be read only by the Secure Enclave as a template to compare against for future matches...." (Ex. A, Apple Platform Security, at 19.)</p> <p>"Touch ID can read multiple fingerprints, and it can read fingerprints in 360-degrees of orientation. It then creates a mathematical representation of your fingerprint and compares this to your enrolled fingerprint data to identify a match and unlock your device. " (<a href="https://support.apple.com/en-us/HT204587">https://support.apple.com/en-us/HT204587</a>)</p>

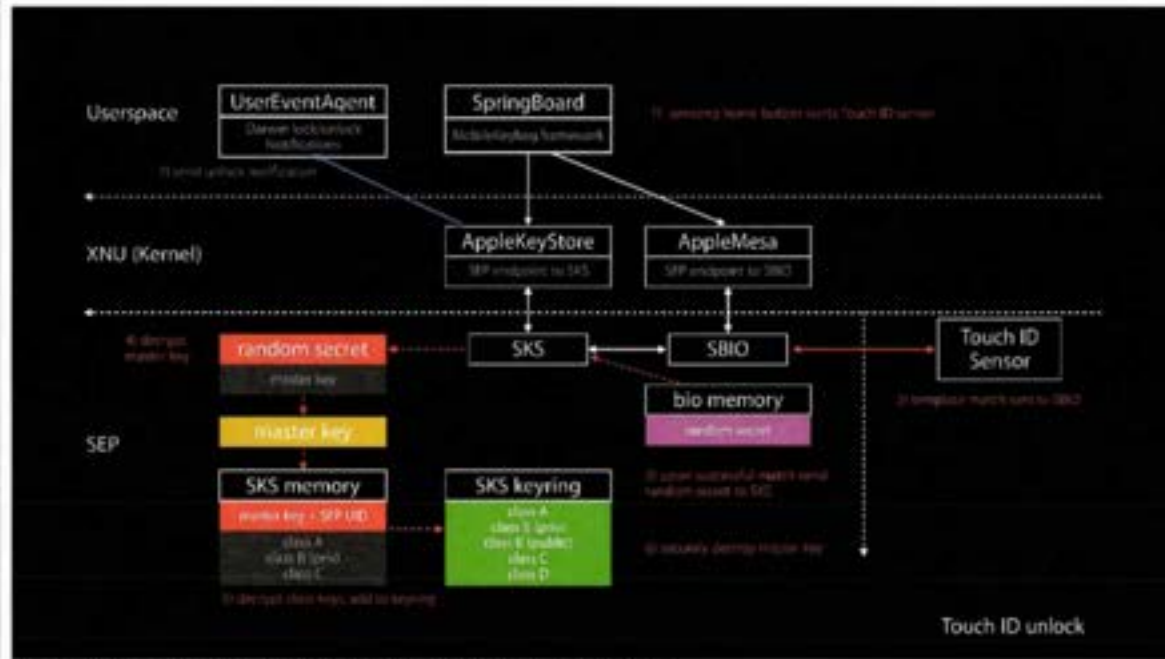
<u>Claim 10</u>	<u>Accused Instrumentalities</u>
	<p>"Touch ID can read multiple fingerprints and recognize fingerprints at any orientation of the finger. The system then creates a mathematical representation of your fingerprint and compares it to the registered fingerprint data to determine a match and unlock your device." (<a href="https://support.apple.com/de-de/HT204587">https://support.apple.com/de-de/HT204587</a>)</p> <p>For <b>Face ID</b>, the Secure Enclave has a neural network protected by it, i.e., a Secure Neural Engine, which is used to verify the match:</p> <p>"Face ID uses neural networks for determining attention, <b>matching</b>, and antispoofing, so a user can unlock their phone with a glance." (Ex. A, Apple Platform Security, at 20.)</p> <p>"A portion of the Secure Neural Engine-protected within the Secure Enclave-transforms this data into a mathematical representation and compares that representation to the enrolled facial data. This enrolled facial data is itself a mathematical representation of the user's face captured across a variety of poses." (<i>Id.</i>).</p> <p>"Facial matching security Facial matching is performed within the Secure Enclave using neural networks trained specifically for that purpose... Face ID data, including mathematical representations of a user's face, is encrypted and available only to the Secure Enclave. This data never leaves the device." (<i>Id.</i> at 23.)</p> <p>When the Secure Enclave, or more precisely the Touch ID or Face ID subsystem within the Secure Enclave, has determined that a match exists, an accessibility attribute is issued by the corresponding Touch ID or Face ID subsystem. This Touch ID or Face ID subsystem is also referred to as the SBIO. The accessibility attribute confirms that there is a match and that the iPhone is to be unlocked ("... determine whether to unlock the device ...").</p>

<u>Claim 10</u>	<u>Accused Instrumentalities</u>
	<p>This confirmation of the match is signaled by the SBIO by issuing a random secret to which only the Touch ID or Face ID subsystem within the Secure Enclave has access:</p> <p>"During matching, the Secure Enclave compares incoming data from the biometric sensor against the stored templates to determine whether to unlock the device [...]."  <i>(Id. at 19.)</i></p> <p>"Uses for Touch ID and Face ID</p> <p><b>Unlocking a device or user account</b></p> <p>[...] <b>keys for the highest class of Data Protection-which are held in the Secure Enclave [...].</b></p> <p>With Touch ID or Face ID enabled, the keys aren't discarded when the device or account locks; instead, <b>they're wrapped with a key that's given to the Touch ID or Face ID subsystem inside the Secure Enclave.</b> When a user attempts to unlock the device or account, <b>if the device detects a successful match, it provides the key for unwrapping the Data Protection keys,</b> and the device or account is unlocked. This process provides additional protection by requiring cooperation between the Data Protection and Touch ID or Face ID subsystems to unlock the device."  <i>(Id. at 24.)</i></p> <p>"The class key is protected with the hardware UID and, for some classes, the user's passcode."  <i>(Id. at 85.)</i></p> <p><b>"Complete Protection</b></p> <p><i>(NSFileProtectionComplete):</i> The class key is protected with a key derived from the user passcode or password and the device UID. Shortly after the user locks a device (10 seconds, if the Require Password setting is Immediately), the decrypted class key is discarded, <b>rendering all data in this class inaccessible until the user enters the passcode again or unlocks (logs in to) the device using Touch ID or Face ID.</b>"  <i>(Id. at 86.)</i></p>

**Claim 10**

**Accused Instrumentalities**

The Touch ID or Face ID subsystem within the Secure Enclave is the SBIO shown below. SBIO is an application that runs within the Secure Enclave on the SEP and is responsible for checking the match of biometric features. SBIO receives the corresponding biometric data from a biometric sensor, such as the Touch ID sensor. The random secret is stored in a memory ("bio memory") associated with the SBIO and is output from the bio memory upon match, see step 3 in the diagram below ("3) upon successful match send random secret to SKS"):



(Ex. B, Behind the Scenes with iOS Security, at 34.)

The class keys are encrypted with a master key:

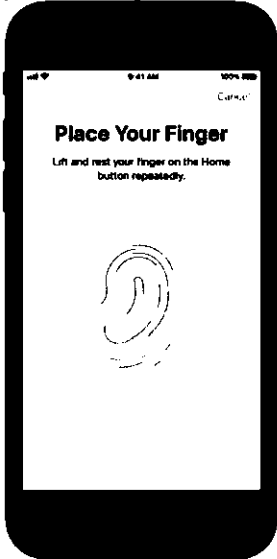
<u>Claim 10</u>	<u>Accused Instrumentalities</u>
	<p data-bbox="619 293 1044 370"><b>User Keybags</b></p> <p data-bbox="619 386 910 444">Background</p> <p data-bbox="619 500 1613 540">Sets of keys generated for each user to protect their data at rest</p> <p data-bbox="619 565 1710 605">Keys wrapped by master key derived from user passcode and SEP UID</p> <p data-bbox="619 630 1817 670">After 10 incorrect passcode entries, SEP will not process any further attempts</p> <p data-bbox="619 695 1698 735">Different policy associated with each keybag key—Usage, availability</p> <p data-bbox="612 760 753 792"><i>(Id., at 25.)</i></p> <p data-bbox="612 865 1889 1076">The random secret is issued to SKS. SKS is a Secure Key Service application which is located within the Secure Enclave on the SEP and is responsible for decrypting class keys. The random secret provided by SBIO is used to decrypt a master key ("4) decrypt master key"). The master key is concatenated with the UID of the SEP and thus class keys are decrypted and added to the SKS keyring ("5) decrypt class keys, add to keyring") for further use by the Secure Enclave. The decrypted class keys include, for example, the class key of class A.</p>
<p data-bbox="251 1122 540 1360">10c. a transmitter configured to emit a secure access signal conveying said information dependent upon said accessibility attribute;</p>	<p data-bbox="612 1122 1817 1187"><i>The Accused Instrumentalities include a transmitter configured to emit a secure access signal conveying information dependent upon said accessibility attribute.</i></p> <p data-bbox="612 1222 1710 1255">For example, the Secure Enclave emits a signal with ephemerally re-encrypted file keys:</p> <p data-bbox="612 1295 1859 1393">"sepOS can then use the ephemeral wrapping key to wrap file keys for use by the Application Processor file-system driver. When the file-system driver reads or writes a file, it sends the wrapped key to the AES Engine."</p>



<u>Claim 10</u>	<u>Accused Instrumentalities</u>
	<p>(Ex. A, Apple Platform Security, at 14.)</p> <p>"All wrapped file key handling occurs in the Secure Enclave; the file key is never directly exposed to the Application Processor. [...] When the Secure Enclave unwraps a file's keys, they're rewrapped with the ephemeral key and sent back to the Application Processor." (<i>Id.</i> at 85.)</p> <p>The signal with the ephemerally re-encrypted file keys is a secure signal because it comes from the Secure Enclave and thus from a secure environment. Furthermore, the signal is secure because the transmitted information is encrypted. The emitted file keys are encrypted with the ephemeral key:</p> <p>"All wrapped file key handling occurs in the Secure Enclave; the file key is never directly exposed to the Application Processor. At startup, the Secure Enclave negotiates an ephemeral key with the AES Engine. When the Secure Enclave unwraps a file's keys, they're rewrapped with the ephemeral key and sent back to the Application Processor." (<i>Id.</i>)</p> <div data-bbox="612 878 1902 1383" style="background-color: black; color: white; padding: 10px;"> <h2 style="margin: 0;">Filesystem Data Protection</h2> <h3 style="margin: 0;">Overview</h3> <p style="margin: 0;">File blocks are encrypted using AES-XTS with 128-bit keys</p> <p style="margin: 0;">Each file on the user partition is encrypted using a unique random key chosen by SEP</p> <p style="margin: 0;">Raw file keys are never exposed to the AP</p> <ul style="list-style-type: none"> <li style="margin: 0;">• Wrapped with a key from the user keybag for long-term storage</li> <li style="margin: 0;">• Wrapped with an ephemeral key while in use, bound to boot session</li> </ul> </div>

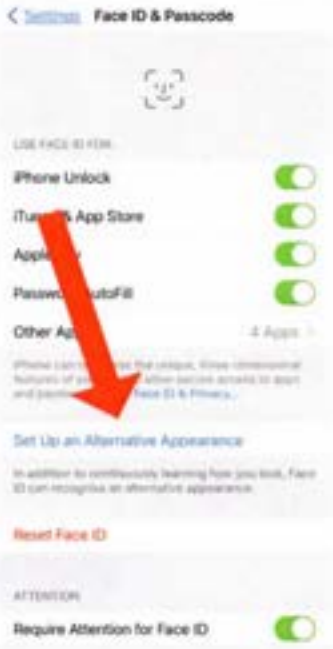
<u>Claim 10</u>	<u>Accused Instrumentalities</u>
	<p>(Ex. B, Behind the Scenes with iOS Security, at 29.)</p> <div data-bbox="612 349 1787 1003" style="background-color: black; color: white; padding: 10px;"> <h3 style="text-align: center;">Filesystem Data Protection</h3> <p>The diagram illustrates the process of filesystem data protection across four domains: User, Kernel, SEP (Secure Enclave Platform), and Hardware.          <ul style="list-style-type: none"> <li><b>User:</b> Initiates the process with the command <code>open("foo.txt", ...)</code>.</li> <li><b>Kernel:</b> <ol style="list-style-type: none"> <li>Fetches wrapped file keys from metadata (HFS).</li> <li>Communicates with the Key Store in the SEP.</li> <li>Communicates with the NVME Driver.</li> <li>Sends an IO command with an ephemerally wrapped file key to the Storage Controller.</li> </ol> </li> <li><b>SEP:</b> <ol style="list-style-type: none"> <li>Unwraps the file key using a keybag key.</li> <li>Wraps the file key using an ephemeral key and returns the ephemerally wrapped file key to the kernel.</li> </ol> </li> <li><b>Hardware:</b> <ul style="list-style-type: none"> <li>NAND storage holds the data.</li> <li>Storage Controller receives the ephemerally wrapped file key and sends cipher text to the NAND.</li> <li>An Ephemeral Key is established on boot.</li> </ul> </li> </ul> </p> </div> <p>(<i>Id.</i>, at 30.)</p> <p>The information transmitted by the emitted signal, i.e., the ephemerally re-encrypted file keys, is dependent on the availability attribute, i.e., the confirmation that a biometric "template match" exists. This confirmation is signaled by the issuance of the random secret (cf. step 3): Only if there is a confirmation of the match and the random secret is issued by the Touch ID or Face ID subsystem within the Secure Enclave, i.e. SBIO, the class key is available for re-encrypting the file keys.</p> <p>The re-encrypted file keys are therefore information which is emitted depending on the fact that the availability attribute has been emitted.</p>

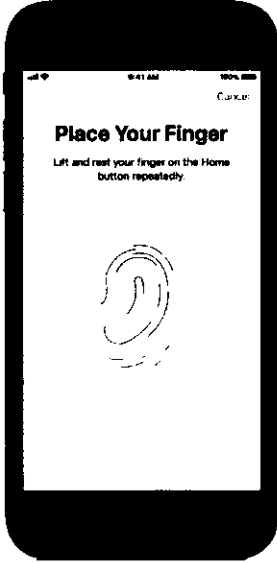
<u>Claim 10</u>	<u>Accused Instrumentalities</u>
10d. wherein the controller is further configured to:	<i>The Accused Instrumentalities include a controller that is configured to be used as set forth in elements 10d1, 10d2, and 10d3 below.</i>
10d1. receive a series of entries of the biometric signal, said series being characterised according to at least one of the number of said entries and a duration of each said entry;	<p><i>The Accused Instrumentalities include a transmitter sub-system controller configured to receive a series of entries of the biometric signal, said series being characterized according to at least one of the number of said entries and a duration of each said entry.</i></p> <p>More specifically, the Secure Enclave of the iPhone with the Secure Enclave Processor forms the means for receiving a series of entries of the biometric signal.</p> <p>"Apple's biometric security architecture relies on a strict separation of responsibilities between the biometric sensor and the Secure Enclave, and a secure connection between the two. The sensor captures the biometric image and securely transmits it to the Secure Enclave." (Ex. A, Apple Platform Security, at 19.)</p> <p><b>Touch ID</b></p> <p>When a finger is placed on the biometric sensor, the finger is scanned and the corresponding biometric signal entry is received by the Secure Enclave.</p> <p>"When the fingerprint sensor detects the touch of a finger, it triggers the advanced imaging array to scan the finger and sends the scan to the Secure Enclave." (<i>Id.</i>)</p> <p>To enroll a fingerprint in the database, the iPhone's fingerprint sensor records an entry of a biometric signal when the user places his finger on the sensor. This is done multiple times, resulting in a series of entries of such biometric signals.</p> <p>Receiving a series of entries of the biometric signal by repeatedly placing a finger on the Touch ID sensor will use Touch ID on iPhone.</p>

<u>Claim 10</u>	<u>Accused Instrumentalities</u>
	<p data-bbox="612 321 840 354"><b>Set up Touch ID</b></p> <p data-bbox="612 380 1825 412">Before you can set up Touch ID, you must first create a <u>code</u> for your device,* then follow these steps:</p> <ol data-bbox="661 415 1902 659" style="list-style-type: none"> <li data-bbox="661 415 1485 448">7. Make sure the Touch ID sensor and your finger are clean and dry.</li> <li data-bbox="697 464 1455 496">8. Tap Settings &gt; Touch ID &amp; Code, and then enter your code.</li> <li data-bbox="697 513 1872 578">9. Tap "Add fingerprint" and hold the device as you normally would when touching the Touch ID sensor.</li> <li data-bbox="697 594 1902 659">10. Touch the Touch ID sensor with one finger, but do not press. Keep your finger on the button until you feel a quick vibration or are prompted to lift your finger.</li> </ol>  <ol data-bbox="697 1235 1876 1300" style="list-style-type: none"> <li data-bbox="697 1235 1876 1300">11. Continue by raising and slowly lowering your finger over and over again, changing the position of your finger just a tiny bit at a time.</li> </ol>

<u>Claim 10</u>	<u>Accused Instrumentalities</u>
	<p>12. The next screen will ask you to change your finger position. Hold your device as you normally would when unlocking it. Touch the Touch ID sensor with the outer edges of your fingertip instead of the middle part as you would during the first scan.”</p> <p>(<a href="https://support.apple.com/en-us/HT201371">https://support.apple.com/en-us/HT201371</a>)</p> <p>Accordingly, the user is prompted to place his finger on the sensor several times, in particular in accordance with step 5. Each time the finger is placed on the sensor, a corresponding biometric entry is generated, i.e. a series of such entries. All these entries, which result from placing the same finger on the sensor, form a series.</p> <p><b>Face ID</b></p> <p>The means for receiving a series of entries of the biometric signal includes a Secure Neural Engine, which is protected by the Secure Enclave. The Secure Neural Engine transforms the series of entries of the biometric signal received by the Secure Enclave into a biometric signature ("mathematical representation").</p> <p>"After the TrueDepth camera confirms the presence of an attentive face, it projects and reads over 30,000 infrared dots to form a depth map of the face along with a 2D infrared image. This data is used to create <b>a sequence of 2D images and depth maps</b>, which are digitally signed and <b>sent to the Secure Enclave</b>. To counter both digital and physical spoofs, the TrueDepth camera randomizes the sequence of 2D images and depth map captures, and projects a device-specific random pattern. A portion of the <b>Secure Neural Engine-protected</b> within the Secure Enclave-transforms this data into a mathematical representation and compares that representation to the enrolled facial data. This enrolled facial data is itself a mathematical representation of the user's face captured across a variety of poses." (Ex. A, Apple Platform Security, at 20.)</p> <p>Each entry of the biometric signal thus contains a two-dimensional infrared image with 30,000 infrared points for capturing depth information. By continuously capturing such infrared images into a Face ID scan while the user moves his head into different poses, a series of entries of the biometric signal</p>


<u>Claim 10</u>	<u>Accused Instrumentalities</u>
	<p>results. Two such Face ID scans are required to generate a biometric signature of a single face, so that two series of entries of the biometric signal are received accordingly.</p> <p>Using Face ID on iPhone</p> <ol style="list-style-type: none"> <li>1. Tap Settings &gt; Face ID &amp; Code. Enter your code when prompted.</li> <li>2. Tap on "Configure Face ID".</li> <li>3. Hold the device in portrait mode in front of your face and tap "Let's go".</li> <li>4. Make sure your face is inside the frame and slowly move your head until the circle shown is completed. If you can't move your head, tap on "Options for operating aids".</li> <li>5. After performing the first Face ID scan, tap "Next".</li> <li>6. Again, slowly describe a circle with your head until it is completed.</li> <li>7. Tap "Done."</li> </ol> <p>(<a href="https://support.apple.com/en-us/HT208109">https://support.apple.com/en-us/HT208109</a>)</p> <p>The biometric signature of a single face is thus determined by two successive Face ID scans, each of which receives a series of entries of the biometric signal (compare steps 4. and 6. above).</p> <p>To register a second face, the iPhone offers a corresponding option in its settings. If the user selects the option "Set up an alternative appearance" as shown in the figure below on <a href="https://www.macworld.co.uk/how-to/second-face-id-3803421/">https://www.macworld.co.uk/how-to/second-face-id-3803421/</a>, a second face is registered by the iPhone in the same way as the first face.</p>


<u>Claim 10</u>	<u>Accused Instrumentalities</u>
	 <p>The series of entries of the biometric signal is identified on the iPhone by both the number and duration of each such entry.</p> <p><b>Touch ID</b></p> <p>According to step 5 of the instructions <a href="https://support.apple.com/en-us/HT201371">https://support.apple.com/en-us/HT201371</a>, for the enrollment of a single finger, the user has to repeatedly place the respective finger on the sensor and thus a number of entries in a row predetermined via the user guidance are captured by the iPhone. Each one of the entries must also be of a predetermined duration given to the user via the iPhone display, i.e. the user's finger must remain on the sensor for a predetermined duration for each entry of the biometric signal in order to capture the biometric signal during this time.</p>

<u>Claim 10</u>	<u>Accused Instrumentalities</u>
	<p>Receiving a series of entries of the biometric signal by repeatedly placing a finger on the Touch ID sensor will use Touch ID on iPhone and iPad.</p> <p><b>Set up Touch ID</b></p> <p>...</p> <p>4. Touch the Touch ID sensor with one finger, but do not press. Keep your finger on the button until you feel a quick vibration or are prompted to lift your finger.</p>  <p>5. Continue by raising and slowly lowering your finger over and over again, changing the position of your finger just a tiny bit at a time.</p> <p>6. The next screen will ask you to change your finger position. Hold your device as you normally would when unlocking it. Touch the Touch ID sensor with the outer edges of your fingertip instead of the middle part as you did during the first scan.</p> <p>(<a href="https://support.apple.com/en-us/HT201371">https://support.apple.com/en-us/HT201371</a>)</p>



<u>Claim 10</u>	<u>Accused Instrumentalities</u>
	<p>After placing a finger on the home button, a fingerprint appears on the display with red progress bars spreading along some of the papillary bars until the capture of the biometric entry in question is complete:</p> <div data-bbox="1115 386 1395 951" data-label="Image"> </div> <p>When the required duration is reached, the iPhone vibrates after an entry of the biometric signal is received or it issues a prompt to the user to lift the finger. The user then lifts the finger in question and replaces the same finger so that the iPhone receives a series of biometric signal entries of sufficient duration for that finger. The process is repeated for the same finger for as long as required according to the iPhone's user guidance.</p> <p>This is shown in the Apple You Tube video (32) How to set up Touch ID on your iPhone or iPad - Apple Support - YouTube (<a href="https://www.youtube.com/watch?v=xTZ2LALWZlg">https://www.youtube.com/watch?v=xTZ2LALWZlg</a>):</p>


<u>Claim 10</u>	<u>Accused Instrumentalities</u>
	 <p>Both the number of entries, i.e. the number of repetitions for placing the finger on the screen, and their respective duration are specified by the iPhone via the user guidance.</p>

<u>Claim 10</u>	<u>Accused Instrumentalities</u>
	<p><b>Face ID</b></p> <p>The user moves his face in front of the camera to strike different poses, and the camera system with image sensor continuously captures a large number of biometric entries, i.e. here the 2D images with depth information, in a row.</p> <p>"This enrolled facial data is itself a mathematical representation of the user's face captured across a variety of poses." (Ex. A, Apple Platform Security, at 20.)</p> <p>The sufficient duration of an entry for a pose, i.e. an angular position of the head specified via the user interface of the iPhone, is indicated to the user by the transformation of a gray line into a green line:</p>  <p>(Individual images taken from: <a href="https://support.apple.com/en-us/HT208109">https://support.apple.com/en-us/HT208109</a>)</p>
<p>10d2. map said series into an instruction; and</p>	<p><i>The Accused Instrumentalities include a transmitter sub-system controller configured to map said series into an instruction.</i></p>

<u>Claim 10</u>	<u>Accused Instrumentalities</u>
	<p>More specifically, the Secure Enclave of the iPhone contains means to assign the received row to an instruction: The Secure Enclave, after receiving the full set of entries of the biometric signal, assigns this set to an instruction for processing, encrypting and storing the biometric signature ("Touch ID and Face ID template data").</p> <p>"The sensor captures the biometric image and securely transmits it to the Secure Enclave. During enrollment, the Secure Enclave processes, encrypts, and stores the corresponding Touch ID and Face ID template data." (Ex. A, Apple Platform Security, at 19.)</p> <p>To carry out this instruction, the Secure Enclave has its own processor: "The Secure Enclave Processor provides the main computing power for the Secure Enclave." (<i>Id.</i>, at 10.)</p> <p><b>Touch ID</b></p> <p>The instruction here involves the processing of under-the-skin fingerprint characteristics and their encrypted storage.</p> <p>"The analysis uses subdermal ridge flow angle mapping, a lossy process that discards "finger minutiae data" that would be required to reconstruct the user's actual fingerprint. During enrollment, the resulting map of nodes is stored in an encrypted format that can be read only by the Secure Enclave as a template to compare against for future matches, but without any identity information." (<i>Id.</i>, at 19.)</p> <p><b>Face ID</b></p> <p>The instruction involves the transformation of the set of entries of the biometric signal captured via the Face ID scans into a mathematical representation, i.e. the biometric signature of the face in question by the Secure Neural Engine of the Secure Enclave, as well as its encryption and storage.</p>

<u>Claim 10</u>	<u>Accused Instrumentalities</u>
	<p>"A portion of the Secure Neural Engine-protected within the Secure Enclave-transforms this data into a mathematical representation and compares that representation to the enrolled facial data. This enrolled facial data is itself a mathematical representation of the user's face captured across a variety of poses." <i>(Id.</i>, at 20.)</p> <p>"Face ID data, including mathematical representations of a user's face, is encrypted and available only to the Secure Enclave. This data never leaves the device. It's not sent to Apple, nor is it included in device backups. The following Face ID data is saved, encrypted only for use by the Secure Enclave, during normal operation:</p> <ul style="list-style-type: none"> <li>• The mathematical representations of a user's face calculated during enrollment</li> <li>• ..."</li> </ul> <p><i>(Id.</i>, at 23.)</p>
<p>10d3. populate the database according to the instruction, wherein the controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing device.</p>	<p><b><i>The Accused Instrumentalities include a transmitter sub-system controller configured to populate the database according to the instruction.</i></b></p> <p>More specifically, the Secure Enclave stores the biometric signature, i.e. the encrypted mathematical representation of the fingerprint or face, in the database 105, i.e. the "secure nonvolatile storage":</p> <p>"The secure nonvolatile storage is used for all anti-replay services in the Secure Enclave. Anti-replay services on the Secure Enclave are used for revocation of data over events that mark anti-replay boundaries including, but not limited to, the following:</p> <ul style="list-style-type: none"> <li>• ...</li> <li>• ...</li> <li>• Adding or removing a Touch ID fingerprint or Face ID face".</li> </ul> <p>(Ex. A, Apple Platform Security, at 16.)</p> <p>"During enrollment, the Secure Enclave processes, encrypts, and stores the corresponding Touch ID and Face ID template data." <i>(Id.</i>, at 19.)</p>


<u>Claim 10</u>	<u>Accused Instrumentalities</u>
	<p><b>Touch ID</b></p> <p>"During enrollment, the resulting map of nodes is stored in an encrypted format that can be read only by the Secure Enclave as a template to compare against for future matches...."  <i>(Id.)</i></p> <p><b>Face ID</b></p> <p>The following Face ID data is saved, encrypted only for use by the Secure Enclave, during normal operation:</p> <ul style="list-style-type: none"> <li>• The mathematical representations of a user's face calculated during enrollment".  <i>(Id., at 23.)</i></li> </ul> <p>More specifically, the controlled item is a locking mechanism of the door lock of the user's home. The Accused Instrumentalities are configured to provide secure access to the user's home via Yale Smart Locks when the user provides biometric signal to the Accused Instrumentalities via Touch ID or Face ID.</p> <p>"When the "Secure Remote Access" feature is turned on, the app will use your phone's built-in authentication tools to prompt fingerprint or facial recognition before you can unlock or lock your home remotely (note: if your phone does not have these features, it will prompt you to use your PIN code). This further ensures that your door is only operated by the right people at the time you intend for it."  <i>(https://us.yalehome.com/en/yale-news/blog/latest-blog-posts/introducing-biometric-verification-for-august-and-yale-locks1/)</i></p>


<u>Claim 10</u>	<u>Accused Instrumentalities</u>
	 <p>The screenshot shows a mobile application interface for Yale. At the top, there is a yellow circular logo with the word "Yale" in black. To the left of the logo is a hamburger menu icon and the word "Open". To the right is a magnifying glass search icon. Below the header, the text "Introducing Biometric Verification for August and Yale Locks" is displayed in a bold, black font. Underneath the text is a photograph of a hand holding a smartphone. The phone's screen displays a biometric verification interface with a red circular camera viewfinder and a black square in the center containing a white Yale logo. Below the photograph, the URL <a href="https://us.yalehome.com/en/yale-news/blog/latest-blog-posts/introducing-biometric-verification-for-august-and-yale-locks1/">(https://us.yalehome.com/en/yale-news/blog/latest-blog-posts/introducing-biometric-verification-for-august-and-yale-locks1/)</a> is provided.</p>

<u>Claim 10</u>	<u>Accused Instrumentalities</u>
	 <p>(<a href="https://www.apple.com/shop/product/HPAR2ZM/A/yale-assure-lock-sl-touchscreen-deadbolt-black">https://www.apple.com/shop/product/HPAR2ZM/A/yale-assure-lock-sl-touchscreen-deadbolt-black</a>)</p>

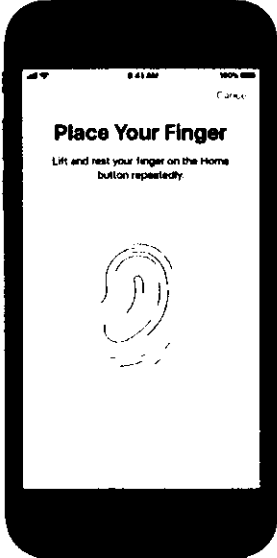


<u>Claim 11</u>	<u>Accused Instrumentalities</u>
<p>11. A method for providing secure access to a controlled item in a system comprising a database of biometric signatures, a transmitter sub-system comprising a biometric sensor configured to receive a biometric signal, and a transmitter configured to emit a secure access signal capable of granting access to the controlled item, and a receiver sub-system comprising a receiver sub-system controller configured to receive the transmitted secure access signal, and provide conditional access to the controlled item dependent upon information in said secure access signal, the method comprising:</p>	<p><i>To the extent that the preamble is deemed to be a limitation, the Accused Instrumentalities are configured to use a method in accordance with this claim.</i></p> <p>More specifically, the controlled item is a locking mechanism of the door lock of the user's home. The Accused Instrumentalities are configured to provide secure access to the user's home via Yale Smart Locks when the user provides biometric signal to the Accused Instrumentalities via Touch ID or Face ID.</p> <p>"When the "Secure Remote Access" feature is turned on, the app will use your phone's built-in authentication tools to prompt fingerprint or facial recognition before you can unlock or lock your home remotely (note: if your phone does not have these features, it will prompt you to use your PIN code). This further ensures that your door is only operated by the right people at the time you intend for it."</p> <p>(<a href="https://us.yalehome.com/en/yale-news/blog/latest-blog-posts/introducing-biometric-verification-for-august-and-yale-locks1/">https://us.yalehome.com/en/yale-news/blog/latest-blog-posts/introducing-biometric-verification-for-august-and-yale-locks1/</a>)</p>

<u>Claim 11</u>	<u>Accused Instrumentalities</u>
	 <p data-bbox="634 1133 1868 1203">(https://us.yalehome.com/en/yale-news/blog/latest-blog-posts/introducing-biometric-verification-for-august-and-yale-locks1/)</p>

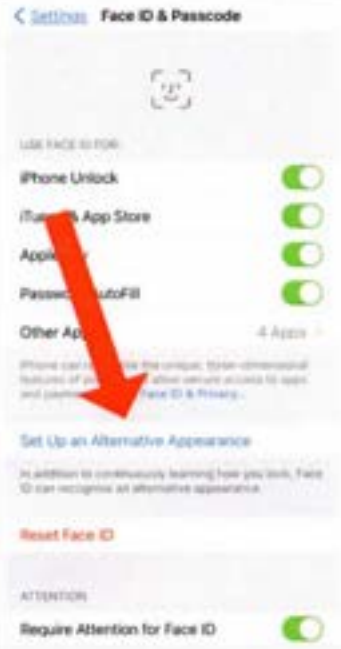
<u>Claim 11</u>	<u>Accused Instrumentalities</u>
	 <p data-bbox="612 1078 1874 1110">(https://www.apple.com/shop/product/HPAR2ZM/A/yale-assure-lock-sl-touchscreen-deadbolt-black)</p>
<p>11a. populating the database of biometric signatures by:</p>	<p><i>The Accused Instrumentalities are configured to populate the database of biometric signatures as set forth in elements 11a1, 11a2, and 11a3 below.</i></p>

<u>Claim 11</u>	<u>Accused Instrumentalities</u>
11a1. receiving a series of entries of the biometric signal;	<p><i>The Accused Instrumentalities are configured to populate the database of biometric signatures by: receiving a series of entries of the biometric signal.</i></p> <p>More specifically, the Secure Enclave of the iPhone with the Secure Enclave Processor forms the means for receiving a series of entries of the biometric signal.</p> <p>"Apple's biometric security architecture relies on a strict separation of responsibilities between the biometric sensor and the Secure Enclave, and a secure connection between the two. The sensor captures the biometric image and securely transmits it to the Secure Enclave." (Ex. A, Apple Platform Security, at 19.)</p> <p><b>Touch ID</b></p> <p>When a finger is placed on the biometric sensor, the finger is scanned and the corresponding biometric signal entry is received by the Secure Enclave.</p> <p>"When the fingerprint sensor detects the touch of a finger, it triggers the advanced imaging array to scan the finger and sends the scan to the Secure Enclave." (Ex. A, Apple Platform Security, at 19.)</p> <p>To enroll a fingerprint in the database, the iPhone's fingerprint sensor records an entry of a biometric signal when the user places his finger on the sensor. This is done multiple times, resulting in a series of entries of such biometric signals.</p> <p>Receiving a series of entries of the biometric signal by repeatedly placing a finger on the Touch ID sensor will use Touch ID on iPhone.</p> <p><b>Set up Touch ID</b></p> <p>Before you can set up Touch ID, you must first create a <a href="#">code</a> for your device,* then follow these steps:</p> <ol style="list-style-type: none"> <li>1. Make sure the Touch ID sensor and your finger are clean and dry.</li> </ol>

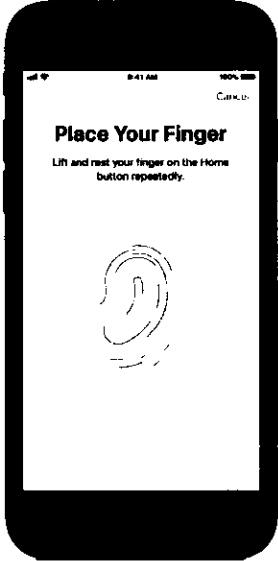
<u>Claim 11</u>	<u>Accused Instrumentalities</u>
	<ol style="list-style-type: none"><li>2. Tap Settings &gt; Touch ID &amp; Code, and then enter your code.</li><li>3. Tap "Add fingerprint" and hold the device as you normally would when touching the Touch ID sensor.</li><li>4. Touch the Touch ID sensor with one finger, but do not press. Keep your finger on the button until you feel a quick vibration or are prompted to lift your finger.</li></ol>  <ol style="list-style-type: none"><li>5. Continue by raising and slowly lowering your finger over and over again, changing the position of your finger just a tiny bit at a time.</li><li>6. The next screen will ask you to change your finger position. Hold your device as you normally would when unlocking it. Touch the Touch ID sensor with the outer edges of your fingertip instead of the middle part as you would during the first scan.”</li></ol> <p>(<a href="https://support.apple.com/en-us/HT201371">https://support.apple.com/en-us/HT201371</a>)</p>

<u>Claim 11</u>	<u>Accused Instrumentalities</u>
	<p>Accordingly, the user is prompted to place his finger on the sensor several times, in particular in accordance with step 5. Each time the finger is placed on the sensor, a corresponding biometric entry is generated, i.e. a series of such entries. All these entries, which result from placing the same finger on the sensor, form a series.</p> <p><b>Face ID</b></p> <p>The means for receiving a series of entries of the biometric signal includes a Secure Neural Engine, which is protected by the Secure Enclave. The Secure Neural Engine transforms the series of entries of the biometric signal received by the Secure Enclave into a biometric signature ("mathematical representation").</p> <p>"After the TrueDepth camera confirms the presence of an attentive face, it projects and reads over 30,000 infrared dots to form a depth map of the face along with a 2D infrared image. This data is used to create a <b>sequence of 2D images and depth maps</b>, which are digitally signed and <b>sent to the Secure Enclave</b>. To counter both digital and physical spoofs, the TrueDepth camera randomizes the sequence of 2D images and depth map captures, and projects a device-specific random pattern. A portion of the <b>Secure Neural Engine-protected</b> within the Secure Enclave-transforms this data into a mathematical representation and compares that representation to the enrolled facial data. This enrolled facial data is itself a mathematical representation of the user's face captured across a variety of poses." (emphasis added) (Ex. A, Apple Platform Security, at 20.)</p> <p>Each entry of the biometric signal thus contains a two-dimensional infrared image with 30,000 infrared points for capturing depth information. By continuously capturing such infrared images into a Face ID scan while the user moves his head into different poses, a series of entries of the biometric signal results. Two such Face ID scans are required to generate a biometric signature of a single face, so that two series of entries of the biometric signal are received accordingly.</p> <p>Using Face ID on iPhone or iPad Pro - Apple Support</p>

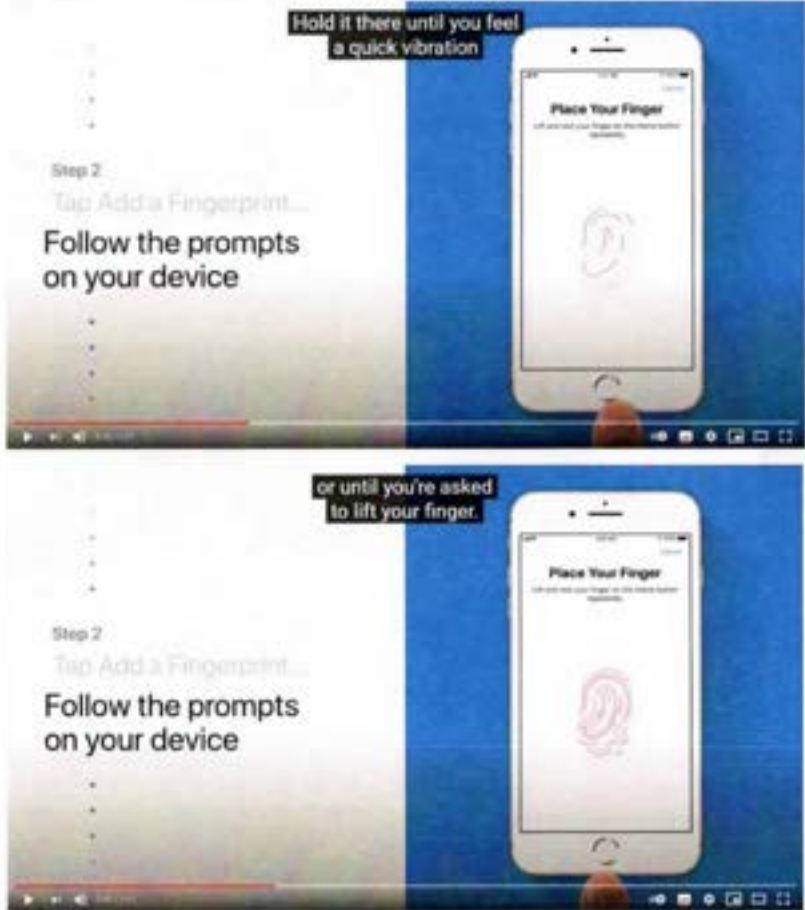
<u>Claim 11</u>	<u>Accused Instrumentalities</u>
	<p>Configure Face ID</p> <p>Before configuring Face ID, make sure that neither the TrueDepth camera nor your face are covered by anything....</p> <p>Follow the steps below to configure Face ID:</p> <ol style="list-style-type: none"> <li>1. Tap Settings &gt; Face ID &amp; Code. Enter your code when prompted.</li> <li>2. Tap on "Configure Face ID".</li> <li>3. Hold the device in portrait mode in front of your face and tap "Let's go".</li> <li>4. Make sure your face is inside the frame and slowly move your head until the circle shown is completed. If you can't move your head, tap on "Options for operating aids".</li> <li>5. After performing the first Face ID scan, tap "Next".</li> <li>6. Again, slowly describe a circle with your head until it is completed.</li> <li>7. Tap "Done."</li> </ol> <p>(<a href="https://support.apple.com/en-us/HT208109">https://support.apple.com/en-us/HT208109</a>)</p> <p>The biometric signature of a single face is thus determined by two successive Face ID scans, each of which receives a series of entries of the biometric signal (compare steps 4. and 6. above).</p> <p>To register a second face, the iPhone offers a corresponding option in its settings. If the user selects the option "Set up an alternative appearance" as shown in the figure below on <a href="https://www.macworld.co.uk/how-to/second-face-id-3803421/">https://www.macworld.co.uk/how-to/second-face-id-3803421/</a>, a second face is registered by the iPhone in the same way as the first face.</p>


<u>Claim 11</u>	<u>Accused Instrumentalities</u>
	 <p>The series of entries of the biometric signal is identified on the iPhone by both the number and duration of each such entry.</p> <p><b>Touch ID</b></p> <p>According to step 5 of the instructions <a href="https://support.apple.com/en-us/HT201371">https://support.apple.com/en-us/HT201371</a>, for the enrollment of a single finger, the user has to repeatedly place the respective finger on the sensor and thus a number of entries in a row predetermined via the user guidance are captured by the iPhone. Each one of the entries must also be of a predetermined duration given to the user via the iPhone display, i.e. the user's finger must remain on the sensor for a predetermined duration for each entry of the biometric signal in order to capture the biometric signal during this time.</p>



<u>Claim 11</u>	<u>Accused Instrumentalities</u>
	<p>Receiving a series of entries of the biometric signal by repeatedly placing a finger on the Touch ID sensor will use Touch ID on iPhone.</p> <p><b>Set up Touch ID</b></p> <p>...</p> <p>4. Touch the Touch ID sensor with one finger, but do not press. Keep your finger on the button until you feel a quick vibration or are prompted to lift your finger.</p>  <p>5. Continue by raising and slowly lowering your finger over and over again, changing the position of your finger just a tiny bit at a time.</p> <p>6. The next screen will ask you to change your finger position. Hold your device as you normally would when unlocking it. Touch the Touch ID sensor with the outer edges of your fingertip instead of the middle part as you did during the first scan.</p> <p>(<a href="https://support.apple.com/en-us/HT201371">https://support.apple.com/en-us/HT201371</a>)</p>

<u>Claim 11</u>	<u>Accused Instrumentalities</u>
	<p>After placing a finger on the home button, a fingerprint appears on the display with red progress bars spreading along some of the papillary bars until the capture of the biometric entry in question is complete:</p> <div data-bbox="1115 431 1391 992" data-label="Image"> </div> <p>When the required duration is reached, the iPhone vibrates after an entry of the biometric signal is received or it issues a prompt to the user to lift the finger. The user then lifts the finger in question and replaces the same finger so that the iPhone receives a series of biometric signal entries of sufficient duration for that finger. The process is repeated for the same finger for as long as required according to the iPhone's user guidance.</p> <p>This is shown in the Apple YouTube video (32) How to set up Touch ID on your iPhone or iPad - Apple Support - YouTube (<a href="https://www.youtube.com/watch?v=xTZ2LALWZlg">https://www.youtube.com/watch?v=xTZ2LALWZlg</a>):</p>

<u>Claim 11</u>	<u>Accused Instrumentalities</u>
	 <p>Both the number of entries, i.e. the number of repetitions for placing the finger on the screen, and their respective duration are specified by the iPhone via the user guidance.</p>

<u>Claim 11</u>	<u>Accused Instrumentalities</u>
	<p><b>Face ID</b></p> <p>The user moves his face in front of the camera to strike different poses, and the camera system with image sensor continuously captures a large number of biometric entries, i.e. here the 2D images with depth information, in a row.</p> <p>"This enrolled facial data is itself a mathematical representation of the user's face captured across a variety of poses." (Ex. A, Apple Platform Security, at 20.)</p> <p>The sufficient duration of an entry for a pose, i.e. an angular position of the head specified via the user interface of the iPhone, is indicated to the user by the transformation of a gray line into a green line:</p>  <p>(Individual images taken from: <a href="https://support.apple.com/en-us/HT208109">https://support.apple.com/en-us/HT208109</a>)</p>

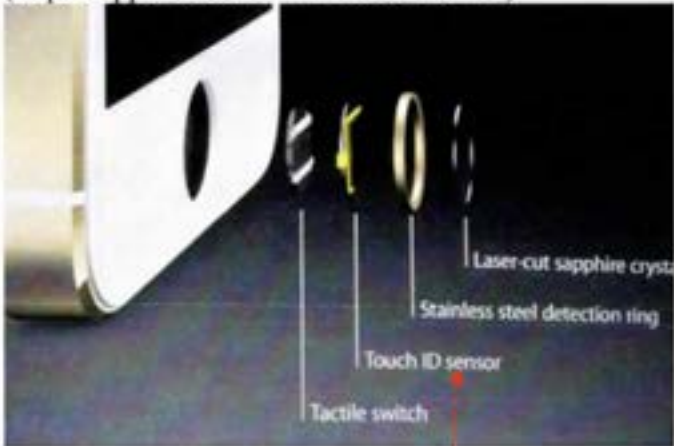
<u>Claim 11</u>	<u>Accused Instrumentalities</u>
<p>11a2. determining at least one of the number of said entries and a duration of each said entry;</p>	<p><b><i>The Accused instrumentalities are configured to populate the database of biometric signatures by: determining at least one of the number of said entries and a duration of each said entry.</i></b></p> <p>More specifically, as discussed above, both Face ID and Touch ID require a specific number of entries to enroll a Touch ID or Face ID. The Accused Instrumentalities must determine that the specific number of entries have been input. Likewise, while not necessary for the claim, upon information and belief, the Accused Instrumentalities determine that each input of either facial or fingerprint data is of a sufficient duration. Again, when setting up Touch ID in the Accused Instrumentalities, the users are required to touch the home button with their finger several times for a certain duration. Similarly, the users need to scan their face twice, and each scan requires the users to move their head in a circle for a certain duration for Face ID.</p> <p>Touch ID: Register a fingerprint for Apple Touch ID by the user tapping a finger several times on the home button to record the fingerprint data. (<a href="https://video.search.yahoo.com/yhs/search?fr=yhs-pty-pty_converter&amp;hsimp=yhs-pty_converter&amp;hspart=pty&amp;p=registering+fingerprint+apple+touch+id+on+screen+instructions#id=1&amp;vid=156de65ae06ca453643009fc0ea9cf79&amp;action=click">https://video.search.yahoo.com/yhs/search?fr=yhs-pty-pty_converter&amp;hsimp=yhs-pty_converter&amp;hspart=pty&amp;p=registering+fingerprint+apple+touch+id+on+screen+instructions#id=1&amp;vid=156de65ae06ca453643009fc0ea9cf79&amp;action=click</a>)</p> <p>Touch ID: The user's finger must remain on the home button long enough for the data to be recorded. "Touch the Touch ID sensor with your finger, but don't press it. Hold it there until you feel a quick vibration, or until you're asked to lift your finger." "Continue to lift and rest your finger slowly, making small adjustments to the position of your finger each time." (<a href="https://support.apple.com/en-au/HT201371">https://support.apple.com/en-au/HT201371</a>)</p> <p>Touch ID: "you shouldn't tap too quickly or move your finger around" (<a href="https://support.apple.com/en-us/HT207537">https://support.apple.com/en-us/HT207537</a>)</p> <p>Face ID: Setting up Face ID requires two scans of the user's face. Each scan asks users to move their head slowly in a circle to register different angles of the user's face. (<a href="https://www.imore.com/how-set-face-id-iphone">https://www.imore.com/how-set-face-id-iphone</a>)</p>

<u>Claim 11</u>	<u>Accused Instrumentalities</u>
<p>11a3. mapping said series into an instruction; and</p>	<p><i>The Accused Instrumentalities include a transmitter sub-system controller configured to map said series into an instruction.</i></p> <p>More specifically, the Secure Enclave of the iPhone contains means to assign the received row to an instruction: The Secure Enclave, after receiving the full set of entries of the biometric signal, assigns this set to an instruction for processing, encrypting and storing the biometric signature ("Touch ID and Face ID template data").</p> <p>"The sensor captures the biometric image and securely transmits it to the Secure Enclave. During enrollment, the Secure Enclave processes, encrypts, and stores the corresponding Touch ID and Face ID template data." (Ex. A, Apple Platform Security, at 19.)</p> <p>To carry out this instruction, the Secure Enclave has its own processor: "The Secure Enclave Processor provides the main computing power for the Secure Enclave." (<i>Id.</i>, at 10.)</p> <p><b>Touch ID</b></p> <p>The instruction here involves the processing of under-the-skin fingerprint characteristics and their encrypted storage.</p> <p>"The analysis uses subdermal ridge flow angle mapping, a lossy process that discards "finger minutiae data" that would be required to reconstruct the user's actual fingerprint. During enrollment, the resulting map of nodes is stored in an encrypted format that can be read only by the Secure Enclave as a template to compare against for future matches, but without any identity information." (<i>Id.</i>, at 19.)</p> <p><b>Face ID</b></p>


<u>Claim 11</u>	<u>Accused Instrumentalities</u>
	<p>The instruction involves the transformation of the set of entries of the biometric signal captured via the Face ID scans into a mathematical representation, i.e. the biometric signature of the face in question by the Secure Neural Engine of the Secure Enclave, as well as its encryption and storage.</p> <p>"A portion of the Secure Neural Engine-protected within the Secure Enclave-transforms this data into a mathematical representation and compares that representation to the enrolled facial data. This enrolled facial data is itself a mathematical representation of the user's face captured across a variety of poses. "<i>(Id., at 20.)</i></p> <p>"Face ID data, including mathematical representations of a user's face, is encrypted and available only to the Secure Enclave. This data never leaves the device. It's not sent to Apple, nor is it included in device backups. The following Face ID data is saved, encrypted only for use by the Secure Enclave, during normal operation:</p> <ul style="list-style-type: none"> <li>• The mathematical representations of a user's face calculated during enrollment</li> <li>• ..."</li> </ul> <p><i>(Id., at 23.)</i></p>
<p>11a4. populating the database according to the instruction;</p>	<p><b><i>The Accused Instrumentalities include a transmitter sub-system controller configured to populate the database according to the instruction.</i></b></p> <p>More specifically, the Secure Enclave stores the biometric signature, i.e. the encrypted mathematical representation of the fingerprint or face, in the database 105, i.e. the "secure nonvolatile storage":</p> <p>"The secure nonvolatile storage is used for all anti-replay services in the Secure Enclave. Anti-replay services on the Secure Enclave are used for revocation of data over events that mark anti-replay boundaries including, but not limited to, the following:</p> <ul style="list-style-type: none"> <li>• ...</li> <li>• ...</li> <li>• Adding or removing a Touch ID fingerprint or Face ID face".</li> </ul> <p><i>(Ex. A, Apple Platform Security, at 16.)</i></p>

<u>Claim 11</u>	<u>Accused Instrumentalities</u>
	<p>"During enrollment, the Secure Enclave processes, encrypts, and stores the corresponding Touch ID and Face ID template data." (<i>Id.</i>, at 19.)</p> <p><b>Touch ID</b></p> <p>"During enrollment, the resulting map of nodes is stored in an encrypted format that can be read only by the Secure Enclave as a template to compare against for future matches...." (<i>Id.</i>)</p> <p><b>Face ID</b></p> <p>The following Face ID data is saved, encrypted only for use by the Secure Enclave, during normal operation:</p> <ul style="list-style-type: none"> <li>• The mathematical representations of a user's face calculated during enrollment".</li> </ul> <p>(<i>Id.</i>, at 23.)</p>
11b. receiving the biometric signal;	<p><b><i>The Accused Instrumentalities include a biometric sensor configured to receive the biometric signal.</i></b></p> <p>More specifically, the iPhone has at least one biometric sensor for capturing a fingerprint or a face (Touch ID and/or Face ID), namely a Touch ID sensor and a camera system with image sensor, respectively.</p> <p><b>Touch ID</b></p> <p>"Apple devices with a Touch ID sensor can be unlocked using a fingerprint." (Ex. A, Apple Platform Security, at 19.)</p> <p>"Touch ID is the fingerprint sensing system that makes secure access to supported Apple devices faster and easier. This technology reads fingerprint data from any angle and learns more about a user's fingerprint over time, with the <b>sensor</b> continuing to expand the fingerprint map as additional overlapping nodes are identified with each use."</p>



<u>Claim 11</u>	<u>Accused Instrumentalities</u>
	<p>(<i>Id.</i>)</p> <p>"When the fingerprint sensor detects the touch of a finger, it triggers the advanced imaging array to scan the finger and sends the scan to the Secure Enclave."  (<i>Id.</i>)</p> <p>The biometric sensor for Touch ID is located below the home button:</p> <p>"The Home button is a stack of different materials, capped with a sapphire crystal lens. The surrounding stainless-steel ring works as a ground and detects the user's finger. This action activates a capacitive touch sensor installed underneath the cover: A CMOS chip with small capacitors."  (<a href="https://appleinsider.com/inside/touch-id">https://appleinsider.com/inside/touch-id</a>)</p>  <p style="text-align: center;">Biometric sensor 121</p> <p>"Where is the Touch ID sensor located?"</p>

<u>Claim 11</u>	<u>Accused Instrumentalities</u>
	<p>The Touch ID sensor is located either in the home button or - on the iPad Air (4th generation) - in the top button.</p> <p>(<a href="https://support.apple.com/en-us/HT201371">https://support.apple.com/en-us/HT201371</a>)</p> <p>The image sensor captures an 88-by-88-pixel, 500 PPI raster scan:</p> <p>"The 88-by-88-pixel, 500-ppi raster scan is temporarily stored in encrypted memory within the Secure Enclave while being vectorized for analysis, and then it's discarded. The analysis utilizes subdermal ridge flow angle mapping, which is a lossy process that discards minutia data that would be required to reconstruct the user's actual fingerprint. The resulting map of nodes is stored without any identity information in an encrypted format that can only be read by the Secure Enclave, and is never sent to Apple or backed up to iCloud or iTunes. "</p> <p>(Ex. C, iOS Security white paper, at 8.)</p> <p><b>Face ID</b></p> <p>The biometric sensor for facial biometrics is a camera system ("TrueDepth camera system") with an image sensor.</p> <p>"With a simple glance, Face ID securely unlocks supported Apple devices. It provides intuitive and secure authentication enabled by the TrueDepth camera system, which uses advanced technologies to accurately map the geometry of a user's face. "</p> <p>(Ex. A, Apple Platform Security, at 20.)</p> <p>To receive a biometric signal, the camera system with image sensor reads over 30,000 infrared points to capture depth information along with a two-dimensional infrared image.</p> <p>"After the TrueDepth camera confirms the presence of an attentive face, it projects and <b>reads over 30,000 infrared dots to form a depth map of the face along with a 2D infrared image.</b> This data is</p>

<u>Claim 11</u>	<u>Accused Instrumentalities</u>
	<p>used to <b>create a sequence of 2D images and depth maps</b>, which are digitally signed and sent to the Secure Enclave. To counter both digital and physical spoofs, the TrueDepth camera randomizes the sequence of 2D images and depth map captures, and projects a device-specific random pattern. A portion of the Secure Neural Engine-protected within the Secure Enclave-transforms this data into a mathematical representation and compares that representation to the enrolled facial data. This enrolled facial data is itself a mathematical representation of the user's face captured across a variety of poses." (<i>Id.</i>, at 20.)</p> <p>The camera system includes a biometric image sensor, namely a "CMOS image" sensor from Sony, to perform facial biometrics:</p>  <p>(<a href="https://appleinsider.com/articles/17/09/09/inner-workings-of-apples-face-id-camera-detailed-in-report">https://appleinsider.com/articles/17/09/09/inner-workings-of-apples-face-id-camera-detailed-in-report</a>)</p>

<u>Claim 11</u>	<u>Accused Instrumentalities</u>
<p>11c. matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute;</p>	<p><i>The Accused Instrumentalities include a transmitter controller configured to emit a secure access signal conveying information dependent upon said accessibility attribute.</i></p> <p>More specifically, the iPhone's System on Chip (SOC), i.e. the Secure Enclave with its Secure Enclave Processor (SEP) or a Secure Neural Engine contained therein, is a means (103) to check a match of the biometric signal with elements of the biometric signature database.</p> <p>"The <i>Secure Enclave</i> is a system on chip (SoC) that is included on all recent iPhone, ... devices" (Ex. A, Apple Platform Security, at 7.)</p> <p>"During <b>matching</b>, the Secure Enclave <b>compares</b> incoming data from the biometric sensor against the stored templates <b>to determine whether to unlock the device</b> or respond that a match is valid (for Apple Pay, in-app, and other uses of Touch ID and Face ID). " (<i>Id.</i>, at 19.)</p> <p>The biometric signal received from the biometric sensor ("incoming data from the biometric sensor") is thus checked by the Secure Enclave and its SEP with the elements of the database of biometric signatures 105, i.e. the "stored templates", for the presence of a match.</p> <p>For Touch ID, the Secure Enclave match verification is performed as follows:</p> <p>"The Secure Enclave is responsible for processing fingerprint data from the Touch ID sensor, determining if there is a match against registered fingerprints, and then enabling access or purchases on behalf of the user ..." (Ex. C, iOS Security white paper, at 7.)</p> <p>"During enrollment, the resulting map of nodes is stored in an encrypted format that can be read only by the Secure Enclave as a template to compare against for future matches...." (Ex. A, Apple Platform Security, at 19.)</p>

<u>Claim 11</u>	<u>Accused Instrumentalities</u>
	<p>"Touch ID can read multiple fingerprints, and it can read fingerprints in 360-degrees of orientation. It then creates a mathematical representation of your fingerprint and compares this to your enrolled fingerprint data to identify a match and unlock your device. " (<a href="https://support.apple.com/en-us/HT204587">https://support.apple.com/en-us/HT204587</a>)</p> <p>"Touch ID can read multiple fingerprints and recognize fingerprints at any orientation of the finger. The system then creates a mathematical representation of your fingerprint and compares it to the registered fingerprint data to determine a match and unlock your device." (<a href="https://support.apple.com/de-de/HT204587">https://support.apple.com/de-de/HT204587</a>)</p> <p>For <b>Face ID</b>, the Secure Enclave has a neural network protected by it, i.e., a Secure Neural Engine, which is used to verify the match:</p> <p>"Face ID uses neural networks for determining attention, <b>matching</b>, and antispooofing, so a user can unlock their phone with a glance." (Ex. A, Apple Platform Security, at 20.)</p> <p>"A portion of the Secure Neural Engine-protected within the Secure Enclave-transforms this data into a mathematical representation and compares that representation to the enrolled facial data. This enrolled facial data is itself a mathematical representation of the user's face captured across a variety of poses." (<i>Id.</i>).</p> <p>"Facial matching security Facial matching is performed within the Secure Enclave using neural networks trained specifically for that purpose... Face ID data, including mathematical representations of a user's face, is encrypted and available only to the Secure Enclave. This data never leaves the device." (<i>Id.</i> at 23.)</p> <p>When the Secure Enclave, or more precisely the Touch ID or Face ID subsystem within the Secure Enclave, has determined that a match exists, an accessibility attribute is issued by the corresponding</p>

<u>Claim 11</u>	<u>Accused Instrumentalities</u>
	<p>Touch ID or Face ID subsystem. This Touch ID or Face ID subsystem is also referred to as the SBIO. The accessibility attribute confirms that there is a match and that the iPhone is to be unlocked ("... determine whether to unlock the device ...").</p> <p>This confirmation of the match is signaled by the SBIO by issuing a random secret to which only the Touch ID or Face ID subsystem within the Secure Enclave has access:</p> <p>"During matching, the Secure Enclave compares incoming data from the biometric sensor against the stored templates to determine whether to unlock the device [...]." (<i>Id.</i> at 19.)</p> <p>"Uses for Touch ID and Face ID</p> <p><b>Unlocking a device or user account</b></p> <p>[...] <b>keys for the highest class of Data Protection-which are held in the Secure Enclave [...].</b></p> <p>With Touch ID or Face ID enabled, the keys aren't discarded when the device or account locks; instead, <b>they're wrapped with a key that's given to the Touch ID or Face ID subsystem inside the Secure Enclave.</b> When a user attempts to unlock the device or account, <b>if the device detects a successful match, it provides the key for unwrapping the Data Protection keys,</b> and the device or account is unlocked. This process provides additional protection by requiring cooperation between the Data Protection and Touch ID or Face ID subsystems to unlock the device." (<i>Id.</i> at 24.)</p> <p>"The class key is protected with the hardware UID and, for some classes, the user's passcode." (<i>Id.</i> at 85.)</p> <p><b>"Complete Protection</b></p> <p>(<i>NSFileProtectionComplete</i>): The class key is protected with a key derived from the user passcode or password and the device UID. Shortly after the user locks a device (10 seconds, if the Require</p>

Claim 11	Accused Instrumentalities
	<p>Password setting is Immediately), the decrypted class key is discarded, rendering all data in this class inaccessible until the user enters the passcode again or unlocks (logs in to) the device using Touch ID or Face ID."</p> <p>(Id. at 86.)</p> <p>The Touch ID or Face ID subsystem within the Secure Enclave is the SBIO shown below. SBIO is an application that runs within the Secure Enclave on the SEP and is responsible for checking the match of biometric features. SBIO receives the corresponding biometric data from a biometric sensor, such as the Touch ID sensor. The random secret is stored in a memory ("bio memory") associated with the SBIO and is output from the bio memory upon match, see step 3 in the diagram below ("3) upon successful match send random secret to SKS"):</p> <p>(Ex. B, Behind the Scenes with iOS Security, at 34.)</p>

<u>Claim 11</u>	<u>Accused Instrumentalities</u>
	<p>The class keys are encrypted with a master key:</p> <div data-bbox="612 349 1825 828" style="background-color: black; color: white; padding: 10px;"> <p><b>User Keybags</b> Background</p> <p>Sets of keys generated for each user to protect their data at rest Keys wrapped by master key derived from user passcode and SEP UID After 10 incorrect passcode entries, SEP will not process any further attempts Different policy associated with each keybag key—Usage, availability</p> </div> <p>(<i>Id.</i>, at 25.)</p> <p>The random secret is issued to SKS. SKS is a Secure Key Service application which is located within the Secure Enclave on the SEP and is responsible for decrypting class keys. The random secret provided by SBIO is used to decrypt a master key ("4) decrypt master key"). The master key is concatenated with the UID of the SEP and thus class keys are decrypted and added to the SKS keyring ("5) decrypt class keys, add to keyring") for further use by the Secure Enclave. The decrypted class keys include, for example, the class key of class A.</p>
<p>11d. emitting a secure access signal conveying information dependent upon said accessibility attribute; and</p>	<p><i>The Accused Instrumentalities include a transmitter configured to emit a secure access signal conveying information dependent upon said accessibility attribute.</i></p> <p>For example, the Secure Enclave emits a signal with ephemerally re-encrypted file keys:</p>




<u>Claim 11</u>	<u>Accused Instrumentalities</u>
	<p>“sepOS can then use the ephemeral wrapping key to wrap file keys for use by the Application Processor file-system driver. When the file-system driver reads or writes a file, it sends the wrapped key to the AES Engine.” (Ex. A, Apple Platform Security, at 14.)</p> <p>"All wrapped file key handling occurs in the Secure Enclave; the file key is never directly exposed to the Application Processor. [...] When the Secure Enclave unwraps a file's keys, they're rewrapped with the ephemeral key and sent back to the Application Processor." (<i>Id.</i> at 85.)</p> <p>The signal with the ephemerally re-encrypted file keys is a secure signal because it comes from the Secure Enclave and thus from a secure environment. Furthermore, the signal is secure because the transmitted information is encrypted. The emitted file keys are encrypted with the ephemeral key:</p> <p>"All wrapped file key handling occurs in the Secure Enclave; the file key is never directly exposed to the Application Processor. At startup, the Secure Enclave negotiates an ephemeral key with the AES Engine. When the Secure Enclave unwraps a file's keys, they're rewrapped with the ephemeral key and sent back to the Application Processor." (<i>Id.</i>)</p>

<u>Claim 11</u>	<u>Accused Instrumentalities</u>
	<p data-bbox="612 285 1412 354">Filesystem Data Protection</p> <p data-bbox="612 378 834 427">Overview</p> <p data-bbox="612 488 1476 524">File blocks are encrypted using AES-XTS with 128-bit keys</p> <p data-bbox="612 548 1896 584">Each file on the user partition is encrypted using a unique random key chosen by SEP</p> <p data-bbox="612 613 1240 649">Raw file keys are never exposed to the AP</p> <ul data-bbox="612 678 1636 776" style="list-style-type: none"> <li data-bbox="612 678 1566 714">• Wrapped with a key from the user keybag for long-term storage</li> <li data-bbox="612 737 1636 773">• Wrapped with an ephemeral key while in use, bound to boot session</li> </ul> <p data-bbox="612 784 1264 820">(Ex. B, Behind the Scenes with iOS Security, at 29.)</p>

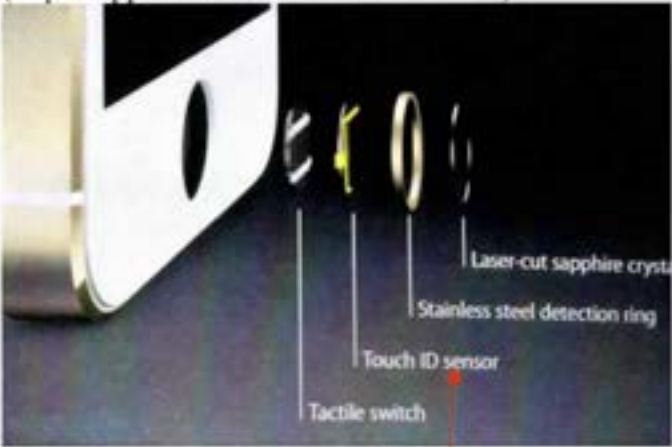
<u>Claim 11</u>	<u>Accused Instrumentalities</u>
	<div data-bbox="604 277 1766 933" style="background-color: black; color: white; padding: 20px;"> <h2 style="text-align: center;">Filesystem Data Protection</h2> <p>The diagram illustrates the process of filesystem data protection across four layers: User, Kernel, SEP (Secure Enclave Platform), and Hardware. The User layer shows a file being opened. The Kernel layer involves fetching a wrapped file key from metadata and sending an ID command with an ephemerally wrapped file key. The SEP layer shows the Key Store and AES Engine, where the file key is unwrapped using a keytag key and then wrapped using an ephemerally wrapped key returned from the Key Store. The Hardware layer shows the NAND and Storage Controller, where the cipher text is stored and the ephemerally wrapped key is established on boot.</p> <pre> graph TD     subgraph User         U[User]     end     subgraph Kernel         HFS[HFS]         NVME[NVME Driver]     end     subgraph SEP         KS[Key Store]         AE[AES Engine]     end     subgraph Hardware         NAND[NAND]         SC[Storage Controller]     end      U -- "open('foo.txt', ...)" --&gt; HFS     HFS -- "1. Fetch wrapped file_key from metadata" --&gt; NVME     NVME -- "4. Send ID command with ephemerally wrapped file_key" --&gt; SC     SC -- "Cipher Text" --&gt; NAND     SC -- "Ephemeral Key established on boot" --&gt; AE     AE -- "3. Wrap file_key using ephemeral_key, return ephemerally wrapped file_key to kernel" --&gt; KS     KS -- "2. Unwrap file_key using keytag key" --&gt; AE     KS &lt;--&gt; AE     </pre> </div> <p><i>(Id., at 30.)</i></p> <p>The information transmitted by the emitted signal, i.e., the ephemerally re-encrypted file keys, is dependent on the availability attribute, i.e., the confirmation that a biometric "template match" exists. This confirmation is signaled by the issuance of the random secret (cf. step 3): Only if there is a confirmation of the match and the random secret is issued by the Touch ID or Face ID subsystem within the Secure Enclave, i.e. SBIO, the class key is available for re-encrypting the file keys.</p> <p>The re-encrypted file keys are therefore information which is emitted depending on the fact that the availability attribute has been emitted.</p>

<u>Claim 11</u>	<u>Accused Instrumentalities</u>
<p>11e. providing conditional access to the controlled item dependent upon said information, wherein the controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing device.</p>	<p><i>The Accused Instrumentalities are configured to provide conditional access to the controlled item dependent upon said information, wherein the controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing device</i></p> <p>More specifically, the controlled item is a locking mechanism of the door lock of the user's home. The Accused Instrumentalities are configured to provide secure access to the user's home via Yale Smart Locks when the user provides biometric signal to the Accused Instrumentalities via Touch ID or Face ID.</p> <p>"When the "Secure Remote Access" feature is turned on, the app will use your phone's built-in authentication tools to prompt fingerprint or facial recognition before you can unlock or lock your home remotely (note: if your phone does not have these features, it will prompt you to use your PIN code). This further ensures that your door is only operated by the right people at the time you intend for it."</p> <p>(<a href="https://us.yalehome.com/en/yale-news/blog/latest-blog-posts/introducing-biometric-verification-for-august-and-yale-locks/">https://us.yalehome.com/en/yale-news/blog/latest-blog-posts/introducing-biometric-verification-for-august-and-yale-locks/</a>)</p>

<u>Claim 11</u>	<u>Accused Instrumentalities</u>
	 <p>The screenshot shows a mobile application interface for Yale. At the top, there is a yellow circular logo with the word "Yale" in black. To the left of the logo is a hamburger menu icon and the word "Open". To the right is a magnifying glass search icon. Below the header, the text "Introducing Biometric Verification for August and Yale Locks" is displayed in a bold, black font. Underneath the text is a photograph of a hand holding a smartphone. The phone's screen displays a biometric verification interface with a red circular camera viewfinder and a black square in the center containing a white icon of a face. The background of the photo is a blurred outdoor scene with green foliage.</p> <p>(<a href="https://us.yalehome.com/en/yale-news/blog/latest-blog-posts/introducing-biometric-verification-for-august-and-yale-locks/">https://us.yalehome.com/en/yale-news/blog/latest-blog-posts/introducing-biometric-verification-for-august-and-yale-locks/</a>)</p>

<u>Claim 11</u>	<u>Accused Instrumentalities</u>
	 <p>(<a href="https://www.apple.com/shop/product/HPAR2ZM/A/yale-assure-lock-sl-touchscreen-deadbolt-black">https://www.apple.com/shop/product/HPAR2ZM/A/yale-assure-lock-sl-touchscreen-deadbolt-black</a>)</p>

<u>Claim 12</u>	<u>Accused Instrumentalities</u>
<p>12. The method according to claim 11, wherein populating the database of biometric signatures further comprises enrolling a biometric signature into the database of biometric signatures, and wherein enrolling the biometric signature into the database comprises:</p>	<p><i>The Accused Instrumentalities are configured to enroll a biometric signature into the database of biometric signatures as set forth in elements 12a and 12b below.</i></p>
<p>12a. receiving a biometric signal; and</p>	<p><i>The Accused Instrumentalities include a biometric sensor configured to receive the biometric signal.</i></p> <p>More specifically, the iPhone has at least one biometric sensor for capturing a fingerprint or a face (Touch ID and/or Face ID), namely a Touch ID sensor and a camera system with image sensor, respectively.</p> <p><b>Touch ID</b></p> <p>"Apple devices with a Touch ID sensor can be unlocked using a fingerprint." (Ex. A, Apple Platform Security, at 19.)</p> <p>"Touch ID is the fingerprint sensing system that makes secure access to supported Apple devices faster and easier. This technology reads fingerprint data from any angle and learns more about a user's fingerprint over time, with the <b>sensor</b> continuing to expand the fingerprint map as additional overlapping nodes are identified with each use." (<i>Id.</i>)</p> <p>"When the fingerprint sensor detects the touch of a finger, it triggers the advanced imaging array to scan the finger and sends the scan to the Secure Enclave."</p>

<u>Claim 12</u>	<u>Accused Instrumentalities</u>
	<p>(<i>Id.</i>)</p> <p>The biometric sensor for Touch ID is located below the home button:</p> <p>"The Home button is a stack of different materials, capped with a sapphire crystal lens. The surrounding stainless-steel ring works as a ground and detects the user's finger. This action activates a capacitive touch sensor installed underneath the cover: A CMOS chip with small capacitors." (<a href="https://appleinsider.com/inside/touch-id">https://appleinsider.com/inside/touch-id</a>)</p>  <p style="text-align: center;">Biometric sensor 121</p> <p>"Where is the Touch ID sensor located?"</p> <p>The Touch ID sensor is located either in the home button or - on the iPad Air (4th generation) - in the top button.</p> <p>(<a href="https://support.apple.com/en-us/HT201371">https://support.apple.com/en-us/HT201371</a>)</p>




<u>Claim 12</u>	<u>Accused Instrumentalities</u>
	<p>The image sensor captures an 88-by-88-pixel, 500 PPI raster scan:</p> <p>"The 88-by-88-pixel, 500-ppi raster scan is temporarily stored in encrypted memory within the Secure Enclave while being vectorized for analysis, and then it's discarded. The analysis utilizes subdermal ridge flow angle mapping, which is a lossy process that discards minutia data that would be required to reconstruct the user's actual fingerprint. The resulting map of nodes is stored without any identity information in an encrypted format that can only be read by the Secure Enclave, and is never sent to Apple or backed up to iCloud or iTunes. "</p> <p>(Ex. C, iOS Security white paper, at 8.)</p> <p><b>Face ID</b></p> <p>The biometric sensor for facial biometrics is a camera system ("TrueDepth camera system") with an image sensor.</p> <p>"With a simple glance, Face ID securely unlocks supported Apple devices. It provides intuitive and secure authentication enabled by the TrueDepth camera system, which uses advanced technologies to accurately map the geometry of a user's face. "</p> <p>(Ex. A, Apple Platform Security, at 20.)</p> <p>To receive a biometric signal, the camera system with image sensor reads over 30,000 infrared points to capture depth information along with a two-dimensional infrared image.</p> <p>"After the TrueDepth camera confirms the presence of an attentive face, it projects and <b>reads over 30,000 infrared dots to form a depth map of the face along with a 2D infrared image.</b> This data is used to <b>create a sequence of 2D images and depth maps</b>, which are digitally signed and sent to the Secure Enclave. To counter both digital and physical spoofs, the TrueDepth camera randomizes the sequence of 2D images and depth map captures, and projects a device-specific random pattern. A portion of the Secure Neural Engine-protected within the Secure Enclave-transforms this data into a</p>

<u>Claim 12</u>	<u>Accused Instrumentalities</u>
	<p>mathematical representation and compares that representation to the enrolled facial data. This enrolled facial data is itself a mathematical representation of the user's face captured across a variety of poses." (<i>Id.</i>, at 20.)</p> <p>The camera system includes a biometric image sensor, namely a "CMOS image" sensor from Sony, to perform facial biometrics:</p>  <p>(<a href="https://appleinsider.com/articles/17/09/09/inner-workings-of-apples-face-id-camera-detailed-in-report">https://appleinsider.com/articles/17/09/09/inner-workings-of-apples-face-id-camera-detailed-in-report</a>)</p>
<p>12b. enrolling the biometric signal as an administrator signature in response to the database of</p>	<p><i>The Accused instrumentalities are configured to enroll the biometric signal as an administrator signature in response to the database of biometric signatures being empty.</i></p> <p>More specifically, upon information and belief, the iPhone allows the users to enroll their biometric signature as an administrator when the user is setting up their first iOS device. The biometric</p>


<u>Claim 12</u>	<u>Accused Instrumentalities</u>
<p>biometric signatures being empty.</p>	<p>signature enrolled upon the initial set up of the iOS device will be required to add additional fingerprints or faces on the device.</p> <p><b>Set up Face ID or Touch ID and create a passcode</b></p> <p>On some devices, you can set up <a href="#">Face ID</a> or <a href="#">Touch ID</a>. With these features, you can use face recognition or your fingerprint to unlock your device and make purchases. Tap Continue and follow the instructions, or tap "Set Up Later in Settings."</p> <p>Next, set a six-digit passcode to help protect your data. You need a passcode to use features like Face ID, Touch ID, and <a href="#">Apple Pay</a>. If you'd like a four-digit passcode, custom passcode, or no passcode, tap "Passcode Options."</p> <div data-bbox="676 721 1464 1360" style="text-align: center;"> </div> <p>(<a href="https://support.apple.com/en-us/HT202033">https://support.apple.com/en-us/HT202033</a>)</p>

<u>Claim 14</u>	<u>Accused Instrumentalities</u>
<p>14. A non-transitory computer readable storage medium storing a computer program comprising instructions, which when executed by processors causes the processors to:</p>	<p><i>The Accused Instrumentalities are non-transitory computer readable storage medium storing a computer program comprising instructions as set forth below.</i></p>
<p>14a. receive a series of entries of a biometric signal;</p>	<p><i>The Accused Instrumentalities include a transmitter sub-system controller configured to receive a series of entries of the biometric signal.</i></p> <p>More specifically, the Secure Enclave of the iPhone with the Secure Enclave Processor forms the means for receiving a series of entries of the biometric signal.</p> <p>"Apple's biometric security architecture relies on a strict separation of responsibilities between the biometric sensor and the Secure Enclave, and a secure connection between the two. The sensor captures the biometric image and securely transmits it to the Secure Enclave." (Ex. A, Apple Platform Security, at 19.)</p> <p><b>Touch ID</b></p> <p>When a finger is placed on the biometric sensor, the finger is scanned and the corresponding biometric signal entry is received by the Secure Enclave.</p> <p>"When the fingerprint sensor detects the touch of a finger, it triggers the advanced imaging array to scan the finger and sends the scan to the Secure Enclave." (<i>Id.</i>)</p> <p>To enroll a fingerprint in the database, the iPhone's fingerprint sensor records an entry of a biometric signal when the user places his finger on the sensor. This is done multiple times, resulting in a series of entries of such biometric signals.</p>

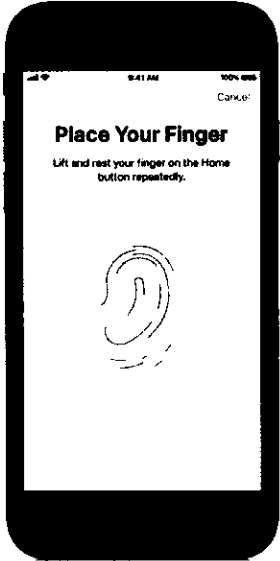
<u>Claim 14</u>	<u>Accused Instrumentalities</u>
	<p>Receiving a series of entries of the biometric signal by repeatedly placing a finger on the Touch ID sensor will use Touch ID on iPhone.</p> <p><b>Set up Touch ID</b></p> <p>Before you can set up Touch ID, you must first create a <a href="#">code</a> for your device,* then follow these steps:</p> <ol style="list-style-type: none"> <li>13. Make sure the Touch ID sensor and your finger are clean and dry.</li> <li>14. Tap Settings &gt; Touch ID &amp; Code, and then enter your code.</li> <li>15. Tap "Add fingerprint" and hold the device as you normally would when touching the Touch ID sensor.</li> <li>16. Touch the Touch ID sensor with one finger, but do not press. Keep your finger on the button until you feel a quick vibration or are prompted to lift your finger.</li> </ol> 

<u>Claim 14</u>	<u>Accused Instrumentalities</u>
	<p>17. Continue by raising and slowly lowering your finger over and over again, changing the position of your finger just a tiny bit at a time.</p> <p>18. The next screen will ask you to change your finger position. Hold your device as you normally would when unlocking it. Touch the Touch ID sensor with the outer edges of your fingertip instead of the middle part as you would during the first scan.”</p> <p>(<a href="https://support.apple.com/en-us/HT201371">https://support.apple.com/en-us/HT201371</a>)</p> <p>Accordingly, the user is prompted to place his finger on the sensor several times, in particular in accordance with step 5. Each time the finger is placed on the sensor, a corresponding biometric entry is generated, i.e. a series of such entries. All these entries, which result from placing the same finger on the sensor, form a series.</p> <p><b>Face ID</b></p> <p>The means for receiving a series of entries of the biometric signal includes a Secure Neural Engine, which is protected by the Secure Enclave. The Secure Neural Engine transforms the series of entries of the biometric signal received by the Secure Enclave into a biometric signature ("mathematical representation").</p> <p>"After the TrueDepth camera confirms the presence of an attentive face, it projects and reads over 30,000 infrared dots to form a depth map of the face along with a 2D infrared image. This data is used to create <b>a sequence of 2D images and depth maps</b>, which are digitally signed and <b>sent to the Secure Enclave</b>. To counter both digital and physical spoofs, the TrueDepth camera randomizes the sequence of 2D images and depth map captures, and projects a device-specific random pattern. A portion of the <b>Secure Neural Engine-protected</b> within the Secure Enclave-transforms this data into a mathematical representation and compares that representation to the enrolled facial data. This enrolled facial data is itself a mathematical representation of the user's face captured across a variety of poses." (Ex. A, Apple Platform Security, at 20.)</p>

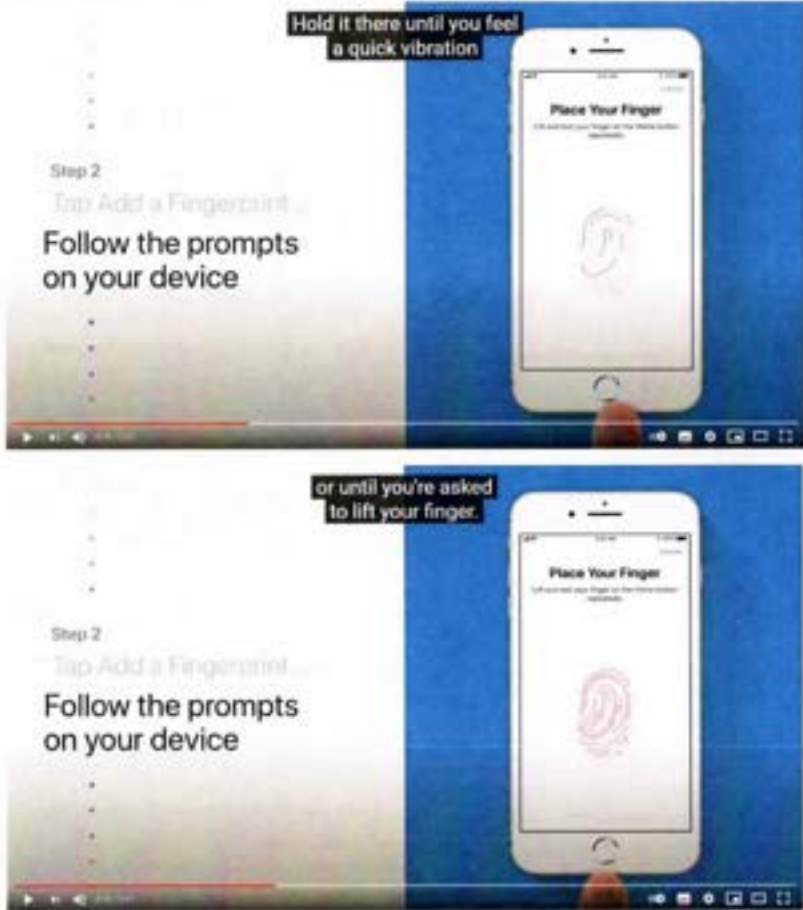
<u>Claim 14</u>	<u>Accused Instrumentalities</u>
	<p>Each entry of the biometric signal thus contains a two-dimensional infrared image with 30,000 infrared points for capturing depth information. By continuously capturing such infrared images into a Face ID scan while the user moves his head into different poses, a series of entries of the biometric signal results. Two such Face ID scans are required to generate a biometric signature of a single face, so that two series of entries of the biometric signal are received accordingly.</p> <p>Using Face ID on iPhone</p> <ol style="list-style-type: none"> <li>1. Tap Settings &gt; Face ID &amp; Code. Enter your code when prompted.</li> <li>2. Tap on "Configure Face ID".</li> <li>3. Hold the device in portrait mode in front of your face and tap "Let's go".</li> <li>4. Make sure your face is inside the frame and slowly move your head until the circle shown is completed. If you can't move your head, tap on "Options for operating aids".</li> <li>5. After performing the first Face ID scan, tap "Next".</li> <li>6. Again, slowly describe a circle with your head until it is completed.</li> <li>7. Tap "Done."</li> </ol> <p>(<a href="https://support.apple.com/en-us/HT208109">https://support.apple.com/en-us/HT208109</a>)</p> <p>The biometric signature of a single face is thus determined by two successive Face ID scans, each of which receives a series of entries of the biometric signal (compare steps 4. and 6. above).</p> <p>To register a second face, the iPhone offers a corresponding option in its settings. If the user selects the option "Set up an alternative appearance" as shown in the figure below on <a href="https://www.macworld.co.uk/how-to/second-face-id-3803421/">https://www.macworld.co.uk/how-to/second-face-id-3803421/</a>, a second face is registered by the iPhone in the same way as the first face.</p>


<u>Claim 14</u>	<u>Accused Instrumentalities</u>
	 <p>The series of entries of the biometric signal is identified on the iPhone by both the number and duration of each such entry.</p> <p><b>Touch ID</b></p> <p>According to step 5 of the instructions <a href="https://support.apple.com/en-us/HT201371">https://support.apple.com/en-us/HT201371</a>, for the enrollment of a single finger, the user has to repeatedly place the respective finger on the sensor and thus a number of entries in a row predetermined via the user guidance are captured by the iPhone. Each one of the entries must also be of a predetermined duration given to the user via the iPhone display, i.e. the user's finger must remain on the sensor for a predetermined duration for each entry of the biometric signal in order to capture the biometric signal during this time.</p>



<u>Claim 14</u>	<u>Accused Instrumentalities</u>
	<p>Receiving a series of entries of the biometric signal by repeatedly placing a finger on the Touch ID sensor will use Touch ID on iPhone and iPad.</p> <p><b>Set up Touch ID</b></p> <p>...</p> <p>4. Touch the Touch ID sensor with one finger, but do not press. Keep your finger on the button until you feel a quick vibration or are prompted to lift your finger.</p>  <p>5. Continue by raising and slowly lowering your finger over and over again, changing the position of your finger just a tiny bit at a time.</p> <p>6. The next screen will ask you to change your finger position. Hold your device as you normally would when unlocking it. Touch the Touch ID sensor with the outer edges of your fingertip instead of the middle part as you did during the first scan.</p> <p>(<a href="https://support.apple.com/en-us/HT201371">https://support.apple.com/en-us/HT201371</a>)</p>

<b><u>Claim 14</u></b>	<b><u>Accused Instrumentalities</u></b>
	<p>After placing a finger on the home button, a fingerprint appears on the display with red progress bars spreading along some of the papillary bars until the capture of the biometric entry in question is complete:</p> <div data-bbox="1115 386 1395 948" data-label="Image"> </div> <p>When the required duration is reached, the iPhone vibrates after an entry of the biometric signal is received or it issues a prompt to the user to lift the finger. The user then lifts the finger in question and replaces the same finger so that the iPhone receives a series of biometric signal entries of sufficient duration for that finger. The process is repeated for the same finger for as long as required according to the iPhone's user guidance.</p> <p>This is shown in the Apple You Tube video (32) How to set up Touch ID on your iPhone or iPad - Apple Support - YouTube (<a href="https://www.youtube.com/watch?v=xTZ2LALWZlg">https://www.youtube.com/watch?v=xTZ2LALWZlg</a>):</p>

<u>Claim 14</u>	<u>Accused Instrumentalities</u>
	 <p>Both the number of entries, i.e. the number of repetitions for placing the finger on the screen, and their respective duration are specified by the iPhone via the user guidance.</p>

<u>Claim 14</u>	<u>Accused Instrumentalities</u>
	<p><b>Face ID</b></p> <p>The user moves his face in front of the camera to strike different poses, and the camera system with image sensor continuously captures a large number of biometric entries, i.e. here the 2D images with depth information, in a row.</p> <p>"This enrolled facial data is itself a mathematical representation of the user's face captured across a variety of poses." (Ex. A, Apple Platform Security, at 20.)</p> <p>The sufficient duration of an entry for a pose, i.e. an angular position of the head specified via the user interface of the iPhone, is indicated to the user by the transformation of a gray line into a green line:</p>  <p>(Individual images taken from: <a href="https://support.apple.com/en-us/HT208109">https://support.apple.com/en-us/HT208109</a>)</p>
<p>14b. determine at least one of a number of said entries</p>	<p><i>The Accused instrumentalities are configured to populate the database of biometric signatures by: determining at least one of the number of said entries and a duration of each said entry.</i></p>

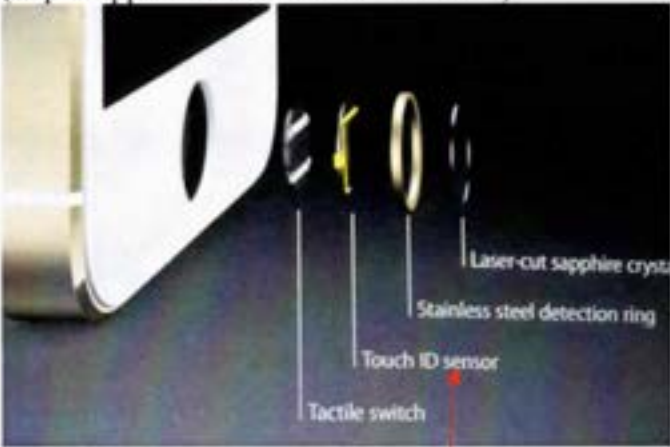
<u>Claim 14</u>	<u>Accused Instrumentalities</u>
and a duration of each of said entries;	<p>More specifically, as discussed above, both Face ID and Touch ID require a specific number of entries to enroll a Touch ID or Face ID. The Accused Instrumentalities must determine that the specific number of entries have been input. Likewise, while not necessary for the claim, upon information and belief, the Accused Instrumentalities determine that each input of either facial or fingerprint data is of a sufficient duration. Again, when setting up Touch ID in the Accused Instrumentalities, the users are required to touch the home button with their finger several times for a certain duration. Similarly, the users need to scan their face twice, and each scan requires the users to move their head in a circle for a certain duration for Face ID.</p> <p>Touch ID: Register a fingerprint for Apple Touch ID by the user tapping a finger several times on the home button to record the fingerprint data. (<a href="https://video.search.yahoo.com/yhs/search?fr=yhs-pty-pty_converter&amp;hsimp=yhs-pty_converter&amp;hspart=pty&amp;p=registering+fingerprint+apple+touch+id+on+screen+instructions#id=1&amp;vid=156de65ae06ca453643009fc0ea9cf79&amp;action=click">https://video.search.yahoo.com/yhs/search?fr=yhs-pty-pty_converter&amp;hsimp=yhs-pty_converter&amp;hspart=pty&amp;p=registering+fingerprint+apple+touch+id+on+screen+instructions#id=1&amp;vid=156de65ae06ca453643009fc0ea9cf79&amp;action=click</a>)</p> <p>Touch ID: The user's finger must remain on the home button long enough for the data to be recorded. "Touch the Touch ID sensor with your finger, but don't press it. Hold it there until you feel a quick vibration, or until you're asked to lift your finger." "Continue to lift and rest your finger slowly, making small adjustments to the position of your finger each time." (<a href="https://support.apple.com/en-au/HT201371">https://support.apple.com/en-au/HT201371</a>)</p> <p>Touch ID: "you shouldn't tap too quickly or move your finger around" (<a href="https://support.apple.com/en-us/HT207537">https://support.apple.com/en-us/HT207537</a>)</p> <p>Face ID: Setting up Face ID requires two scans of the user's face. Each scan asks users to move their head slowly in a circle to register different angles of the user's face. (<a href="https://www.imore.com/how-set-face-id-iphone">https://www.imore.com/how-set-face-id-iphone</a>)</p>
14c. map said series into an instruction;	<b><i>The Accused Instrumentalities include a transmitter sub-system controller configured to map said series into an instruction.</i></b>

<u>Claim 14</u>	<u>Accused Instrumentalities</u>
	<p>More specifically, the Secure Enclave of the iPhone contains means to assign the received row to an instruction: The Secure Enclave, after receiving the full set of entries of the biometric signal, assigns this set to an instruction for processing, encrypting and storing the biometric signature ("Touch ID and Face ID template data").</p> <p>"The sensor captures the biometric image and securely transmits it to the Secure Enclave. During enrollment, the Secure Enclave processes, encrypts, and stores the corresponding Touch ID and Face ID template data." (Ex. A, Apple Platform Security, at 19.)</p> <p>To carry out this instruction, the Secure Enclave has its own processor: "The Secure Enclave Processor provides the main computing power for the Secure Enclave." (<i>Id.</i>, at 10.)</p> <p><b>Touch ID</b></p> <p>The instruction here involves the processing of under-the-skin fingerprint characteristics and their encrypted storage.</p> <p>"The analysis uses subdermal ridge flow angle mapping, a lossy process that discards "finger minutiae data" that would be required to reconstruct the user's actual fingerprint. During enrollment, the resulting map of nodes is stored in an encrypted format that can be read only by the Secure Enclave as a template to compare against for future matches, but without any identity information." (<i>Id.</i>, at 19.)</p> <p><b>Face ID</b></p> <p>The instruction involves the transformation of the set of entries of the biometric signal captured via the Face ID scans into a mathematical representation, i.e. the biometric signature of the face in question by the Secure Neural Engine of the Secure Enclave, as well as its encryption and storage.</p>


<u>Claim 14</u>	<u>Accused Instrumentalities</u>
	<p>"A portion of the Secure Neural Engine-protected within the Secure Enclave-transforms this data into a mathematical representation and compares that representation to the enrolled facial data. This enrolled facial data is itself a mathematical representation of the user's face captured across a variety of poses." <i>(Id., at 20.)</i></p> <p>"Face ID data, including mathematical representations of a user's face, is encrypted and available only to the Secure Enclave. This data never leaves the device. It's not sent to Apple, nor is it included in device backups. The following Face ID data is saved, encrypted only for use by the Secure Enclave, during normal operation:</p> <ul style="list-style-type: none"> <li>• The mathematical representations of a user's face calculated during enrollment</li> <li>• ..."</li> </ul> <p><i>(Id., at 23.)</i></p>
<p>14d. populate a database of biometric signatures according to the instruction;</p>	<p><b><i>The Accused Instrumentalities include a transmitter sub-system controller configured to populate the database according to the instruction.</i></b></p> <p>More specifically, the Secure Enclave stores the biometric signature, i.e. the encrypted mathematical representation of the fingerprint or face, in the database 105, i.e. the "secure nonvolatile storage":</p> <p>"The secure nonvolatile storage is used for all anti-replay services in the Secure Enclave. Anti-replay services on the Secure Enclave are used for revocation of data over events that mark anti-replay boundaries including, but not limited to, the following:</p> <ul style="list-style-type: none"> <li>• ...</li> <li>• ...</li> <li>• Adding or removing a Touch ID fingerprint or Face ID face".</li> </ul> <p><i>(Ex. A, Apple Platform Security, at 16.)</i></p> <p>"During enrollment, the Secure Enclave processes, encrypts, and stores the corresponding Touch ID and Face ID template data." <i>(Id., at 19.)</i></p>

<u>Claim 14</u>	<u>Accused Instrumentalities</u>
	<p><b>Touch ID</b></p> <p>"During enrollment, the resulting map of nodes is stored in an encrypted format that can be read only by the Secure Enclave as a template to compare against for future matches...." (<i>Id.</i>)</p> <p><b>Face ID</b></p> <p>The following Face ID data is saved, encrypted only for use by the Secure Enclave, during normal operation:</p> <ul style="list-style-type: none"> <li>• The mathematical representations of a user's face calculated during enrollment".</li> </ul> <p>(<i>Id.</i>, at 23.)</p>
14e. receive the biometric signal;	<p><b><i>The Accused Instrumentalities include a biometric sensor configured to receive the biometric signal.</i></b></p> <p>More specifically, the iPhone has at least one biometric sensor for capturing a fingerprint or a face (Touch ID and/or Face ID), namely a Touch ID sensor and a camera system with image sensor, respectively.</p> <p><b>Touch ID</b></p> <p>"Apple devices with a Touch ID sensor can be unlocked using a fingerprint." (Ex. A, Apple Platform Security, at 19.)</p> <p>"Touch ID is the fingerprint sensing system that makes secure access to supported Apple devices faster and easier. This technology reads fingerprint data from any angle and learns more about a user's fingerprint over time, with the <b>sensor</b> continuing to expand the fingerprint map as additional overlapping nodes are identified with each use." (<i>Id.</i>)</p> <p>"When the fingerprint sensor detects the touch of a finger, it triggers the advanced imaging array to scan the finger and sends the scan to the Secure Enclave."</p>



<u>Claim 14</u>	<u>Accused Instrumentalities</u>
	<p data-bbox="604 285 659 315"><i>(Id.)</i></p> <p data-bbox="604 391 1453 420">The biometric sensor for Touch ID is located below the home button:</p> <p data-bbox="604 461 1854 597">"The Home button is a stack of different materials, capped with a sapphire crystal lens. The surrounding stainless-steel ring works as a ground and detects the user's finger. This action activates a capacitive touch sensor installed underneath the cover: A CMOS chip with small capacitors." (<a href="https://appleinsider.com/inside/touch-id">https://appleinsider.com/inside/touch-id</a>)</p>  <p data-bbox="894 1117 1157 1146">Biometric sensor 121</p> <p data-bbox="604 1190 1108 1219">"Where is the Touch ID sensor located?"</p> <p data-bbox="604 1252 1829 1313">The Touch ID sensor is located either in the home button or - on the iPad Air (4th generation) - in the top button.</p> <p data-bbox="604 1349 1129 1378">(https://support.apple.com/en-us/HT201371)</p>

<u>Claim 14</u>	<u>Accused Instrumentalities</u>
	<p>The image sensor captures an 88-by-88-pixel, 500 PPI raster scan:</p> <p>"The 88-by-88-pixel, 500-ppi raster scan is temporarily stored in encrypted memory within the Secure Enclave while being vectorized for analysis, and then it's discarded. The analysis utilizes subdermal ridge flow angle mapping, which is a lossy process that discards minutia data that would be required to reconstruct the user's actual fingerprint. The resulting map of nodes is stored without any identity information in an encrypted format that can only be read by the Secure Enclave, and is never sent to Apple or backed up to iCloud or iTunes. "</p> <p>(Ex. C, iOS Security white paper, at 8.)</p> <p><b>Face ID</b></p> <p>The biometric sensor for facial biometrics is a camera system ("TrueDepth camera system") with an image sensor.</p> <p>"With a simple glance, Face ID securely unlocks supported Apple devices. It provides intuitive and secure authentication enabled by the TrueDepth camera system, which uses advanced technologies to accurately map the geometry of a user's face. "</p> <p>(Ex. A, Apple Platform Security, at 20.)</p> <p>To receive a biometric signal, the camera system with image sensor reads over 30,000 infrared points to capture depth information along with a two-dimensional infrared image.</p> <p>"After the TrueDepth camera confirms the presence of an attentive face, it projects and <b>reads over 30,000 infrared dots to form a depth map of the face along with a 2D infrared image</b>. This data is used to <b>create a sequence of 2D images and depth maps</b>, which are digitally signed and sent to the Secure Enclave. To counter both digital and physical spoofs, the TrueDepth camera randomizes the sequence of 2D images and depth map captures, and projects a device-specific random pattern. A portion of the Secure Neural Engine-protected within the Secure Enclave-transforms this data into a</p>

<u>Claim 14</u>	<u>Accused Instrumentalities</u>
	<p>mathematical representation and compares that representation to the enrolled facial data. This enrolled facial data is itself a mathematical representation of the user's face captured across a variety of poses." (<i>Id.</i>, at 20.)</p> <p>The camera system includes a biometric image sensor, namely a "CMOS image" sensor from Sony, to perform facial biometrics:</p>  <p>(<a href="https://appleinsider.com/articles/17/09/09/inner-workings-of-apples-face-id-camera-detailed-in-report">https://appleinsider.com/articles/17/09/09/inner-workings-of-apples-face-id-camera-detailed-in-report</a>)</p>
<p>14f. match the biometric signal against members of the database of biometric signatures to thereby</p>	<p><i>The Accused Instrumentalities include a transmitter controller configured to emit a secure access signal conveying information dependent upon said accessibility attribute.</i></p>

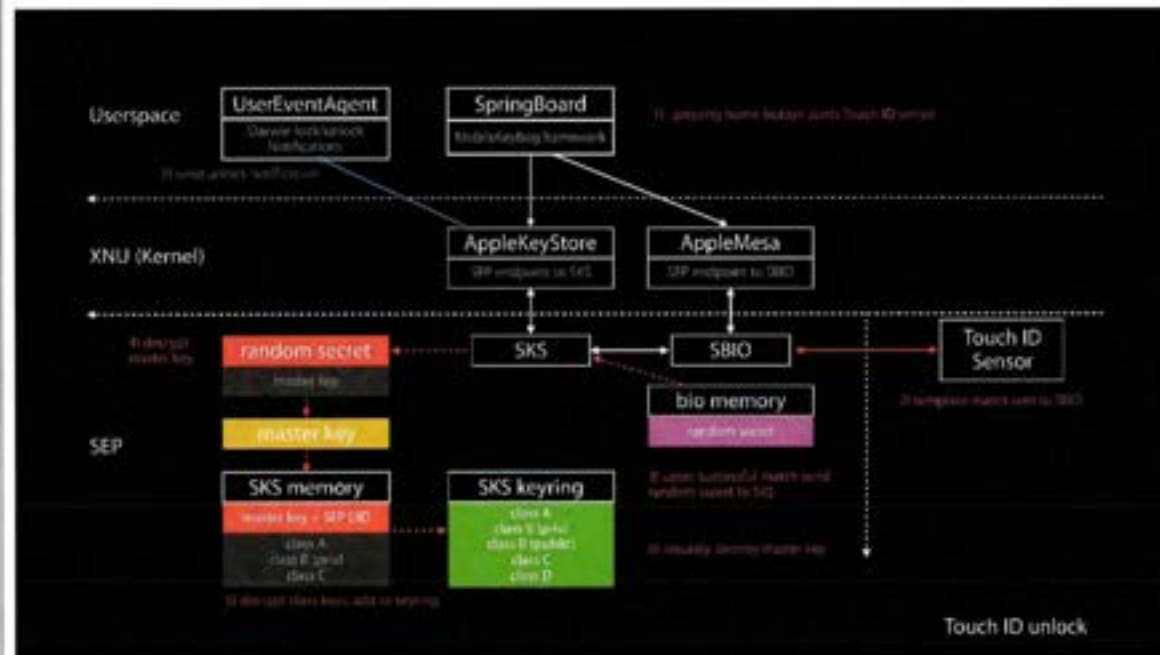
<u>Claim 14</u>	<u>Accused Instrumentalities</u>
output an accessibility attribute;	<p>More specifically, the iPhone's System on Chip (SOC), i.e. the Secure Enclave with its Secure Enclave Processor (SEP) or a Secure Neural Engine contained therein, is a means (103) to check a match of the biometric signal with elements of the biometric signature database.</p> <p>"The <i>Secure Enclave</i> is a system on chip (SoC) that is included on all recent iPhone, ... devices" (Ex. A, Apple Platform Security, at 7.)</p> <p>"During <b>matching</b>, the Secure Enclave <b>compares</b> incoming data from the biometric sensor against the stored templates <b>to determine whether to unlock the device</b> or respond that a match is valid (for Apple Pay, in-app, and other uses of Touch ID and Face ID). " (<i>Id.</i>, at 19.)</p> <p>The biometric signal received from the biometric sensor ("incoming data from the biometric sensor") is thus checked by the Secure Enclave and its SEP with the elements of the database of biometric signatures 105, i.e. the "stored templates", for the presence of a match.</p> <p>For Touch ID, the Secure Enclave match verification is performed as follows:</p> <p>"The Secure Enclave is responsible for processing fingerprint data from the Touch ID sensor, determining if there is a match against registered fingerprints, and then enabling access or purchases on behalf of the user ..." (Ex. C, iOS Security white paper, at 7.)</p> <p>"During enrollment, the resulting map of nodes is stored in an encrypted format that can be read only by the Secure Enclave as a template to compare against for future matches...." (Ex. A, Apple Platform Security, at 19.)</p> <p>"Touch ID can read multiple fingerprints, and it can read fingerprints in 360-degrees of orientation. It then creates a mathematical representation of your fingerprint and compares this to your enrolled fingerprint data to identify a match and unlock your device. " (<a href="https://support.apple.com/en-us/HT204587">https://support.apple.com/en-us/HT204587</a>)</p>

<u>Claim 14</u>	<u>Accused Instrumentalities</u>
	<p>"Touch ID can read multiple fingerprints and recognize fingerprints at any orientation of the finger. The system then creates a mathematical representation of your fingerprint and compares it to the registered fingerprint data to determine a match and unlock your device." (<a href="https://support.apple.com/de-de/HT204587">https://support.apple.com/de-de/HT204587</a>)</p> <p>For <b>Face ID</b>, the Secure Enclave has a neural network protected by it, i.e., a Secure Neural Engine, which is used to verify the match:</p> <p>"Face ID uses neural networks for determining attention, <b>matching</b>, and antispoofing, so a user can unlock their phone with a glance." (Ex. A, Apple Platform Security, at 20.)</p> <p>"A portion of the Secure Neural Engine-protected within the Secure Enclave-transforms this data into a mathematical representation and compares that representation to the enrolled facial data. This enrolled facial data is itself a mathematical representation of the user's face captured across a variety of poses." (<i>Id.</i>).</p> <p>"Facial matching security Facial matching is performed within the Secure Enclave using neural networks trained specifically for that purpose... Face ID data, including mathematical representations of a user's face, is encrypted and available only to the Secure Enclave. This data never leaves the device." (<i>Id.</i> at 23.)</p> <p>When the Secure Enclave, or more precisely the Touch ID or Face ID subsystem within the Secure Enclave, has determined that a match exists, an accessibility attribute is issued by the corresponding Touch ID or Face ID subsystem. This Touch ID or Face ID subsystem is also referred to as the SBIO. The accessibility attribute confirms that there is a match and that the iPhone is to be unlocked ("... determine whether to unlock the device ...").</p>

<u>Claim 14</u>	<u>Accused Instrumentalities</u>
	<p>This confirmation of the match is signaled by the SBIO by issuing a random secret to which only the Touch ID or Face ID subsystem within the Secure Enclave has access:</p> <p>"During matching, the Secure Enclave compares incoming data from the biometric sensor against the stored templates to determine whether to unlock the device [...]." (<i>Id.</i> at 19.)</p> <p>"Uses for Touch ID and Face ID</p> <p><b>Unlocking a device or user account</b></p> <p>[...] keys for the highest class of Data Protection-which are held in the Secure Enclave [...].</p> <p>With Touch ID or Face ID enabled, the keys aren't discarded when the device or account locks; instead, <b>they're wrapped with a key that's given to the Touch ID or Face ID subsystem inside the Secure Enclave.</b> When a user attempts to unlock the device or account, <b>if the device detects a successful match, it provides the key for unwrapping the Data Protection keys,</b> and the device or account is unlocked. This process provides additional protection by requiring cooperation between the Data Protection and Touch ID or Face ID subsystems to unlock the device." (<i>Id.</i> at 24.)</p> <p>"The class key is protected with the hardware UID and, for some classes, the user's passcode." (<i>Id.</i> at 85.)</p> <p><b>"Complete Protection</b></p> <p>(<i>NSFileProtectionComplete</i>): The class key is protected with a key derived from the user passcode or password and the device UID. Shortly after the user locks a device (10 seconds, if the Require Password setting is Immediately), the decrypted class key is discarded, <b>rendering all data in this class inaccessible until the user enters the passcode again or unlocks (logs in to) the device using Touch ID or Face ID.</b>" (<i>Id.</i> at 86.)</p>

Claim 14Accused Instrumentalities

The Touch ID or Face ID subsystem within the Secure Enclave is the SBIO shown below. SBIO is an application that runs within the Secure Enclave on the SEP and is responsible for checking the match of biometric features. SBIO receives the corresponding biometric data from a biometric sensor, such as the Touch ID sensor. The random secret is stored in a memory ("bio memory") associated with the SBIO and is output from the bio memory upon match, see step 3 in the diagram below ("3) upon successful match send random secret to SKS"):



(Ex. B, Behind the Scenes with iOS Security, at 34.)

The class keys are encrypted with a master key:

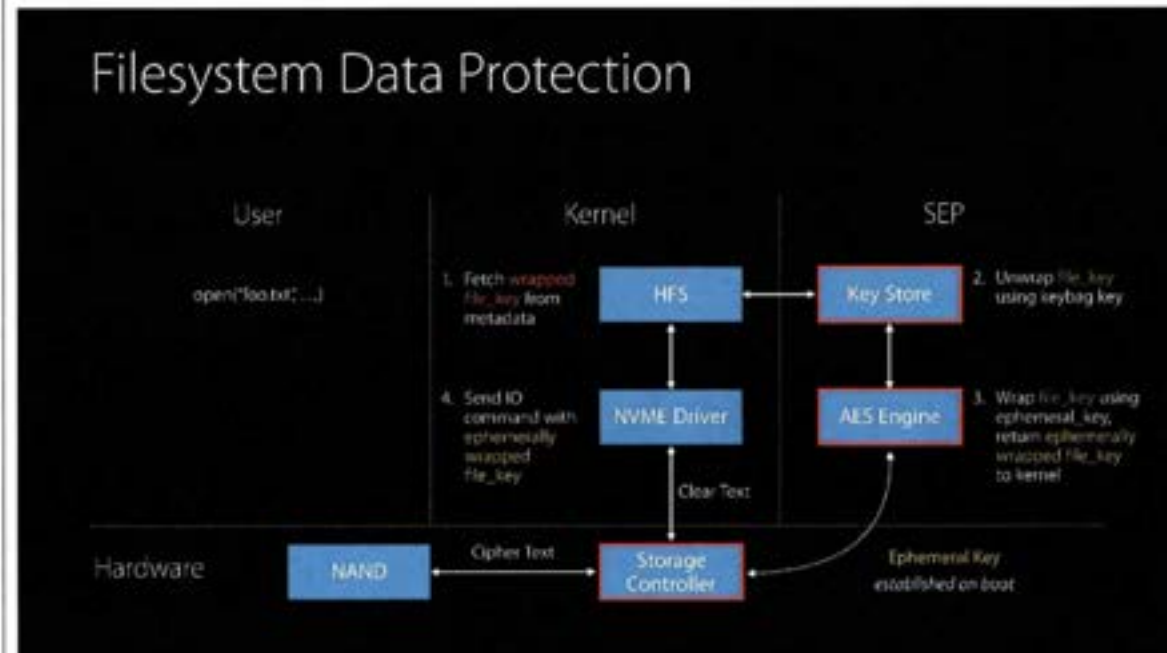
<u>Claim 14</u>	<u>Accused Instrumentalities</u>
	<p data-bbox="611 289 1024 365"><b>User Keybags</b></p> <p data-bbox="611 386 892 440">Background</p> <p data-bbox="611 500 1591 537">Sets of keys generated for each user to protect their data at rest</p> <p data-bbox="611 565 1682 602">Keys wrapped by master key derived from user passcode and SEP UID</p> <p data-bbox="611 630 1787 667">After 10 incorrect passcode entries, SEP will not process any further attempts</p> <p data-bbox="611 695 1671 732">Different policy associated with each keybag key—Usage, availability</p> <p data-bbox="600 760 741 792"><i>(Id., at 25.)</i></p> <p data-bbox="600 867 1864 1073">The random secret is issued to SKS. SKS is a Secure Key Service application which is located within the Secure Enclave on the SEP and is responsible for decrypting class keys. The random secret provided by SBIO is used to decrypt a master key ("4) decrypt master key"). The master key is concatenated with the UID of the SEP and thus class keys are decrypted and added to the SKS keyring ("5) decrypt class keys, add to keyring") for further use by the Secure Enclave. The decrypted class keys include, for example, the class key of class A.</p>
<p data-bbox="243 1118 558 1284">14g. emit a secure access signal conveying information dependent upon said accessibility attribute; and</p>	<p data-bbox="600 1118 1787 1182"><b><i>The Accused Instrumentalities include a transmitter configured to emit a secure access signal conveying information dependent upon said accessibility attribute.</i></b></p> <p data-bbox="600 1222 1688 1255">For example, the Secure Enclave emits a signal with ephemerally re-encrypted file keys:</p> <p data-bbox="600 1295 1829 1393">"sepOS can then use the ephemeral wrapping key to wrap file keys for use by the Application Processor file-system driver. When the file-system driver reads or writes a file, it sends the wrapped key to the AES Engine."</p>



<u>Claim 14</u>	<u>Accused Instrumentalities</u>
	<p>(Ex. A, Apple Platform Security, at 14.)</p> <p>"All wrapped file key handling occurs in the Secure Enclave; the file key is never directly exposed to the Application Processor. [...] When the Secure Enclave unwraps a file's keys, they're rewrapped with the ephemeral key and sent back to the Application Processor." (<i>Id.</i> at 85.)</p> <p>The signal with the ephemerally re-encrypted file keys is a secure signal because it comes from the Secure Enclave and thus from a secure environment. Furthermore, the signal is secure because the transmitted information is encrypted. The emitted file keys are encrypted with the ephemeral key:</p> <p>"All wrapped file key handling occurs in the Secure Enclave; the file key is never directly exposed to the Application Processor. At startup, the Secure Enclave negotiates an ephemeral key with the AES Engine. When the Secure Enclave unwraps a file's keys, they're rewrapped with the ephemeral key and sent back to the Application Processor." (<i>Id.</i>)</p> <div data-bbox="612 878 1902 1378" style="background-color: black; color: white; padding: 10px;"> <h2 style="margin: 0;">Filesystem Data Protection</h2> <h3 style="margin: 0;">Overview</h3> <p style="margin: 0;">File blocks are encrypted using AES-XTS with 128-bit keys</p> <p style="margin: 0;">Each file on the user partition is encrypted using a unique random key chosen by SEP</p> <p style="margin: 0;">Raw file keys are never exposed to the AP</p> <ul style="list-style-type: none"> <li>• Wrapped with a key from the user keybag for long-term storage</li> <li>• Wrapped with an ephemeral key while in use, bound to boot session</li> </ul> </div>

Claim 14Accused Instrumentalities

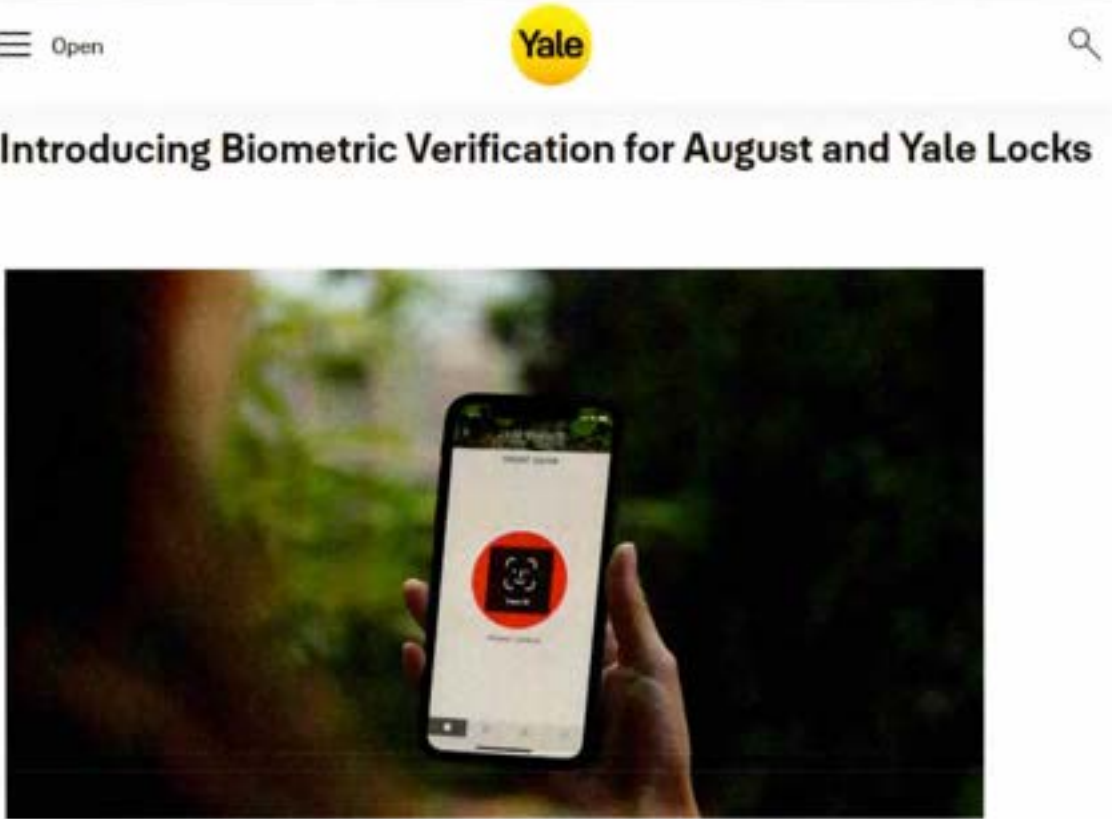
(Ex. B, Behind the Scenes with iOS Security, at 29.)

*(Id.*, at 30.)


The information transmitted by the emitted signal, i.e., the ephemeral re-encrypted file keys, is dependent on the availability attribute, i.e., the confirmation that a biometric "template match" exists. This confirmation is signaled by the issuance of the random secret (cf. step 3): Only if there is a confirmation of the match and the random secret is issued by the Touch ID or Face ID subsystem within the Secure Enclave, i.e. SBIO, the class key is available for re-encrypting the file keys.

The re-encrypted file keys are therefore information which is emitted depending on the fact that the availability attribute has been emitted.

<u>Claim 14</u>	<u>Accused Instrumentalities</u>
<p>14h. provide conditional access to a controlled item dependent upon said information, wherein the controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing device.</p>	<p><i>The Accused Instrumentalities are configured to provide conditional access to a controlled item dependent upon said information, wherein the controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing device.</i></p> <p>More specifically, the controlled item is a locking mechanism of the door lock of the user's home. The Accused Instrumentalities are configured to provide secure access to the user's home via Yale Smart Locks when the user provides biometric signal to the Accused Instrumentalities via Touch ID or Face ID.</p> <p>"When the "Secure Remote Access" feature is turned on, the app will use your phone's built-in authentication tools to prompt fingerprint or facial recognition before you can unlock or lock your home remotely (note: if your phone does not have these features, it will prompt you to use your PIN code). This further ensures that your door is only operated by the right people at the time you intend for it."</p> <p>(<a href="https://us.yalehome.com/en/yale-news/blog/latest-blog-posts/introducing-biometric-verification-for-august-and-yale-locks1/">https://us.yalehome.com/en/yale-news/blog/latest-blog-posts/introducing-biometric-verification-for-august-and-yale-locks1/</a>)</p>

<u>Claim 14</u>	<u>Accused Instrumentalities</u>
	 <p>The screenshot shows a mobile application interface for Yale. At the top, there is a yellow circular logo with the word "Yale" in black. To the left of the logo is a hamburger menu icon and the word "Open". To the right is a magnifying glass search icon. Below the navigation bar, the main heading reads "Introducing Biometric Verification for August and Yale Locks". Underneath the heading is a photograph of a hand holding a smartphone. The phone's screen displays a biometric verification interface with a red circular camera viewfinder and a black square containing a white Yale logo. Below the photograph, there is a URL: <a href="https://us.yalehome.com/en/yale-news/blog/latest-blog-posts/introducing-biometric-verification-for-august-and-yale-locks1/">(https://us.yalehome.com/en/yale-news/blog/latest-blog-posts/introducing-biometric-verification-for-august-and-yale-locks1/)</a></p>

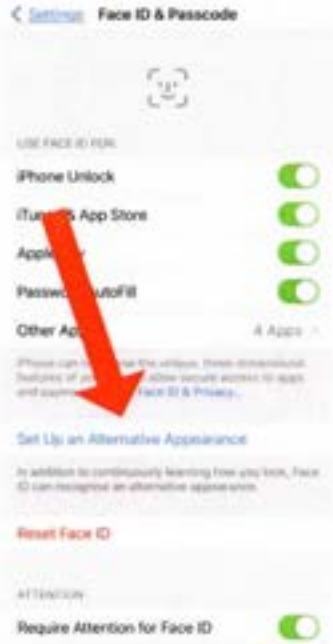
<u>Claim 14</u>	<u>Accused Instrumentalities</u>
	 <p>(<a href="https://www.apple.com/shop/product/HPAR2ZM/A/yale-assure-lock-sl-touchscreen-deadbolt-black">https://www.apple.com/shop/product/HPAR2ZM/A/yale-assure-lock-sl-touchscreen-deadbolt-black</a>)</p>

<u>Claim 15</u>	<u>Accused Instrumentalities</u>
15. A system for providing secure access to a controlled item, the system comprising:	<i>The Accused Instrumentalities are non-transitory computer readable storage medium storing a computer program comprising instructions as set forth below.</i>
15a. a memory comprising a database of biometric signatures;	<p><i>The Accused Instrumentalities include a memory comprising a database of biometric signatures.</i></p> <p>More specifically, the iPhone allows multiple biometric signatures to be entered into a database on the iPhone:</p> <p><b>Touch ID</b></p> <p>The iPhone allows the registration of multiple fingerprints:</p>  <p>Fig. from <a href="https://support.apple.com/en-us/HT201371">https://support.apple.com/en-us/HT201371</a> under Manage Touch ID Settings. In the second bullet, it literally says:</p>

<u>Claim 15</u>	<u>Accused Instrumentalities</u>
	<p>"Register up to five fingerprints."</p> <p>"Touch ID can read multiple fingerprints, and it can read fingerprints in 360-degrees of orientation. It then creates a mathematical representation of your fingerprint and compares this to your enrolled fingerprint data to identify a match and unlock your device. " (<a href="https://support.apple.com/en-us/HT204587">https://support.apple.com/en-us/HT204587</a>)</p> <p>"Touch ID can read multiple fingerprints and recognize fingerprints at any orientation of the finger. The system then creates a mathematical representation of your fingerprint and compares it to the registered fingerprint data to determine a match and unlock your device." (<a href="https://support.apple.com/en-us/HT204587">https://support.apple.com/en-us/HT204587</a>)</p> <p><b>Face ID</b></p> <p>The iPhone allows the registration of multiple faces:</p>

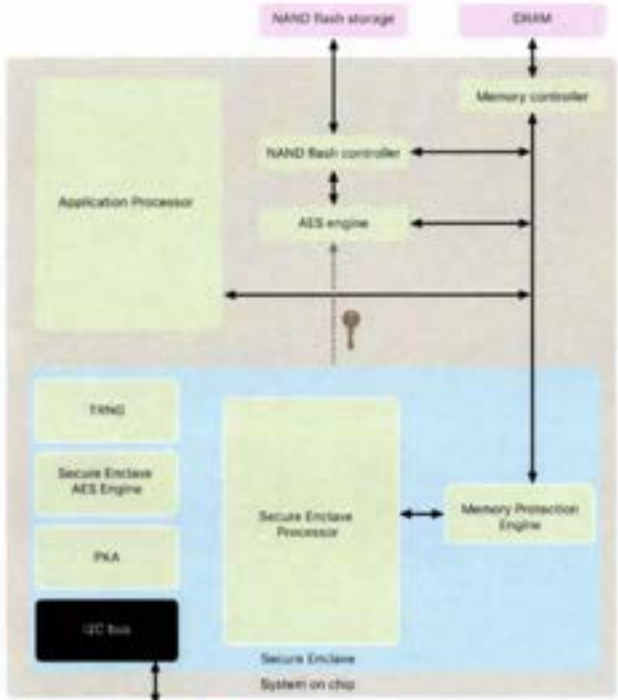
<u>Claim 15</u>	<u>Accused Instrumentalities</u>
	<div data-bbox="611 285 884 837" data-label="Image"> </div> <p data-bbox="604 883 1850 984">To register a face, the iPhone takes a series of pictures of the user in different poses while circling his head. This is revealed in detail in <a href="https://support.apple.com/en-us/HT208109">https://support.apple.com/en-us/HT208109</a> in the second section "Configure Face ID", there also the figure shown above.</p> <p data-bbox="604 1060 1871 1198">To register a second face, the iPhone offers a corresponding option in its settings. If the user selects the option "Set up an alternative appearance" as shown in the figure below (from How To Add A Second Face To Face ID - Macworld UK; <a href="https://www.macworld.co.uk/how-to/second-face-id-3803421/">https://www.macworld.co.uk/how-to/second-face-id-3803421/</a>), a second face is registered by the iPhone in the same way as the first face.</p> <p data-bbox="604 1239 1066 1268">"Set up Face ID or add another face.</p> <ul data-bbox="701 1305 1780 1367" style="list-style-type: none"> <li>• Select "Settings" &gt; "Face ID &amp; Code" &gt; "Configure alternate appearance" if you want to configure another face to be recognized by Face ID."</li> </ul>



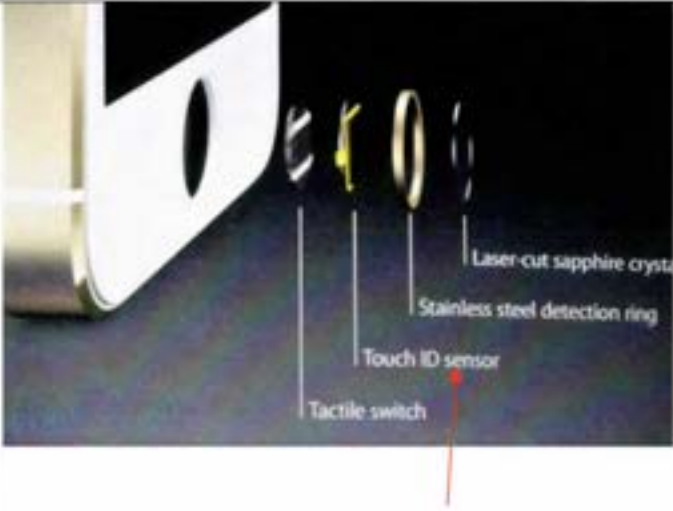
<u>Claim 15</u>	<u>Accused Instrumentalities</u>
	<p>(<a href="https://support.apple.com/de-de/guide/iphone/iph6d162927a/ios">https://support.apple.com/de-de/guide/iphone/iph6d162927a/ios</a>)</p>  <p>The screenshot shows the 'Face ID &amp; Passcode' settings page. At the top, there is a back arrow and the title 'Face ID &amp; Passcode'. Below that is a 'USE FACE ID FOR' section with several items: 'iPhone Unlock', 'iTunes &amp; App Store', 'App Store', 'Passwords Autofill', and 'Other Apps'. Each item has a green toggle switch to its right. A red arrow points to the 'Other Apps' section. Below this section, there is a note: 'iPhone can recognize the various, three-dimensional features of your face. Allow remote access to apps and content. See Face ID &amp; Privacy.' Below the note are links for 'Set Up an Alternative Appearance' and 'Reset Face ID'. At the bottom, there is an 'ATTENTION' section with a toggle for 'Require Attention for Face ID'.</p> <p>The page <a href="https://www.macworld.co.uk/how-to/second-face-id-3803421/">How To Add A Second Face To Face ID - Macworld UK</a> (<a href="https://www.macworld.co.uk/how-to/second-face-id-3803421/">https://www.macworld.co.uk/how-to/second-face-id-3803421/</a>) literally states:</p> <p>"Face ID is a fast and secure way to unlock your iPhone or iPad Pro, but you may not know that you can actually set up more than one face to use the feature."</p>

<u>Claim 15</u>	<u>Accused Instrumentalities</u>
	<p>This second face could belong to a loved one, enabling your partner or child to access your phone without requiring your smiling mug to unlock it. ”</p> <p>To store the biometric signatures ("template data") from the received biometric signals, the iPhone has a System on Chip (SOC) called a Secure Enclave. A Secure Enclave Processor provides the Secure Enclave with computing power:</p> <p>"The <i>Secure Enclave</i> is a system on chip (SoC) that is included on all recent iPhone, ... devices" (Ex. A, Apple Platform Security, at 7.)</p> <p>"The Secure Enclave is a dedicated secure subsystem integrated into Apple systems on chip (SoCs)." (<i>Id.</i>, at 9.)</p> <p>The Secure Enclave Processor provides the main computing power for the Secure Enclave." (<i>Id.</i>, at 10.)</p> <p>"During enrollment, the Secure Enclave processes, encrypts, and <b>stores</b> the corresponding Touch ID and Face ID template data." (<i>Id.</i>, at 19.)</p> <p>The Secure Enclave has access to a memory assigned to it and accessible only to it:</p> <p><b>Secure nonvolatile storage</b>  "The Secure Enclave is equipped with a dedicated secure nonvolatile storage device. The secure nonvolatile storage is connected to the Secure Enclave using a dedicated I2C bus, so that it can only be accessed by the Secure Enclave." (<i>Id.</i>, at 15.)</p> <p>This memory serves as a database for storing the biometric signatures:</p>


<u>Claim 15</u>	<u>Accused Instrumentalities</u>
	<p>"The secure nonvolatile storage is used for all anti-replay services in the Secure Enclave. Anti-replay services on the Secure Enclave are used for revocation of data over events that mark anti-replay boundaries including, but not limited to, the following:</p> <ul style="list-style-type: none"> <li>• ...</li> <li>• Adding or removing a Touch ID fingerprint or Face ID face".</li> </ul> <p>(<i>Id.</i>, at 16.)</p> <p>This database is shown in the figure from Apple Platform Security reproduced below:</p>

<u>Claim 15</u>	<u>Accused Instrumentalities</u>
	 <p>The diagram illustrates a Secure Enclave System on chip. It is divided into two main sections: a main system on chip (top) and a Secure Enclave (bottom). The main system on chip includes an Application Processor, NAND Flash controller, NAND Flash storage, AES engine, and Memory controller. The Secure Enclave includes a Secure Enclave Processor, Memory Protection Engine, NAND, Secure Enclave AES Engine, and PKA. A key is shown being passed from the Secure Enclave to the AES engine. The Secure Enclave is connected to the main system on chip via an I2C bus, which is also connected to Secure Nonvolatile Storage. A red arrow points to the Secure Nonvolatile Storage component.</p> <p>The Secure Enclave components.</p> <p>Database 105 (Ex. A, Apple Platform Security, at 9.)</p>
<p>15b. a transmitter sub-system comprising:</p>	<p><i>As set forth in elements 15b1, 15b2, and 15b3 below, the Accused Instrumentalities include a transmitter subsystem</i></p>
<p>15b1. a biometric sensor capable of receiving a biometric signal;</p>	<p><i>The Accused Instrumentalities include a biometric sensor configured to receive a biometric signal.</i></p>

<u>Claim 15</u>	<u>Accused Instrumentalities</u>
	<p>More specifically, the iPhone has at least one biometric sensor for capturing a fingerprint or a face (Touch ID and/or Face ID), namely a Touch ID sensor and a camera system with image sensor, respectively.</p> <p><b>Touch ID</b></p> <p>"Apple devices with a Touch ID sensor can be unlocked using a fingerprint." (Ex. A, Apple Platform Security, at 19.)</p> <p>"Touch ID is the fingerprint sensing system that makes secure access to supported Apple devices faster and easier. This technology reads fingerprint data from any angle and learns more about a user's fingerprint over time, with the <b>sensor</b> continuing to expand the fingerprint map as additional overlapping nodes are identified with each use." (<i>Id.</i>)</p> <p>"When the fingerprint sensor detects the touch of a finger, it triggers the advanced imaging array to scan the finger and sends the scan to the Secure Enclave." (<i>Id.</i>)</p> <p>The biometric sensor for Touch ID is located below the home button:</p> <p>"The Home button is a stack of different materials, capped with a sapphire crystal lens. The surrounding stainless-steel ring works as a ground and detects the user's finger. This action activates a capacitive touch sensor installed underneath the cover: A CMOS chip with small capacitors." (<a href="https://appleinsider.com/inside/touch-id">https://appleinsider.com/inside/touch-id</a>)</p>

<u>Claim 15</u>	<u>Accused Instrumentalities</u>
	 <p data-bbox="904 797 1172 829">Biometric sensor 121</p> <p data-bbox="612 867 1123 899">"Where is the Touch ID sensor located?"</p> <p data-bbox="612 927 1853 992">The Touch ID sensor is located either in the home button or - on the iPad Air (4th generation) - in the top button.</p> <p data-bbox="612 1024 1144 1057"><a href="https://support.apple.com/en-us/HT201371">https://support.apple.com/en-us/HT201371</a>)</p> <p data-bbox="612 1094 1438 1127">The image sensor captures an 88-by-88-pixel, 500 PPI raster scan:</p> <p data-bbox="612 1164 1896 1372">"The 88-by-88-pixel, 500-ppi raster scan is temporarily stored in encrypted memory within the Secure Enclave while being vectorized for analysis, and then it's discarded. The analysis utilizes subdermal ridge flow angle mapping, which is a lossy process that discards minutia data that would be required to reconstruct the user's actual fingerprint. The resulting map of nodes is stored without any identity information in an encrypted format that can only be read by the Secure Enclave, and is never sent to Apple or backed up to iCloud or iTunes."</p>

<u>Claim 15</u>	<u>Accused Instrumentalities</u>
	<p>(Ex. C, iOS Security white paper, at 8.)</p> <p><b>Face ID</b></p> <p>The biometric sensor for facial biometrics is a camera system ("<b>TrueDepth camera system</b>") with an image sensor.</p> <p>"With a simple glance, Face ID securely unlocks supported Apple devices. It provides intuitive and secure authentication enabled by the TrueDepth camera system, which uses advanced technologies to accurately map the geometry of a user's face." (Ex. A, Apple Platform Security, at 20.)</p> <p>To receive a biometric signal, the camera system with image sensor reads over 30,000 infrared points to capture depth information along with a two-dimensional infrared image.</p> <p>"After the TrueDepth camera confirms the presence of an attentive face, it projects and <b>reads over 30,000 infrared dots to form a depth map of the face along with a 2D infrared image</b>. This data is used to <b>create a sequence of 2D images and depth maps</b>, which are digitally signed and sent to the Secure Enclave. To counter both digital and physical spoofs, the TrueDepth camera randomizes the sequence of 2D images and depth map captures, and projects a device-specific random pattern. A portion of the Secure Neural Engine-protected within the Secure Enclave-transforms this data into a mathematical representation and compares that representation to the enrolled facial data. This enrolled facial data is itself a mathematical representation of the user's face captured across a variety of poses." (<i>Id.</i>)</p> <p>The camera system includes a biometric image sensor, namely a "CMOS image" sensor from Sony, to perform facial biometrics:</p>

<u>Claim 15</u>	<u>Accused Instrumentalities</u>
	 <p>(<a href="https://appleinsider.com/articles/17/09/09/inner-workings-of-apples-face-id-camera-detailed-in-report">https://appleinsider.com/articles/17/09/09/inner-workings-of-apples-face-id-camera-detailed-in-report</a>)</p>
<p>15b2. a transmitter sub-system controller capable of matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute; and</p>	<p><i>The Accused Instrumentalities include a transmitter controller configured to emit a secure access signal conveying information dependent upon said accessibility attribute.</i></p> <p>More specifically, the iPhone's System on Chip (SOC), i.e. the Secure Enclave with its Secure Enclave Processor (SEP) or a Secure Neural Engine contained therein, is a means (103) to check a match of the biometric signal with elements of the biometric signature database.</p> <p>"The <i>Secure Enclave</i> is a system on chip (SoC) that is included on all recent iPhone, ... devices" (Ex. A, Apple Platform Security, at 7.)</p>



<u>Claim 15</u>	<u>Accused Instrumentalities</u>
	<p>"During <b>matching</b>, the Secure Enclave <b>compares</b> incoming data from the biometric sensor against the stored templates <b>to determine whether to unlock the device</b> or respond that a match is valid (for Apple Pay, in-app, and other uses of Touch ID and Face ID). " (<i>Id.</i>, at 19.)</p> <p>The biometric signal received from the biometric sensor ("incoming data from the biometric sensor") is thus checked by the Secure Enclave and its SEP with the elements of the database of biometric signatures 105, i.e. the "stored templates", for the presence of a match.</p> <p>For Touch ID, the Secure Enclave match verification is performed as follows:</p> <p>"The Secure Enclave is responsible for processing fingerprint data from the Touch ID sensor, determining if there is a match against registered fingerprints, and then enabling access or purchases on behalf of the user ..." (Ex. C, iOS Security white paper, at 7.)</p> <p>"During enrollment, the resulting map of nodes is stored in an encrypted format that can be read only by the Secure Enclave as a template to compare against for future matches...." (Ex. A, Apple Platform Security, at 19.)</p> <p>"Touch ID can read multiple fingerprints, and it can read fingerprints in 360-degrees of orientation. It then creates a mathematical representation of your fingerprint and compares this to your enrolled fingerprint data to identify a match and unlock your device. " (<a href="https://support.apple.com/en-us/HT204587">https://support.apple.com/en-us/HT204587</a>)</p> <p>"Touch ID can read multiple fingerprints and recognize fingerprints at any orientation of the finger. The system then creates a mathematical representation of your fingerprint and compares it to the registered fingerprint data to determine a match and unlock your device." (<a href="https://support.apple.com/de-de/HT204587">https://support.apple.com/de-de/HT204587</a>)</p>

<u>Claim 15</u>	<u>Accused Instrumentalities</u>
	<p>For <b>Face ID</b>, the Secure Enclave has a neural network protected by it, i.e., a Secure Neural Engine, which is used to verify the match:</p> <p>"Face ID uses neural networks for determining attention, <b>matching</b>, and antispoofing, so a user can unlock their phone with a glance." (Ex. A, Apple Platform Security, at 20.)</p> <p>"A portion of the Secure Neural Engine-protected within the Secure Enclave-transforms this data into a mathematical representation and compares that representation to the enrolled facial data. This enrolled facial data is itself a mathematical representation of the user's face captured across a variety of poses." (<i>Id.</i>).</p> <p>"Facial matching security Facial matching is performed within the Secure Enclave using neural networks trained specifically for that purpose... Face ID data, including mathematical representations of a user's face, is encrypted and available only to the Secure Enclave. This data never leaves the device." (<i>Id.</i> at 23.)</p> <p>When the Secure Enclave, or more precisely the Touch ID or Face ID subsystem within the Secure Enclave, has determined that a match exists, an accessibility attribute is issued by the corresponding Touch ID or Face ID subsystem. This Touch ID or Face ID subsystem is also referred to as the SBIO. The accessibility attribute confirms that there is a match and that the iPhone is to be unlocked ("... determine whether to unlock the device ...").</p> <p>This confirmation of the match is signaled by the SBIO by issuing a random secret to which only the Touch ID or Face ID subsystem within the Secure Enclave has access:</p> <p>"During matching, the Secure Enclave compares incoming data from the biometric sensor against the stored templates to determine whether to unlock the device [...]." (<i>Id.</i> at 19.)</p>

<u>Claim 15</u>	<u>Accused Instrumentalities</u>
	<p>"Uses for Touch ID and Face ID</p> <p><b>Unlocking a device or user account</b></p> <p>[...] <b>keys for the highest class of Data Protection-which are held in the Secure Enclave [...].</b></p> <p>With Touch ID or Face ID enabled, the keys aren't discarded when the device or account locks; instead, <b>they're wrapped with a key that's given to the Touch ID or Face ID subsystem inside the Secure Enclave.</b> When a user attempts to unlock the device or account, <b>if the device detects a successful match, it provides the key for unwrapping the Data Protection keys,</b> and the device or account is unlocked. This process provides additional protection by requiring cooperation between the Data Protection and Touch ID or Face ID subsystems to unlock the device."</p> <p>(<i>Id.</i> at 24.)</p> <p>"The class key is protected with the hardware UID and, for some classes, the user's passcode." (<i>Id.</i> at 85.)</p> <p><b>"Complete Protection</b></p> <p>(<i>NSFileProtectionComplete</i>): The class key is protected with a key derived from the user passcode or password and the device UID. Shortly after the user locks a device (10 seconds, if the Require Password setting is Immediately), the decrypted class key is discarded, <b>rendering all data in this class inaccessible until the user enters the passcode again or unlocks (logs in to) the device using Touch ID or Face ID.</b>"</p> <p>(<i>Id.</i> at 86.)</p> <p>The Touch ID or Face ID subsystem within the Secure Enclave is the SBIO shown below. SBIO is an application that runs within the Secure Enclave on the SEP and is responsible for checking the match of biometric features. SBIO receives the corresponding biometric data from a biometric sensor, such as the Touch ID sensor. The random secret is stored in a memory ("bio memory") associated with the</p>

Claim 15	Accused Instrumentalities
	<p>SBIO and is output from the bio memory upon match, see step 3 in the diagram below ("3) upon successful match send random secret to SKS"):</p> <p>(Ex. B, Behind the Scenes with iOS Security, at 34.)</p> <p>The class keys are encrypted with a master key:</p>

<u>Claim 15</u>	<u>Accused Instrumentalities</u>
	<p data-bbox="623 289 1044 365"><b>User Keybags</b></p> <p data-bbox="623 386 910 440">Background</p> <p data-bbox="623 496 1613 537">Sets of keys generated for each user to protect their data at rest</p> <p data-bbox="623 561 1704 602">Keys wrapped by master key derived from user passcode and SEP UID</p> <p data-bbox="623 626 1810 667">After 10 incorrect passcode entries, SEP will not process any further attempts</p> <p data-bbox="623 691 1693 732">Different policy associated with each keybag key—Usage, availability</p> <p data-bbox="623 756 757 789"><i>(Id., at 25.)</i></p> <p data-bbox="623 865 1885 1073">The random secret is issued to SKS. SKS is a Secure Key Service application which is located within the Secure Enclave on the SEP and is responsible for decrypting class keys. The random secret provided by SBIO is used to decrypt a master key ("4) decrypt master key"). The master key is concatenated with the UID of the SEP and thus class keys are decrypted and added to the SKS keyring ("5) decrypt class keys, add to keyring") for further use by the Secure Enclave. The decrypted class keys include, for example, the class key of class A.</p>
15b3. a transmitter capable of emitting a secure access signal conveying information dependent upon said accessibility attribute; and	<p data-bbox="623 1117 1810 1182"><i>The Accused Instrumentalities include a transmitter configured to emit a secure access signal conveying information dependent upon said accessibility attribute.</i></p> <p data-bbox="623 1222 1710 1255">For example, the Secure Enclave emits a signal with ephemerally re-encrypted file keys:</p> <p data-bbox="623 1295 1853 1391">"sepOS can then use the ephemeral wrapping key to wrap file keys for use by the Application Processor file-system driver. When the file-system driver reads or writes a file, it sends the wrapped key to the AES Engine."</p>

<u>Claim 15</u>	<u>Accused Instrumentalities</u>
	<p>(Ex. A, Apple Platform Security, at 14.)</p> <p>"All wrapped file key handling occurs in the Secure Enclave; the file key is never directly exposed to the Application Processor. [...] When the Secure Enclave unwraps a file's keys, they're rewrapped with the ephemeral key and sent back to the Application Processor."  <i>(Id.</i> at 85.)</p> <p>The signal with the ephemerally re-encrypted file keys is a secure signal because it comes from the Secure Enclave and thus from a secure environment. Furthermore, the signal is secure because the transmitted information is encrypted. The emitted file keys are encrypted with the ephemeral key:</p> <p>"All wrapped file key handling occurs in the Secure Enclave; the file key is never directly exposed to the Application Processor. At startup, the Secure Enclave negotiates an ephemeral key with the AES Engine. When the Secure Enclave unwraps a file's keys, they're rewrapped with the ephemeral key and sent back to the Application Processor."  <i>(Id.)</i></p> <div data-bbox="612 876 1893 1372" style="background-color: black; color: white; padding: 10px;"> <h2 style="margin: 0;">Filesystem Data Protection</h2> <h3 style="margin: 0;">Overview</h3> <p style="margin: 0;">File blocks are encrypted using AES-XTS with 128-bit keys</p> <p style="margin: 0;">Each file on the user partition is encrypted using a unique random key chosen by SEP</p> <p style="margin: 0;">Raw file keys are never exposed to the AP</p> <ul style="list-style-type: none"> <li>• Wrapped with a key from the user keybag for long-term storage</li> <li>• Wrapped with an ephemeral key while in use, bound to boot session</li> </ul> </div>


<u>Claim 15</u>	<u>Accused Instrumentalities</u>
	<p>(Ex. B, Behind the Scenes with iOS Security, at 29.)</p> <div data-bbox="612 344 1783 1003" style="background-color: black; color: white; padding: 10px;"> <h3 style="text-align: center;">Filesystem Data Protection</h3> <p>The diagram illustrates the process of filesystem data protection across four layers: User, Kernel, SEP (Secure Enclave), and Hardware.          <ul style="list-style-type: none"> <li><b>User Layer:</b> A user initiates an <code>open("foo.txt", ...)</code> operation.</li> <li><b>Kernel Layer:</b> <ul style="list-style-type: none"> <li>Step 1: Fetch wrapped file_key from metadata (HFS).</li> <li>Step 4: Send IO command with ephemerally wrapped file_key (NVME Driver).</li> </ul> </li> <li><b>SEP Layer:</b> <ul style="list-style-type: none"> <li>Step 2: Unwrap file_key using keybag key (Key Store).</li> <li>Step 3: Wrap file_key using ephemeral_key, return ephemerally wrapped file_key to kernel (AES Engine).</li> </ul> </li> <li><b>Hardware Layer:</b> <ul style="list-style-type: none"> <li>NAND storage.</li> <li>Storage Controller.</li> <li>Clear Text data flow between NVME Driver and Storage Controller.</li> <li>Ephemerally wrapped file_key flow from Storage Controller to NVME Driver.</li> <li>Ephemeral Key established on boot (AES Engine).</li> </ul> </li> </ul> </p> </div> <p>(<i>Id.</i>, at 30.)</p> <p>The information transmitted by the emitted signal, i.e., the ephemerally re-encrypted file keys, is dependent on the availability attribute, i.e., the confirmation that a biometric "template match" exists. This confirmation is signaled by the issuance of the random secret (cf. step 3): Only if there is a confirmation of the match and the random secret is issued by the Touch ID or Face ID subsystem within the Secure Enclave, i.e. SBIO, the class key is available for re-encrypting the file keys.</p> <p>The re-encrypted file keys are therefore information which is emitted depending on the fact that the availability attribute has been emitted.</p>


<u>Claim 15</u>	<u>Accused Instrumentalities</u>
15c. a receiver sub-system comprising:	<i>As set forth in elements 15c1 and 15c2 below, the Accused Instrumentalities include a receiver sub-system.</i>
15c1. a receiver sub-system controller capable of: receiving the transmitted secure access signal; and	<p><i>The Accused Instrumentalities include a receiver sub-system controller capable of: receiving the transmitted secure access signal.</i></p> <p>An application processor (118) with file system driver, which receives the ephemerally re-encrypted file key. To read files from the NAND Flash storage, the application processor processes the received signal by creating a read command with the ephemerally wrapped file key ("IO command with ephemerally wrapped file_key") and sends it to the storage controller (109) (NAND Flash controller with AES engine). This read command provides the storage controller with all the information required to read and decrypt the encrypted file from the NAND flash storage:</p> <div data-bbox="612 699 1785 1354" data-label="Diagram"> <p>The diagram, titled "Filesystem Data Protection", illustrates the interaction between different system layers during file access. It is divided into four main sections: User, Kernel, SEP (Secure Element Processor), and Hardware.          <ul style="list-style-type: none"> <li><b>User:</b> Initiates the process with the command <code>open("foo.txt", ...)</code>.</li> <li><b>Kernel:</b> Contains the <b>HFS</b> (Hierarchical File System) layer, which performs the following steps:             <ol style="list-style-type: none"> <li>Fetch wrapped file_key from metadata.</li> <li>Send IO command with ephemerally wrapped file_key to the <b>NVME Driver</b>.</li> </ol> </li> <li><b>SEP:</b> Contains the <b>Key Store</b> and <b>AES Engine</b>.             <ul style="list-style-type: none"> <li>The <b>Key Store</b> provides a <b>keybag key</b> to the <b>AES Engine</b>.</li> <li>The <b>AES Engine</b> wraps the file_key using the ephemeral_key and returns the ephemerally wrapped file_key to the kernel.</li> <li>An <b>Ephemeral Key</b> is established on boot.</li> </ul> </li> <li><b>Hardware:</b> Contains the <b>NAND</b> and <b>Storage Controller</b>.             <ul style="list-style-type: none"> <li>The <b>Storage Controller</b> receives a <b>Clear Text</b> command from the <b>NVME Driver</b>.</li> <li>The <b>Storage Controller</b> interacts with the <b>NAND</b> and the <b>AES Engine</b>.</li> <li><b>Cipher Text</b> is sent between the <b>NAND</b> and the <b>Storage Controller</b>.</li> </ul> </li> </ul> </p></div>

(Ex. B, Behind the Scenes with iOS Security, at 30.)

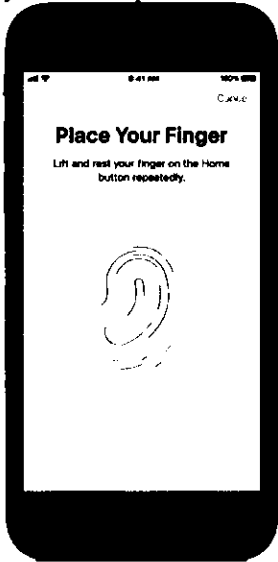


<u>Claim 15</u>	<u>Accused Instrumentalities</u>
	<p>"sepOS can then use the ephemeral wrapping key to wrap file keys <b>for use by the Application Processor file-system driver. When the file-system driver reads or writes a file, it sends the wrapped key to the AES Engine.</b>" (Ex. A, Apple Platform Security, at 14.)</p> <p>"All wrapped file key handling occurs in the Secure Enclave; the file key is never directly exposed to the Application Processor. [...] When the Secure Enclave unwraps a file's keys, they're rewrapped with the ephemeral key and <b>sent back to the Application Processor.</b>" (<i>Id.</i>, at 85.)</p>
15c2. providing conditional access to the controlled item dependent upon said information;	<p><i>The Accused Instrumentalities include a receiver sub-system configured to provide conditional access to the controlled item dependent upon said information.</i></p> <p>More specifically, the controlled item is a locking mechanism of the door lock of the user's home. The Accused Instrumentalities are configured to provide secure access to the user's home via Yale Smart Locks when the user provides biometric signal to the Accused Instrumentalities via Touch ID or Face ID.</p> <p>"When the "Secure Remote Access" feature is turned on, <b>the app will use your phone's built-in authentication tools to prompt fingerprint or facial recognition before you can unlock or lock your home remotely (note: if your phone does not have these features, it will prompt you to use your PIN code).</b> This further ensures that your door is only operated by the right people at the time you intend for it." (<a href="https://us.yalehome.com/en/yale-news/blog/latest-blog-posts/introducing-biometric-verification-for-august-and-yale-locks1/">https://us.yalehome.com/en/yale-news/blog/latest-blog-posts/introducing-biometric-verification-for-august-and-yale-locks1/</a>)</p>

<u>Claim 15</u>	<u>Accused Instrumentalities</u>
	 <p>The screenshot shows a mobile application interface for Yale. At the top, there is a yellow circular logo with the word "Yale" in black. To the left of the logo is a hamburger menu icon and the word "Open". To the right is a magnifying glass search icon. Below the navigation bar, the text "Introducing Biometric Verification for August and Yale Locks" is displayed in a bold, black font. Underneath this text is a photograph of a hand holding a smartphone. The phone's screen displays a biometric verification interface with a large red circle in the center containing a white "1G" logo. The background of the photo is a blurred outdoor scene with green foliage.</p> <p>(<a href="https://us.yalehome.com/en/yale-news/blog/latest-blog-posts/introducing-biometric-verification-for-august-and-yale-locks1/">https://us.yalehome.com/en/yale-news/blog/latest-blog-posts/introducing-biometric-verification-for-august-and-yale-locks1/</a>)</p>


<u>Claim 15</u>	<u>Accused Instrumentalities</u>
	 <p>(<a href="https://www.apple.com/shop/product/HPAR2ZM/A/yale-assure-lock-sl-touchscreen-deadbolt-black">https://www.apple.com/shop/product/HPAR2ZM/A/yale-assure-lock-sl-touchscreen-deadbolt-black</a>)</p>
15d. wherein the transmitter sub-system controller is further capable of:	<i>The Accused Instrumentalities include a transmitter sub-system controller that is configured to be used as set forth in elements 15d1, 15d2, and 15d3 below.</i>

<u>Claim 15</u>	<u>Accused Instrumentalities</u>
<p>15d1. receiving a series of entries of the biometric signal, said series being characterised according to at least one of the number of said entries and a duration of each said entry;</p>	<p><i>The Accused Instrumentalities include a transmitter sub-system controller configured to receive a series of entries of the biometric signal, said series being characterized according to at least one of the number of said entries and a duration of each said entry.</i></p> <p>More specifically, the Secure Enclave of the iPhone with the Secure Enclave Processor forms the means for receiving a series of entries of the biometric signal.</p> <p>"Apple's biometric security architecture relies on a strict separation of responsibilities between the biometric sensor and the Secure Enclave, and a secure connection between the two. The sensor captures the biometric image and securely transmits it to the Secure Enclave." (Ex. A, Apple Platform Security, at 19.)</p> <p><b>Touch ID</b></p> <p>When a finger is placed on the biometric sensor, the finger is scanned and the corresponding biometric signal entry is received by the Secure Enclave.</p> <p>"When the fingerprint sensor detects the touch of a finger, it triggers the advanced imaging array to scan the finger and sends the scan to the Secure Enclave." (<i>Id.</i>)</p> <p>To enroll a fingerprint in the database, the iPhone's fingerprint sensor records an entry of a biometric signal when the user places his finger on the sensor. This is done multiple times, resulting in a series of entries of such biometric signals.</p> <p>Receiving a series of entries of the biometric signal by repeatedly placing a finger on the Touch ID sensor will use Touch ID on iPhone.</p> <p><b>Set up Touch ID</b></p> <p>Before you can set up Touch ID, you must first create a <a href="#">code</a> for your device,* then follow these steps:</p>

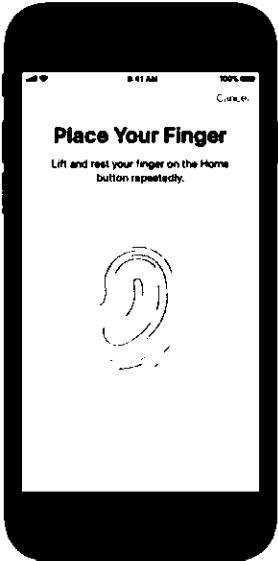
<u>Claim 15</u>	<u>Accused Instrumentalities</u>
	<p>19. Make sure the Touch ID sensor and your finger are clean and dry.</p> <p>20. Tap Settings &gt; Touch ID &amp; Code, and then enter your code.</p> <p>21. Tap "Add fingerprint" and hold the device as you normally would when touching the Touch ID sensor.</p> <p>22. Touch the Touch ID sensor with one finger, but do not press. Keep your finger on the button until you feel a quick vibration or are prompted to lift your finger.</p>  <p>23. Continue by raising and slowly lowering your finger over and over again, changing the position of your finger just a tiny bit at a time.</p> <p>24. The next screen will ask you to change your finger position. Hold your device as you normally would when unlocking it. Touch the Touch ID sensor with the outer edges of your fingertip instead of the middle part as you would during the first scan.”</p> <p>(<a href="https://support.apple.com/en-us/HT201371">https://support.apple.com/en-us/HT201371</a>)</p>

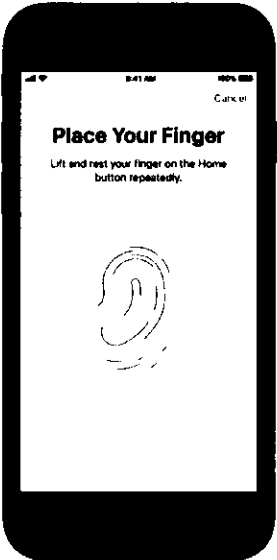
<u>Claim 15</u>	<u>Accused Instrumentalities</u>
	<p>Accordingly, the user is prompted to place his finger on the sensor several times, in particular in accordance with step 5. Each time the finger is placed on the sensor, a corresponding biometric entry is generated, i.e. a series of such entries. All these entries, which result from placing the same finger on the sensor, form a series.</p> <p><b>Face ID</b></p> <p>The means for receiving a series of entries of the biometric signal includes a Secure Neural Engine, which is protected by the Secure Enclave. The Secure Neural Engine transforms the series of entries of the biometric signal received by the Secure Enclave into a biometric signature ("mathematical representation").</p> <p>"After the TrueDepth camera confirms the presence of an attentive face, it projects and reads over 30,000 infrared dots to form a depth map of the face along with a 2D infrared image. This data is used to create <b>a sequence of 2D images and depth maps</b>, which are digitally signed and <b>sent to the Secure Enclave</b>. To counter both digital and physical spoofs, the TrueDepth camera randomizes the sequence of 2D images and depth map captures, and projects a device-specific random pattern. A portion of the <b>Secure Neural Engine-protected</b> within the Secure Enclave-transforms this data into a mathematical representation and compares that representation to the enrolled facial data. This enrolled facial data is itself a mathematical representation of the user's face captured across a variety of poses." (Ex. A, Apple Platform Security, at 20.)</p> <p>Each entry of the biometric signal thus contains a two-dimensional infrared image with 30,000 infrared points for capturing depth information. By continuously capturing such infrared images into a Face ID scan while the user moves his head into different poses, a series of entries of the biometric signal results. Two such Face ID scans are required to generate a biometric signature of a single face, so that two series of entries of the biometric signal are received accordingly.</p> <p>Using Face ID on iPhone</p> <ol style="list-style-type: none"> <li>1. Tap Settings &gt; Face ID &amp; Code. Enter your code when prompted.</li> <li>2. Tap on "Configure Face ID".</li> </ol>

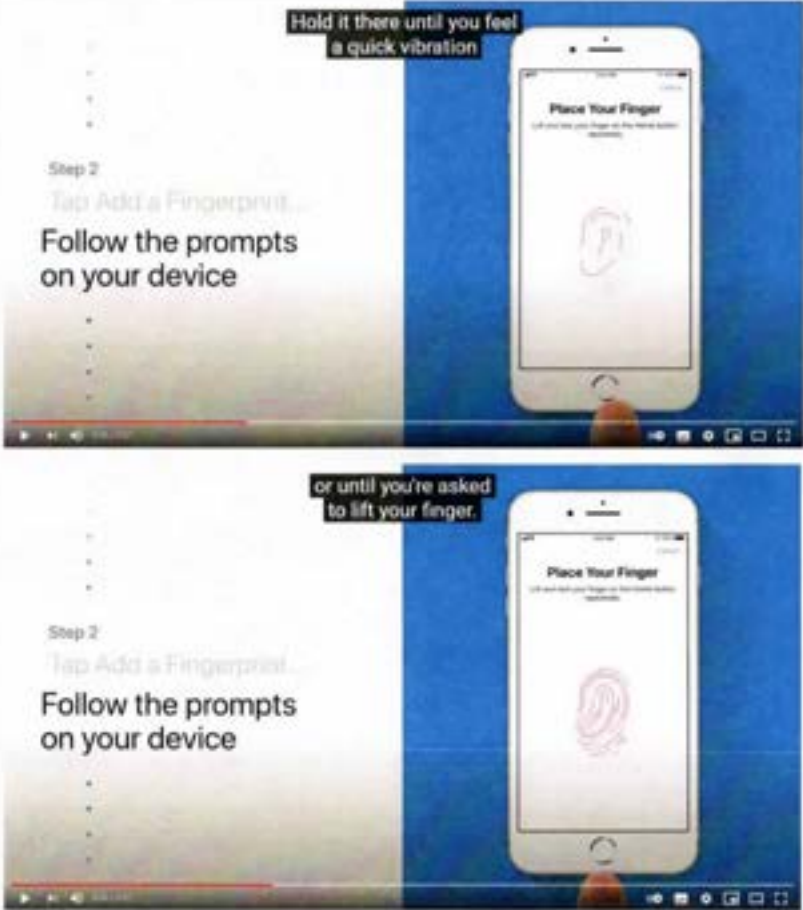
<u>Claim 15</u>	<u>Accused Instrumentalities</u>
	<p>3. Hold the device in portrait mode in front of your face and tap "Let's go".</p> <p>4. Make sure your face is inside the frame and slowly move your head until the circle shown is completed. If you can't move your head, tap on "Options for operating aids".</p> <p>5. After performing the first Face ID scan, tap "Next".</p> <p>6. Again, slowly describe a circle with your head until it is completed.</p> <p>7. Tap "Done."</p> <p>(<a href="https://support.apple.com/en-us/HT208109">https://support.apple.com/en-us/HT208109</a>)</p> <p>The biometric signature of a single face is thus determined by two successive Face ID scans, each of which receives a series of entries of the biometric signal (compare steps 4. and 6. above).</p> <p>To register a second face, the iPhone offers a corresponding option in its settings. If the user selects the option "Set up an alternative appearance" as shown in the figure below on <a href="https://www.macworld.co.uk/how-to/second-face-id-3803421/">https://www.macworld.co.uk/how-to/second-face-id-3803421/</a>, a second face is registered by the iPhone in the same way as the first face.</p>


<u>Claim 15</u>	<u>Accused Instrumentalities</u>
	 <p>The series of entries of the biometric signal is identified on the iPhone by both the number and duration of each such entry.</p> <p><b>Touch ID</b></p> <p>According to step 5 of the instructions <a href="https://support.apple.com/en-us/HT201371">https://support.apple.com/en-us/HT201371</a>, for the enrollment of a single finger, the user has to repeatedly place the respective finger on the sensor and thus a number of entries in a row predetermined via the user guidance are captured by the iPhone. Each one of the entries must also be of a predetermined duration given to the user via the iPhone display, i.e. the user's finger must remain on the sensor for a predetermined duration for each entry of the biometric signal in order to capture the biometric signal during this time.</p>



<u>Claim 15</u>	<u>Accused Instrumentalities</u>
	<p>Receiving a series of entries of the biometric signal by repeatedly placing a finger on the Touch ID sensor will use Touch ID on iPhone and iPad.</p> <p><b>Set up Touch ID</b></p> <p>...</p> <p>4. Touch the Touch ID sensor with one finger, but do not press. Keep your finger on the button until you feel a quick vibration or are prompted to lift your finger.</p>  <p>5. Continue by raising and slowly lowering your finger over and over again, changing the position of your finger just a tiny bit at a time.</p> <p>6. The next screen will ask you to change your finger position. Hold your device as you normally would when unlocking it. Touch the Touch ID sensor with the outer edges of your fingertip instead of the middle part as you did during the first scan.</p> <p>(<a href="https://support.apple.com/en-us/HT201371">https://support.apple.com/en-us/HT201371</a>)</p>

<u>Claim 15</u>	<u>Accused Instrumentalities</u>
	<p>After placing a finger on the home button, a fingerprint appears on the display with red progress bars spreading along some of the papillary bars until the capture of the biometric entry in question is complete:</p>  <p>When the required duration is reached, the iPhone vibrates after an entry of the biometric signal is received or it issues a prompt to the user to lift the finger. The user then lifts the finger in question and replaces the same finger so that the iPhone receives a series of biometric signal entries of sufficient duration for that finger. The process is repeated for the same finger for as long as required according to the iPhone's user guidance.</p> <p>This is shown in the Apple You Tube video (32) How to set up Touch ID on your iPhone or iPad - Apple Support - YouTube (<a href="https://www.youtube.com/watch?v=xTZ2LALWZlg">https://www.youtube.com/watch?v=xTZ2LALWZlg</a>):</p>


<u>Claim 15</u>	<u>Accused Instrumentalities</u>
	 <p>Both the number of entries, i.e. the number of repetitions for placing the finger on the screen, and their respective duration are specified by the iPhone via the user guidance.</p>

<u>Claim 15</u>	<u>Accused Instrumentalities</u>
	<p><b>Face ID</b></p> <p>The user moves his face in front of the camera to strike different poses, and the camera system with image sensor continuously captures a large number of biometric entries, i.e. here the 2D images with depth information, in a row.</p> <p>"This enrolled facial data is itself a mathematical representation of the user's face captured across a variety of poses." (Ex. A, Apple Platform Security, at 20.)</p> <p>The sufficient duration of an entry for a pose, i.e. an angular position of the head specified via the user interface of the iPhone, is indicated to the user by the transformation of a gray line into a green line:</p>  <p>(Individual images taken from: <a href="https://support.apple.com/en-us/HT208109">https://support.apple.com/en-us/HT208109</a>)</p>
<p>15d2. mapping said series into an instruction; and</p>	<p><i>The Accused Instrumentalities include a transmitter sub-system controller configured to map said series into an instruction.</i></p>

<u>Claim 15</u>	<u>Accused Instrumentalities</u>
	<p>More specifically, the Secure Enclave of the iPhone contains means to assign the received row to an instruction: The Secure Enclave, after receiving the full set of entries of the biometric signal, assigns this set to an instruction for processing, encrypting and storing the biometric signature ("Touch ID and Face ID template data").</p> <p>"The sensor captures the biometric image and securely transmits it to the Secure Enclave. During enrollment, the Secure Enclave processes, encrypts, and stores the corresponding Touch ID and Face ID template data." (Ex. A, Apple Platform Security, at 19.)</p> <p>To carry out this instruction, the Secure Enclave has its own processor: "The Secure Enclave Processor provides the main computing power for the Secure Enclave." (<i>Id.</i>, at 10.)</p> <p><b>Touch ID</b></p> <p>The instruction here involves the processing of under-the-skin fingerprint characteristics and their encrypted storage.</p> <p>"The analysis uses subdermal ridge flow angle mapping, a lossy process that discards "finger minutiae data" that would be required to reconstruct the user's actual fingerprint. During enrollment, the resulting map of nodes is stored in an encrypted format that can be read only by the Secure Enclave as a template to compare against for future matches, but without any identity information." (<i>Id.</i>, at 19.)</p> <p><b>Face ID</b></p> <p>The instruction involves the transformation of the set of entries of the biometric signal captured via the Face ID scans into a mathematical representation, i.e. the biometric signature of the face in question by the Secure Neural Engine of the Secure Enclave, as well as its encryption and storage.</p>

<u>Claim 15</u>	<u>Accused Instrumentalities</u>
	<p>"A portion of the Secure Neural Engine-protected within the Secure Enclave-transforms this data into a mathematical representation and compares that representation to the enrolled facial data. This enrolled facial data is itself a mathematical representation of the user's face captured across a variety of poses." (<i>Id.</i>, at 20.)</p> <p>"Face ID data, including mathematical representations of a user's face, is encrypted and available only to the Secure Enclave. This data never leaves the device. It's not sent to Apple, nor is it included in device backups. The following Face ID data is saved, encrypted only for use by the Secure Enclave, during normal operation:</p> <ul style="list-style-type: none"> <li>• The mathematical representations of a user's face calculated during enrollment</li> <li>• ..."</li> </ul> <p>(<i>Id.</i>, at 23.)</p>
15d3. populating the data base according to the instruction,	<p><b><i>The Accused Instrumentalities include a transmitter sub-system controller configured to populate the database according to the instruction.</i></b></p> <p>More specifically, the Secure Enclave stores the biometric signature, i.e. the encrypted mathematical representation of the fingerprint or face, in the database 105, i.e. the "secure nonvolatile storage":</p> <p>"The secure nonvolatile storage is used for all anti-replay services in the Secure Enclave. Anti-replay services on the Secure Enclave are used for revocation of data over events that mark anti-replay boundaries including, but not limited to, the following:</p> <ul style="list-style-type: none"> <li>• ...</li> <li>• ...</li> <li>• Adding or removing a Touch ID fingerprint or Face ID face".</li> </ul> <p>(Ex. A, Apple Platform Security, at 16.)</p> <p>"During enrollment, the Secure Enclave processes, encrypts, and stores the corresponding Touch ID and Face ID template data." (<i>Id.</i>, at 19.)</p>

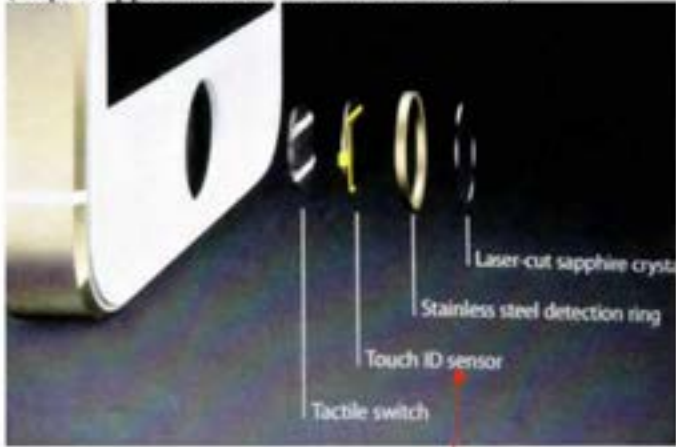
<u>Claim 15</u>	<u>Accused Instrumentalities</u>
	<p><b>Touch ID</b></p> <p>"During enrollment, the resulting map of nodes is stored in an encrypted format that can be read only by the Secure Enclave as a template to compare against for future matches...." (<i>Id.</i>)</p> <p><b>Face ID</b></p> <p>The following Face ID data is saved, encrypted only for use by the Secure Enclave, during normal operation:</p> <ul style="list-style-type: none"> <li>• The mathematical representations of a user's face calculated during enrollment". (<i>Id.</i>, at 23.)</li> </ul>
<p>wherein the controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing device.</p>	<p><i>The Accused Instrumentalities are configured to provide access to the controlled item, wherein the controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing device.</i></p> <p>More specifically, the controlled item is a locking mechanism of the door lock of the user's home. The Accused Instrumentalities are configured to provide secure access to the user's home via Yale Smart Locks when the user provides biometric signal to the Accused Instrumentalities via Touch ID or Face ID.</p> <p>"When the "Secure Remote Access" feature is turned on, the app will use your phone's built-in authentication tools to prompt fingerprint or facial recognition before you can unlock or lock your home remotely (note: if your phone does not have these features, it will prompt you to use your PIN code). This further ensures that your door is only operated by the right people at the time you intend for it." (<a href="https://us.yalehome.com/en/yale-news/blog/latest-blog-posts/introducing-biometric-verification-for-august-and-yale-locks1/">https://us.yalehome.com/en/yale-news/blog/latest-blog-posts/introducing-biometric-verification-for-august-and-yale-locks1/</a>)</p>

<u>Claim 15</u>	<u>Accused Instrumentalities</u>
	 <p>The screenshot shows a mobile application interface for Yale. At the top, there is a yellow circular logo with the word "Yale" in black. To the left of the logo is a hamburger menu icon and the word "Open". To the right is a magnifying glass search icon. Below the navigation bar, the text "Introducing Biometric Verification for August and Yale Locks" is displayed in a bold, black font. Underneath the text is a photograph of a hand holding a smartphone. The phone's screen displays a biometric verification interface with a red circular icon in the center. Below the photograph, a URL is provided: <a href="https://us.yalehome.com/en/yale-news/blog/latest-blog-posts/introducing-biometric-verification-for-august-and-yale-locks1/">(https://us.yalehome.com/en/yale-news/blog/latest-blog-posts/introducing-biometric-verification-for-august-and-yale-locks1/)</a></p>




<u>Claim 15</u>	<u>Accused Instrumentalities</u>
	 <p>(<a href="https://www.apple.com/shop/product/HPAR2ZM/A/yale-assure-lock-sl-touchscreen-deadbolt-black">https://www.apple.com/shop/product/HPAR2ZM/A/yale-assure-lock-sl-touchscreen-deadbolt-black</a>)</p>

<u>Claim 16</u>	<u>Accused Instrumentalities</u>
16. A transmitter sub-system for operating in a system for providing secure access to a controlled item, wherein the transmitter sub-system comprises:	<i>To the extent that the preamble is deemed to be a limitation, the Accused Instrumentalities include a transmitter sub-system for operating in a system for providing secure access to a controlled item in accordance with this claim.</i>
16a. a biometric sensor capable of receiving a biometric signal;	<p><i>The Accused Instrumentalities include a biometric sensor configured to receive a biometric signal.</i></p> <p>More specifically, the iPhone has at least one biometric sensor for capturing a fingerprint or a face (Touch ID and/or Face ID), namely a Touch ID sensor and a camera system with image sensor, respectively.</p> <p><b>Touch ID</b></p> <p>"Apple devices with a Touch ID sensor can be unlocked using a fingerprint." (Ex. A, Apple Platform Security, at 19.)</p> <p>"Touch ID is the fingerprint sensing system that makes secure access to supported Apple devices faster and easier. This technology reads fingerprint data from any angle and learns more about a user's fingerprint over time, with the <b>sensor</b> continuing to expand the fingerprint map as additional overlapping nodes are identified with each use." (<i>Id.</i>)</p> <p>"When the fingerprint sensor detects the touch of a finger, it triggers the advanced imaging array to scan the finger and sends the scan to the Secure Enclave." (<i>Id.</i>)</p> <p>The biometric sensor for Touch ID is located below the home button:</p>

<u>Claim 16</u>	<u>Accused Instrumentalities</u>
	<p data-bbox="612 277 1879 415">"The Home button is a stack of different materials, capped with a sapphire crystal lens. The surrounding stainless-steel ring works as a ground and detects the user's finger. This action activates a capacitive touch sensor installed underneath the cover: A CMOS chip with small capacitors." (<a href="https://appleinsider.com/inside/touch-id">https://appleinsider.com/inside/touch-id</a>)</p>  <p data-bbox="910 935 1172 964">Biometric sensor 121</p> <p data-bbox="612 1008 1129 1037">"Where is the Touch ID sensor located?"</p> <p data-bbox="612 1068 1853 1133">The Touch ID sensor is located either in the home button or - on the iPad Air (4th generation) - in the top button.</p> <p data-bbox="612 1164 1144 1193">(https://support.apple.com/en-us/HT201371)</p> <p data-bbox="612 1235 1438 1265">The image sensor captures an 88-by-88-pixel, 500 PPI raster scan:</p> <p data-bbox="612 1307 1885 1372">"The 88-by-88-pixel, 500-ppi raster scan is temporarily stored in encrypted memory within the Secure Enclave while being vectorized for analysis, and then it's discarded. The analysis utilizes subdermal</p>

<u>Claim 16</u>	<u>Accused Instrumentalities</u>
	<p>ridge flow angle mapping, which is a lossy process that discards minutia data that would be required to reconstruct the user's actual fingerprint. The resulting map of nodes is stored without any identity information in an encrypted format that can only be read by the Secure Enclave, and is never sent to Apple or backed up to iCloud or iTunes. ” (Ex. C, iOS Security white paper, at 8.)</p> <p><b>Face ID</b></p> <p>The biometric sensor for facial biometrics is a camera system ("<b>TrueDepth camera system</b>") with an image sensor.</p> <p>"With a simple glance, Face ID securely unlocks supported Apple devices. It provides intuitive and secure authentication enabled by the TrueDepth camera system, which uses advanced technologies to accurately map the geometry of a user's face. ” (Ex. A, Apple Platform Security, at 20.)</p> <p>To receive a biometric signal, the camera system with image sensor reads over 30,000 infrared points to capture depth information along with a two-dimensional infrared image.</p> <p>"After the TrueDepth camera confirms the presence of an attentive face, it projects and <b>reads over 30,000 infrared dots to form a depth map of the face along with a 2D infrared image.</b> This data is used to <b>create a sequence of 2D images and depth maps,</b> which are digitally signed and sent to the Secure Enclave. To counter both digital and physical spoofs, the TrueDepth camera randomizes the sequence of 2D images and depth map captures, and projects a device-specific random pattern. A portion of the Secure Neural Engine-protected within the Secure Enclave-transforms this data into a mathematical representation and compares that representation to the enrolled facial data. This enrolled facial data is itself a mathematical representation of the user's face captured across a variety of poses." (<i>Id.</i>)</p>

<u>Claim 16</u>	<u>Accused Instrumentalities</u>
	<p>The camera system includes a biometric image sensor, namely a "CMOS image" sensor from Sony, to perform facial biometrics:</p>  <p>(<a href="https://appleinsider.com/articles/17/09/09/inner-workings-of-apples-face-id-camera-detailed-in-report">https://appleinsider.com/articles/17/09/09/inner-workings-of-apples-face-id-camera-detailed-in-report</a>)</p>
<p>16b. a controller capable of matching the biometric signal against members of a database of biometric signatures to thereby output an accessibility attribute; and</p>	<p><i>The Accused Instrumentalities include a transmitter controller configured to emit a secure access signal conveying information dependent upon said accessibility attribute.</i></p> <p>More specifically, the iPhone's System on Chip (SOC), i.e. the Secure Enclave with its Secure Enclave Processor (SEP) or a Secure Neural Engine contained therein, is a means (103) to check a match of the biometric signal with elements of the biometric signature database.</p>

<u>Claim 16</u>	<u>Accused Instrumentalities</u>
	<p>"The <i>Secure Enclave</i> is a system on chip (SoC) that is included on all recent iPhone, ... devices" (Ex. A, Apple Platform Security, at 7.)</p> <p>"During <b>matching</b>, the Secure Enclave <b>compares</b> incoming data from the biometric sensor against the stored templates <b>to determine whether to unlock the device</b> or respond that a match is valid (for Apple Pay, in-app, and other uses of Touch ID and Face ID). " (<i>Id.</i>, at 19.)</p> <p>The biometric signal received from the biometric sensor ("incoming data from the biometric sensor") is thus checked by the Secure Enclave and its SEP with the elements of the database of biometric signatures 105, i.e. the "stored templates", for the presence of a match.</p> <p>For Touch ID, the Secure Enclave match verification is performed as follows:</p> <p>"The Secure Enclave is responsible for processing fingerprint data from the Touch ID sensor, determining if there is a match against registered fingerprints, and then enabling access or purchases on behalf of the user ..." (Ex. C, iOS Security white paper, at 7.)</p> <p>"During enrollment, the resulting map of nodes is stored in an encrypted format that can be read only by the Secure Enclave as a template to compare against for future matches...." (Ex. A, Apple Platform Security, at 19.)</p> <p>"Touch ID can read multiple fingerprints, and it can read fingerprints in 360-degrees of orientation. It then creates a mathematical representation of your fingerprint and compares this to your enrolled fingerprint data to identify a match and unlock your device. " (<a href="https://support.apple.com/en-us/HT204587">https://support.apple.com/en-us/HT204587</a>)</p> <p>"Touch ID can read multiple fingerprints and recognize fingerprints at any orientation of the finger. The system then creates a mathematical representation of your fingerprint and compares it to the registered fingerprint data to determine a match and unlock your device."</p>

<u>Claim 16</u>	<u>Accused Instrumentalities</u>
	<p>(<a href="https://support.apple.com/de-de/HT204587">https://support.apple.com/de-de/HT204587</a>)</p> <p>For <b>Face ID</b>, the Secure Enclave has a neural network protected by it, i.e., a Secure Neural Engine, which is used to verify the match:</p> <p>"Face ID uses neural networks for determining attention, <b>matching</b>, and antispoofing, so a user can unlock their phone with a glance." (Ex. A, Apple Platform Security, at 20.)</p> <p>"A portion of the Secure Neural Engine-protected within the Secure Enclave-transforms this data into a mathematical representation and compares that representation to the enrolled facial data. This enrolled facial data is itself a mathematical representation of the user's face captured across a variety of poses." (<i>Id.</i>).</p> <p>"Facial matching security Facial matching is performed within the Secure Enclave using neural networks trained specifically for that purpose... Face ID data, including mathematical representations of a user's face, is encrypted and available only to the Secure Enclave. This data never leaves the device." (<i>Id.</i> at 23.)</p> <p>When the Secure Enclave, or more precisely the Touch ID or Face ID subsystem within the Secure Enclave, has determined that a match exists, an accessibility attribute is issued by the corresponding Touch ID or Face ID subsystem. This Touch ID or Face ID subsystem is also referred to as the SBIO. The accessibility attribute confirms that there is a match and that the iPhone is to be unlocked ("... determine whether to unlock the device ...").</p> <p>This confirmation of the match is signaled by the SBIO by issuing a random secret to which only the Touch ID or Face ID subsystem within the Secure Enclave has access:</p>

<u>Claim 16</u>	<u>Accused Instrumentalities</u>
	<p>"During matching, the Secure Enclave compares incoming data from the biometric sensor against the stored templates to determine whether to unlock the device [...]." (<i>Id.</i> at 19.)</p> <p>"Uses for Touch ID and Face ID</p> <p><b>Unlocking a device or user account</b></p> <p>[...] <b>keys for the highest class of Data Protection-which are held in the Secure Enclave [...].</b></p> <p>With Touch ID or Face ID enabled, the keys aren't discarded when the device or account locks; instead, <b>they're wrapped with a key that's given to the Touch ID or Face ID subsystem inside the Secure Enclave.</b> When a user attempts to unlock the device or account, <b>if the device detects a successful match, it provides the key for unwrapping the Data Protection keys,</b> and the device or account is unlocked. This process provides additional protection by requiring cooperation between the Data Protection and Touch ID or Face ID subsystems to unlock the device." (<i>Id.</i> at 24.)</p> <p>"The class key is protected with the hardware UID and, for some classes, the user's passcode." (<i>Id.</i> at 85.)</p> <p><b>"Complete Protection</b></p> <p>(<i>NSFileProtectionComplete</i>): The class key is protected with a key derived from the user passcode or password and the device UID. Shortly after the user locks a device (10 seconds, if the Require Password setting is Immediately), the decrypted class key is discarded, <b>rendering all data in this class inaccessible until the user enters the passcode again or unlocks (logs in to) the device using Touch ID or Face ID.</b>" (<i>Id.</i> at 86.)</p> <p>The Touch ID or Face ID subsystem within the Secure Enclave is the SBIO shown below. SBIO is an application that runs within the Secure Enclave on the SEP and is responsible for checking the match</p>




<u>Claim 16</u>	<u>Accused Instrumentalities</u>
	<p>of biometric features. SBIO receives the corresponding biometric data from a biometric sensor, such as the Touch ID sensor. The random secret is stored in a memory ("bio memory") associated with the SBIO and is output from the bio memory upon match, see step 3 in the diagram below ("3) upon successful match send random secret to SKS");</p> <p>(Ex. B, Behind the Scenes with iOS Security, at 34.)</p> <p>The class keys are encrypted with a master key:</p>

<u>Claim 16</u>	<u>Accused Instrumentalities</u>
	<p><b>User Keybags</b> Background</p> <p>Sets of keys generated for each user to protect their data at rest Keys wrapped by master key derived from user passcode and SEP UID After 10 incorrect passcode entries, SEP will not process any further attempts Different policy associated with each keybag key—Usage, availability</p> <p><i>(Id., at 25.)</i></p> <p>The random secret is issued to SKS. SKS is a Secure Key Service application which is located within the Secure Enclave on the SEP and is responsible for decrypting class keys. The random secret provided by SBIO is used to decrypt a master key ("4) decrypt master key"). The master key is concatenated with the UID of the SEP and thus class keys are decrypted and added to the SKS keyring ("5) decrypt class keys, add to keyring") for further use by the Secure Enclave. The decrypted class keys include, for example, the class key of class A.</p>
<p>16c. a transmitter capable of emitting a secure access signal conveying said information dependent upon said accessibility attribute;</p>	<p><i>The Accused Instrumentalities include a transmitter configured to emit a secure access signal conveying information dependent upon said accessibility attribute.</i></p> <p>For example, the Secure Enclave emits a signal with ephemerally re-encrypted file keys:</p> <p>"sepOS can then use the ephemeral wrapping key to wrap file keys for use by the Application Processor file-system driver. When the file-system driver reads or writes a file, it sends the wrapped key to the AES Engine."</p>

<u>Claim 16</u>	<u>Accused Instrumentalities</u>
	<p>(Ex. A, Apple Platform Security, at 14.)</p> <p>"All wrapped file key handling occurs in the Secure Enclave; the file key is never directly exposed to the Application Processor. [...] When the Secure Enclave unwraps a file's keys, they're rewrapped with the ephemeral key and sent back to the Application Processor."  <i>(Id.</i> at 85.)</p> <p>The signal with the ephemerally re-encrypted file keys is a secure signal because it comes from the Secure Enclave and thus from a secure environment. Furthermore, the signal is secure because the transmitted information is encrypted. The emitted file keys are encrypted with the ephemeral key:</p> <p>"All wrapped file key handling occurs in the Secure Enclave; the file key is never directly exposed to the Application Processor. At startup, the Secure Enclave negotiates an ephemeral key with the AES Engine. When the Secure Enclave unwraps a file's keys, they're rewrapped with the ephemeral key and sent back to the Application Processor."  <i>(Id.)</i></p> <div data-bbox="612 873 1896 1369" style="background-color: black; color: white; padding: 10px;"> <h2 style="margin: 0;">Filesystem Data Protection</h2> <h3 style="margin: 0;">Overview</h3> <p style="margin: 0;">File blocks are encrypted using AES-XTS with 128-bit keys</p> <p style="margin: 0;">Each file on the user partition is encrypted using a unique random key chosen by SEP</p> <p style="margin: 0;">Raw file keys are never exposed to the AP</p> <ul style="list-style-type: none"> <li style="margin: 0;">• Wrapped with a key from the user keybag for long-term storage</li> <li style="margin: 0;">• Wrapped with an ephemeral key while in use, bound to boot session</li> </ul> </div>

<u>Claim 16</u>	<u>Accused Instrumentalities</u>
	<p>(Ex. B, Behind the Scenes with iOS Security, at 29.)</p> <div data-bbox="612 345 1783 1000" style="background-color: black; color: white; padding: 10px;"> <h3 style="text-align: center;">Filesystem Data Protection</h3> <p>The diagram illustrates the process of filesystem data protection across four layers: User, Kernel, SEP (Secure Enclave), and Hardware.          <ul style="list-style-type: none"> <li><b>User:</b> Executes the command <code>open("foo.txt", ...)</code>.</li> <li><b>Kernel:</b> <ol style="list-style-type: none"> <li>Fetches wrapped file_key from metadata (HFS).</li> <li>Sends an ID command with an ephemerally wrapped file_key (NVME Driver).</li> </ol> </li> <li><b>SEP:</b> <ol style="list-style-type: none"> <li>Unwraps the file_key using a keybag key (Key Store).</li> <li>Wraps the file_key using an ephemerally established key, returning the ephemerally wrapped file_key to the kernel (AES Engine).</li> </ol> </li> <li><b>Hardware:</b> <ul style="list-style-type: none"> <li>NAND storage contains the data.</li> <li>Storage Controller receives the ephemerally wrapped file_key and sends cipher text back to the NAND.</li> <li>An Ephemeral Key is established on boot within the SEP.</li> </ul> </li> </ul> </p> </div> <p>(<i>Id.</i>, at 30.)</p> <p>The information transmitted by the emitted signal, i.e., the ephemerally re-encrypted file keys, is dependent on the availability attribute, i.e., the confirmation that a biometric "template match" exists. This confirmation is signaled by the issuance of the random secret (cf. step 3): Only if there is a confirmation of the match and the random secret is issued by the Touch ID or Face ID subsystem within the Secure Enclave, i.e. SBIO, the class key is available for re-encrypting the file keys.</p> <p>The re-encrypted file keys are therefore information which is emitted depending on the fact that the availability attribute has been emitted.</p>

<u>Claim 16</u>	<u>Accused Instrumentalities</u>
<p>16d. wherein the controller is further capable of:</p>	<p><i>The Accused Instrumentalities include a controller that has capabilities as set forth in elements 16d1, 16d2, and 16d3 below.</i></p>
<p>16d1. receiving a series of entries of the biometric signal, said series being characterised according to at least one of the number of said entries and a duration of each said entry;</p>	<p><i>The Accused Instrumentalities include a transmitter sub-system controller configured to receive a series of entries of the biometric signal, said series being characterized according to at least one of the number of said entries and a duration of each said entry.</i></p> <p>More specifically, the Secure Enclave of the iPhone with the Secure Enclave Processor forms the means for receiving a series of entries of the biometric signal.</p> <p>"Apple's biometric security architecture relies on a strict separation of responsibilities between the biometric sensor and the Secure Enclave, and a secure connection between the two. The sensor captures the biometric image and securely transmits it to the Secure Enclave." (Ex. A, Apple Platform Security, at 19.)</p> <p><b>Touch ID</b></p> <p>When a finger is placed on the biometric sensor, the finger is scanned and the corresponding biometric signal entry is received by the Secure Enclave.</p> <p>"When the fingerprint sensor detects the touch of a finger, it triggers the advanced imaging array to scan the finger and sends the scan to the Secure Enclave." (<i>Id.</i>)</p> <p>To enroll a fingerprint in the database, the iPhone's fingerprint sensor records an entry of a biometric signal when the user places his finger on the sensor. This is done multiple times, resulting in a series of entries of such biometric signals.</p> <p>Receiving a series of entries of the biometric signal by repeatedly placing a finger on the Touch ID sensor will use Touch ID on iPhone.</p>


<u>Claim 16</u>	<u>Accused Instrumentalities</u>
	<p><b>Set up Touch ID</b></p> <p>Before you can set up Touch ID, you must first create a <a href="#">code</a> for your device,* then follow these steps:</p> <ol style="list-style-type: none"> <li>25. Make sure the Touch ID sensor and your finger are clean and dry.</li> <li>26. Tap Settings &gt; Touch ID &amp; Code, and then enter your code.</li> <li>27. Tap "Add fingerprint" and hold the device as you normally would when touching the Touch ID sensor.</li> <li>28. Touch the Touch ID sensor with one finger, but do not press. Keep your finger on the button until you feel a quick vibration or are prompted to lift your finger.</li> </ol>  <ol style="list-style-type: none"> <li>29. Continue by raising and slowly lowering your finger over and over again, changing the position of your finger just a tiny bit at a time.</li> </ol>

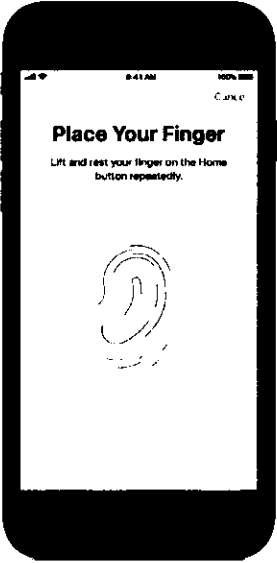
<u>Claim 16</u>	<u>Accused Instrumentalities</u>
	<p>30. The next screen will ask you to change your finger position. Hold your device as you normally would when unlocking it. Touch the Touch ID sensor with the outer edges of your fingertip instead of the middle part as you would during the first scan.”</p> <p>(<a href="https://support.apple.com/en-us/HT201371">https://support.apple.com/en-us/HT201371</a>)</p> <p>Accordingly, the user is prompted to place his finger on the sensor several times, in particular in accordance with step 5. Each time the finger is placed on the sensor, a corresponding biometric entry is generated, i.e. a series of such entries. All these entries, which result from placing the same finger on the sensor, form a series.</p> <p><b>Face ID</b></p> <p>The means for receiving a series of entries of the biometric signal includes a Secure Neural Engine, which is protected by the Secure Enclave. The Secure Neural Engine transforms the series of entries of the biometric signal received by the Secure Enclave into a biometric signature ("mathematical representation").</p> <p>"After the TrueDepth camera confirms the presence of an attentive face, it projects and reads over 30,000 infrared dots to form a depth map of the face along with a 2D infrared image. This data is used to create a <b>sequence of 2D images and depth maps</b>, which are digitally signed and <b>sent to the Secure Enclave</b>. To counter both digital and physical spoofs, the TrueDepth camera randomizes the sequence of 2D images and depth map captures, and projects a device-specific random pattern. A portion of the <b>Secure Neural Engine-protected</b> within the Secure Enclave-transforms this data into a mathematical representation and compares that representation to the enrolled facial data. This enrolled facial data is itself a mathematical representation of the user's face captured across a variety of poses." (Ex. A, Apple Platform Security, at 20.)</p> <p>Each entry of the biometric signal thus contains a two-dimensional infrared image with 30,000 infrared points for capturing depth information. By continuously capturing such infrared images into a Face ID scan while the user moves his head into different poses, a series of entries of the biometric signal</p>

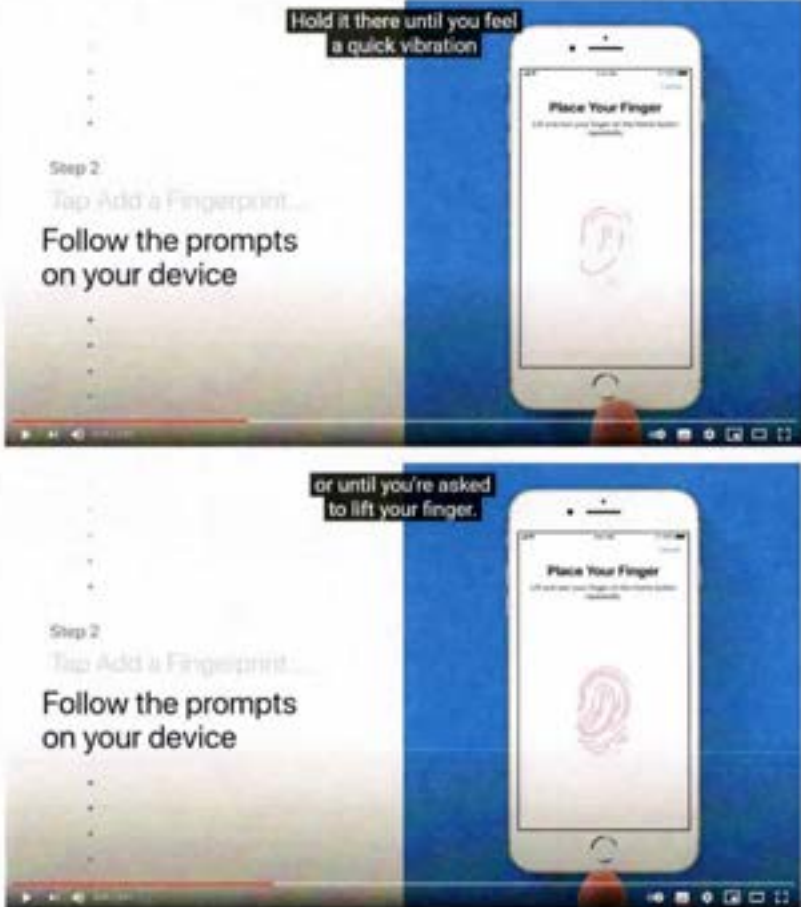
<u>Claim 16</u>	<u>Accused Instrumentalities</u>
	<p>results. Two such Face ID scans are required to generate a biometric signature of a single face, so that two series of entries of the biometric signal are received accordingly.</p> <p>Using Face ID on iPhone</p> <ol style="list-style-type: none"> <li>1. Tap Settings &gt; Face ID &amp; Code. Enter your code when prompted.</li> <li>2. Tap on "Configure Face ID".</li> <li>3. Hold the device in portrait mode in front of your face and tap "Let's go".</li> <li>4. Make sure your face is inside the frame and slowly move your head until the circle shown is completed. If you can't move your head, tap on "Options for operating aids".</li> <li>5. After performing the first Face ID scan, tap "Next".</li> <li>6. Again, slowly describe a circle with your head until it is completed.</li> <li>7. Tap "Done."</li> </ol> <p>(<a href="https://support.apple.com/en-us/HT208109">https://support.apple.com/en-us/HT208109</a>)</p> <p>The biometric signature of a single face is thus determined by two successive Face ID scans, each of which receives a series of entries of the biometric signal (compare steps 4. and 6. above).</p> <p>To register a second face, the iPhone offers a corresponding option in its settings. If the user selects the option "Set up an alternative appearance" as shown in the figure below on <a href="https://www.macworld.co.uk/how-to/second-face-id-3803421/">https://www.macworld.co.uk/how-to/second-face-id-3803421/</a>, a second face is registered by the iPhone in the same way as the first face.</p>




<u>Claim 16</u>	<u>Accused Instrumentalities</u>
	 <p>The series of entries of the biometric signal is identified on the iPhone by both the number and duration of each such entry.</p> <p><b>Touch ID</b></p> <p>According to step 5 of the instructions <a href="https://support.apple.com/en-us/HT201371">https://support.apple.com/en-us/HT201371</a>, for the enrollment of a single finger, the user has to repeatedly place the respective finger on the sensor and thus a number of entries in a row predetermined via the user guidance are captured by the iPhone. Each one of the entries must also be of a predetermined duration given to the user via the iPhone display, i.e. the user's finger must remain on the sensor for a predetermined duration for each entry of the biometric signal in order to capture the biometric signal during this time.</p>

<u>Claim 16</u>	<u>Accused Instrumentalities</u>
	<p>Receiving a series of entries of the biometric signal by repeatedly placing a finger on the Touch ID sensor will use Touch ID on iPhone and iPad.</p> <p><b>Set up Touch ID</b></p> <p>...</p> <p>4. Touch the Touch ID sensor with one finger, but do not press. Keep your finger on the button until you feel a quick vibration or are prompted to lift your finger.</p>  <p>5. Continue by raising and slowly lowering your finger over and over again, changing the position of your finger just a tiny bit at a time.</p> <p>6. The next screen will ask you to change your finger position. Hold your device as you normally would when unlocking it. Touch the Touch ID sensor with the outer edges of your fingertip instead of the middle part as you did during the first scan.</p> <p>(<a href="https://support.apple.com/en-us/HT201371">https://support.apple.com/en-us/HT201371</a>)</p>

<u>Claim 16</u>	<u>Accused Instrumentalities</u>
	<p>After placing a finger on the home button, a fingerprint appears on the display with red progress bars spreading along some of the papillary bars until the capture of the biometric entry in question is complete:</p>  <p>When the required duration is reached, the iPhone vibrates after an entry of the biometric signal is received or it issues a prompt to the user to lift the finger. The user then lifts the finger in question and replaces the same finger so that the iPhone receives a series of biometric signal entries of sufficient duration for that finger. The process is repeated for the same finger for as long as required according to the iPhone's user guidance.</p> <p>This is shown in the Apple YouTube video (32) How to set up Touch ID on your iPhone or iPad - Apple Support - YouTube (<a href="https://www.youtube.com/watch?v=xTZ2LALWZlg">https://www.youtube.com/watch?v=xTZ2LALWZlg</a>):</p>

<u>Claim 16</u>	<u>Accused Instrumentalities</u>
	 <p>Both the number of entries, i.e. the number of repetitions for placing the finger on the screen, and their respective duration are specified by the iPhone via the user guidance.</p>



<u>Claim 16</u>	<u>Accused Instrumentalities</u>
	<p><b>Face ID</b></p> <p>The user moves his face in front of the camera to strike different poses, and the camera system with image sensor continuously captures a large number of biometric entries, i.e. here the 2D images with depth information, in a row.</p> <p>"This enrolled facial data is itself a mathematical representation of the user's face captured across a variety of poses." (Ex. A, Apple Platform Security, at 20.)</p> <p>The sufficient duration of an entry for a pose, i.e. an angular position of the head specified via the user interface of the iPhone, is indicated to the user by the transformation of a gray line into a green line:</p>  <p>(Individual images taken from: <a href="https://support.apple.com/en-us/HT208109">https://support.apple.com/en-us/HT208109</a>)</p>
<p>16d2. mapping said series into an instruction; and</p>	<p><i>The Accused Instrumentalities include a transmitter sub-system controller configured to map said series into an instruction.</i></p>

<u>Claim 16</u>	<u>Accused Instrumentalities</u>
	<p>More specifically, the Secure Enclave of the iPhone contains means to assign the received row to an instruction: The Secure Enclave, after receiving the full set of entries of the biometric signal, assigns this set to an instruction for processing, encrypting and storing the biometric signature ("Touch ID and Face ID template data").</p> <p>"The sensor captures the biometric image and securely transmits it to the Secure Enclave. During enrollment, the Secure Enclave processes, encrypts, and stores the corresponding Touch ID and Face ID template data." (Ex. A, Apple Platform Security, at 19.)</p> <p>To carry out this instruction, the Secure Enclave has its own processor: "The Secure Enclave Processor provides the main computing power for the Secure Enclave." (<i>Id.</i>, at 10.)</p> <p><b>Touch ID</b></p> <p>The instruction here involves the processing of under-the-skin fingerprint characteristics and their encrypted storage.</p> <p>"The analysis uses subdermal ridge flow angle mapping, a lossy process that discards "finger minutiae data" that would be required to reconstruct the user's actual fingerprint. During enrollment, the resulting map of nodes is stored in an encrypted format that can be read only by the Secure Enclave as a template to compare against for future matches, but without any identity information." (<i>Id.</i>, at 19.)</p> <p><b>Face ID</b></p> <p>The instruction involves the transformation of the set of entries of the biometric signal captured via the Face ID scans into a mathematical representation, i.e. the biometric signature of the face in question by the Secure Neural Engine of the Secure Enclave, as well as its encryption and storage.</p>

<u>Claim 16</u>	<u>Accused Instrumentalities</u>
	<p>"A portion of the Secure Neural Engine-protected within the Secure Enclave-transforms this data into a mathematical representation and compares that representation to the enrolled facial data. This enrolled facial data is itself a mathematical representation of the user's face captured across a variety of poses." (<i>Id.</i>, at 20.)</p> <p>"Face ID data, including mathematical representations of a user's face, is encrypted and available only to the Secure Enclave. This data never leaves the device. It's not sent to Apple, nor is it included in device backups. The following Face ID data is saved, encrypted only for use by the Secure Enclave, during normal operation:</p> <ul style="list-style-type: none"> <li>• The mathematical representations of a user's face calculated during enrollment</li> <li>• ..."</li> </ul> <p>(<i>Id.</i>, at 23.)</p>
16d3. populating the database according to the instruction,	<p><b><i>The Accused Instrumentalities include a transmitter sub-system controller configured to populate the database according to the instruction.</i></b></p> <p>More specifically, the Secure Enclave stores the biometric signature, i.e. the encrypted mathematical representation of the fingerprint or face, in the database 105, i.e. the "secure nonvolatile storage":</p> <p>"The secure nonvolatile storage is used for all anti-replay services in the Secure Enclave. Anti-replay services on the Secure Enclave are used for revocation of data over events that mark anti-replay boundaries including, but not limited to, the following:</p> <ul style="list-style-type: none"> <li>• ...</li> <li>• ...</li> <li>• Adding or removing a Touch ID fingerprint or Face ID face".</li> </ul> <p>(Ex. A, Apple Platform Security, at 16.)</p> <p>"During enrollment, the Secure Enclave processes, encrypts, and stores the corresponding Touch ID and Face ID template data." (<i>Id.</i>, at 19.)</p>


<u>Claim 16</u>	<u>Accused Instrumentalities</u>
	<p><b>Touch ID</b></p> <p>"During enrollment, the resulting map of nodes is stored in an encrypted format that can be read only by the Secure Enclave as a template to compare against for future matches...." (<i>Id.</i>)</p> <p><b>Face ID</b></p> <p>The following Face ID data is saved, encrypted only for use by the Secure Enclave, during normal operation:</p> <ul style="list-style-type: none"> <li>• The mathematical representations of a user's face calculated during enrollment". (<i>Id.</i>, at 23.)</li> </ul>
<p>wherein the controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing device.</p>	<p><i>The Accused Instrumentalities include a controller capable of: populating the database according to the instruction, wherein the controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing device.</i></p> <p>More specifically, the controlled item is a locking mechanism of the door lock of the user's home. The Accused Instrumentalities are configured to provide secure access to the user's home via Yale Smart Locks when the user provides biometric signal to the Accused Instrumentalities via Touch ID or Face ID.</p> <p>"When the "Secure Remote Access" feature is turned on, the app will use your phone's built-in authentication tools to prompt fingerprint or facial recognition before you can unlock or lock your home remotely (note: if your phone does not have these features, it will prompt you to use your PIN code). This further ensures that your door is only operated by the right people at the time you intend for it." <a href="https://us.yalehome.com/en/yale-news/blog/latest-blog-posts/introducing-biometric-verification-for-august-and-yale-locks1/">https://us.yalehome.com/en/yale-news/blog/latest-blog-posts/introducing-biometric-verification-for-august-and-yale-locks1/</a></p>




<u>Claim 16</u>	<u>Accused Instrumentalities</u>
	 <p data-bbox="634 310 736 342">☰ Open <span style="margin-left: 150px;"><b>Yale</b></span> <span style="float: right;">🔍</span></p> <h2 data-bbox="634 410 1725 451">Introducing Biometric Verification for August and Yale Locks</h2>  <p data-bbox="634 1130 1853 1195"><a href="https://us.yalehome.com/en/yale-news/blog/latest-blog-posts/introducing-biometric-verification-for-august-and-yale-locks/">https://us.yalehome.com/en/yale-news/blog/latest-blog-posts/introducing-biometric-verification-for-august-and-yale-locks/</a></p>

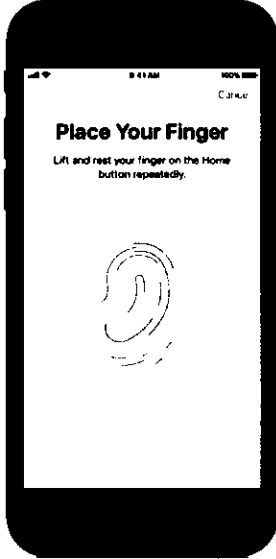
<u>Claim 16</u>	<u>Accused Instrumentalities</u>
	 <p data-bbox="612 1073 1853 1105"><a href="https://www.apple.com/shop/product/HPAR2ZM/A/yale-assure-lock-sl-touchscreen-deadbolt-black">https://www.apple.com/shop/product/HPAR2ZM/A/yale-assure-lock-sl-touchscreen-deadbolt-black</a></p>

<u>Claim 17</u>	<u>Accused Instrumentalities</u>
<p>17. A method for providing secure access to a controlled item in a system comprising a database of biometric signatures, a transmitter sub-system comprising a biometric sensor capable of receiving a biometric signal, and a transmitter capable of emitting a secure access signal capable of granting access to the controlled item, and a receiver sub-system comprising a receiver sub-system controller capable of receiving the transmitted secure access signal, and providing conditional access to the controlled item dependent upon information in said secure access signal, the method comprising:</p>	<p><i>To the extent that the preamble is deemed to be a limitation, the Accused Instrumentalities are configured to use a method in accordance with this claim.</i></p> <p>More specifically, the controlled item is a locking mechanism of the door lock of the user's home. The Accused Instrumentalities are configured to provide secure access to the user's home via Yale Smart Locks when the user provides biometric signal to the Accused Instrumentalities via Touch ID or Face ID.</p> <p>“When the “Secure Remote Access” feature is turned on, the app will use your phone’s built-in authentication tools to prompt fingerprint or facial recognition before you can unlock or lock your home remotely (note: if your phone does not have these features, it will prompt you to use your PIN code). This further ensures that your door is only operated by the right people at the time you intend for it.”                  (https://us.yalehome.com/en/yale-news/blog/latest-blog-posts/introducing-biometric-verification-for-august-and-yale-locks1/)</p>

<u>Claim 17</u>	<u>Accused Instrumentalities</u>
	 <p>The screenshot shows a mobile application interface for Yale. At the top, there is a yellow circular logo with the word "Yale" in black. To the left of the logo is a hamburger menu icon and the word "Open". To the right is a magnifying glass search icon. Below the header, the text "Introducing Biometric Verification for August and Yale Locks" is displayed in a bold, black font. Underneath the text is a photograph of a hand holding a smartphone. The phone's screen displays a biometric verification interface with a red circular camera overlay and a black square in the center containing a white "123" pattern. Below the photograph, the URL <a href="https://us.yalehome.com/en/yale-news/blog/latest-blog-posts/introducing-biometric-verification-for-august-and-yale-locks1/">(https://us.yalehome.com/en/yale-news/blog/latest-blog-posts/introducing-biometric-verification-for-august-and-yale-locks1/)</a> is provided.</p>

<u>Claim 17</u>	<u>Accused Instrumentalities</u>
	 <p data-bbox="608 1076 1874 1109">(https://www.apple.com/shop/product/HPAR2ZM/A/yale-assure-lock-sl-touchscreen-deadbolt-black)</p>
<p>17a. populating the database of biometric signatures by:</p>	<p><i>The Accused Instrumentalities are configured to populate the database of biometric signatures as set forth in elements 17a1 to 17a4 below.</i></p>

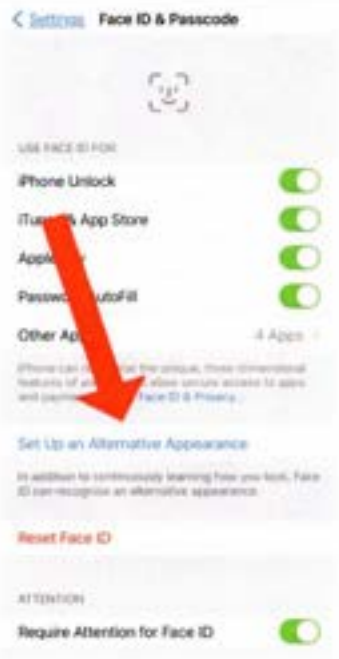
<u>Claim 17</u>	<u>Accused Instrumentalities</u>
17a1. receiving a series of entries of the biometric signal;	<p><b><i>The Accused Instrumentalities are configured to populate the database of biometric signatures by: receiving a series of entries of the biometric signal.</i></b></p> <p>More specifically, the Secure Enclave of the iPhone with the Secure Enclave Processor forms the means for receiving a series of entries of the biometric signal.</p> <p>"Apple's biometric security architecture relies on a strict separation of responsibilities between the biometric sensor and the Secure Enclave, and a secure connection between the two. The sensor captures the biometric image and securely transmits it to the Secure Enclave." (Ex. A, Apple Platform Security, at 19.)</p> <p><b>Touch ID</b></p> <p>When a finger is placed on the biometric sensor, the finger is scanned and the corresponding biometric signal entry is received by the Secure Enclave.</p> <p>"When the fingerprint sensor detects the touch of a finger, it triggers the advanced imaging array to scan the finger and sends the scan to the Secure Enclave." (Ex. A, Apple Platform Security, at 19.)</p> <p>To enroll a fingerprint in the database, the iPhone's fingerprint sensor records an entry of a biometric signal when the user places his finger on the sensor. This is done multiple times, resulting in a series of entries of such biometric signals.</p> <p>Receiving a series of entries of the biometric signal by repeatedly placing a finger on the Touch ID sensor will use Touch ID on iPhone and iPad here - Apple Support ; <a href="https://support.apple.com/en-us/HT201371">https://support.apple.com/en-us/HT201371</a> literally described as follows:</p> <p><b>Set up Touch ID</b></p>

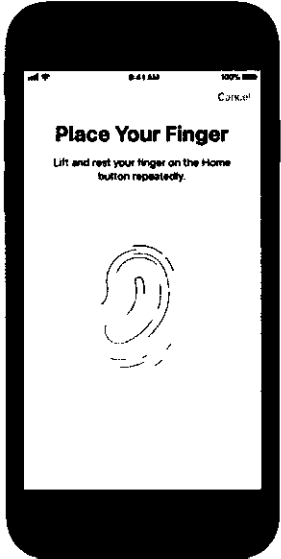
<u>Claim 17</u>	<u>Accused Instrumentalities</u>
	<p>Before you can set up Touch ID, you must first create a code for your device,* then follow these steps:</p> <ol style="list-style-type: none"> <li>1. Make sure the Touch ID sensor and your finger are clean and dry.</li> <li>2. Tap Settings &gt; Touch ID &amp; Code, and then enter your code.</li> <li>3. Tap "Add fingerprint" and hold the device as you normally would when touching the Touch ID sensor.</li> <li>4. Touch the Touch ID sensor with one finger, but do not press. Keep your finger on the button until you feel a quick vibration or are prompted to lift your finger.</li> </ol>  <ol style="list-style-type: none"> <li>5. Continue by raising and slowly lowering your finger over and over again, changing the position of your finger just a tiny bit at a time.</li> <li>6. The next screen will ask you to change your finger position. Hold your device as you normally would when unlocking it. Touch the Touch ID sensor with the outer edges of your fingertip instead of the middle part as you would during the first scan.”</li> </ol>

<u>Claim 17</u>	<u>Accused Instrumentalities</u>
	<p>Accordingly, the user is prompted to place his finger on the sensor several times, in particular in accordance with step 5. Each time the finger is placed on the sensor, a corresponding biometric entry is generated, i.e. a series of such entries. All these entries, which result from placing the same finger on the sensor, form a series.</p> <p><b>Face ID</b></p> <p>The means for receiving a series of entries of the biometric signal includes a Secure Neural Engine, which is protected by the Secure Enclave. The Secure Neural Engine transforms the series of entries of the biometric signal received by the Secure Enclave into a biometric signature ("mathematical representation").</p> <p>"After the TrueDepth camera confirms the presence of an attentive face, it projects and reads over 30,000 infrared dots to form a depth map of the face along with a 2D infrared image. This data is used to create a <b>sequence of 2D images and depth maps</b>, which are digitally signed and <b>sent to the Secure Enclave</b>. To counter both digital and physical spoofs, the TrueDepth camera randomizes the sequence of 2D images and depth map captures, and projects a device-specific random pattern. A portion of the <b>Secure Neural Engine-protected</b> within the Secure Enclave-transforms this data into a mathematical representation and compares that representation to the enrolled facial data. This enrolled facial data is itself a mathematical representation of the user's face captured across a variety of poses." (Ex. A, Apple Platform Security, at 20.)</p> <p>Each entry of the biometric signal thus contains a two-dimensional infrared image with 30,000 infrared points for capturing depth information. By continuously capturing such infrared images into a Face ID scan while the user moves his head into different poses, a series of entries of the biometric signal results. Two such Face ID scans are required to generate a biometric signature of a single face, so that two series of entries of the biometric signal are received accordingly.</p> <p>Under Using Face ID on iPhone or iPad Pro - Apple Support; <a href="https://support.apple.com/en-us/HT208109">https://support.apple.com/en-us/HT208109</a>, the creation of a set of entries is described as follows:</p>

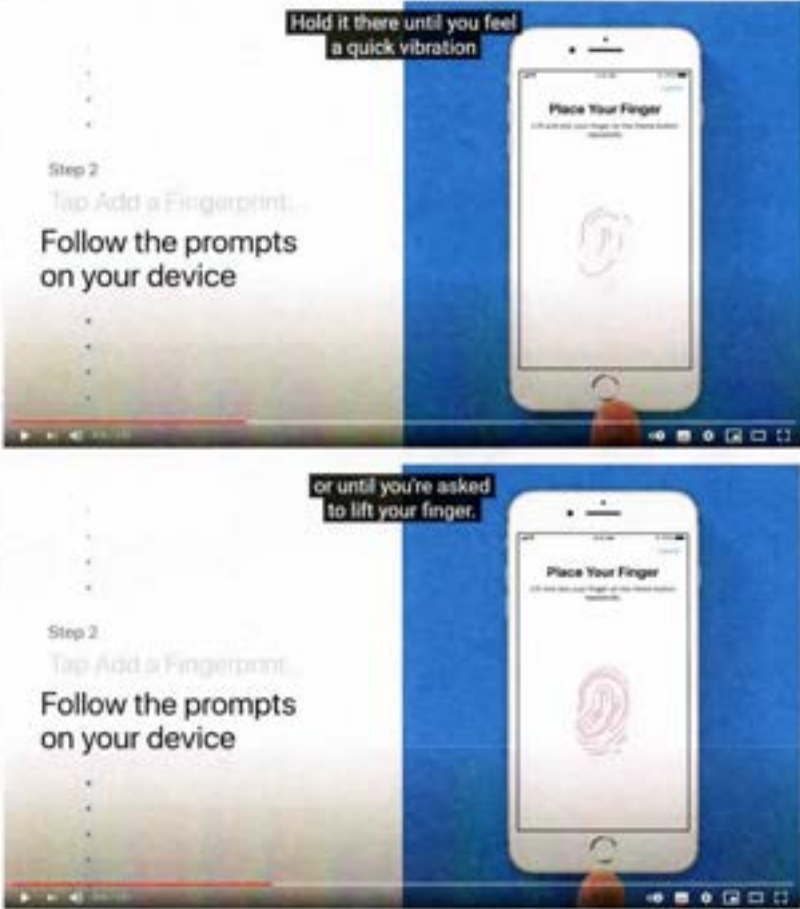



<u>Claim 17</u>	<u>Accused Instrumentalities</u>
	<p>Configure Face ID</p> <p>Before configuring Face ID, make sure that neither the TrueDepth camera nor your face are covered by anything....</p> <p>Follow the steps below to configure Face ID:</p> <ol style="list-style-type: none"> <li>1. Tap Settings &gt; Face ID &amp; Code. Enter your code when prompted.</li> <li>2. Tap on "Configure Face ID".</li> <li>3. Hold the device in portrait mode in front of your face and tap "Let's go".</li> <li>4. Make sure your face is inside the frame and slowly move your head until the circle shown is completed. If you can't move your head, tap on "Options for operating aids".</li> <li>5. After performing the first Face ID scan, tap "Next".</li> <li>6. Again, slowly describe a circle with your head until it is completed.</li> <li>7. Tap "Done."</li> </ol> <p>The biometric signature of a single face is thus determined by two successive Face ID scans, each of which receives a series of entries of the biometric signal (compare steps 4. and 6. above).</p> <p>To register a second face, the iPhone offers a corresponding option in its settings. If the user selects the option "Set up an alternative appearance" as shown in the figure below on <a href="https://www.macworld.co.uk/how-to/second-face-id-3803421/">https://www.macworld.co.uk/how-to/second-face-id-3803421/</a>, a second face is registered by the iPhone in the same way as the first face.</p>

<u>Claim 17</u>	<u>Accused Instrumentalities</u>
	 <p>The series of entries of the biometric signal is identified on the iPhone by both the number and duration of each such entry.</p> <p><b>Touch ID</b></p> <p>According to step 5 of the instructions <a href="https://support.apple.com/en-us/HT201371">https://support.apple.com/en-us/HT201371</a>, for the enrollment of a single finger, the user has to repeatedly place the respective finger on the sensor and thus a number of entries in a row predetermined via the user guidance are captured by the iPhone. Each one of the entries must also be of a predetermined duration given to the user via the iPhone display, i.e. the user's finger must remain on the sensor for a predetermined duration for each entry of the biometric signal in order to capture the biometric signal during this time.</p>

<u>Claim 17</u>	<u>Accused Instrumentalities</u>
	<p>Receiving a series of entries of the biometric signal by repeatedly placing a finger on the Touch ID sensor will use Touch ID on iPhone and iPad here - Apple Support (<a href="https://support.apple.com/en-us/HT201371">https://support.apple.com/en-us/HT201371</a>) literally described as follows:</p> <p><b>Set up Touch ID</b></p> <p>...</p> <p>4. Touch the Touch ID sensor with one finger, but do not press. Keep your finger on the button until you feel a quick vibration or are prompted to lift your finger.</p>  <p>5. Continue by raising and slowly lowering your finger over and over again, changing the position of your finger just a tiny bit at a time.</p> <p>6. The next screen will ask you to change your finger position. Hold your device as you normally would when unlocking it. Touch the Touch ID sensor with the outer edges of your fingertip instead of the middle part as you did during the first scan.</p>

<u>Claim 17</u>	<u>Accused Instrumentalities</u>
	<p>After placing a finger on the home button, a fingerprint appears on the display with red progress bars spreading along some of the papillary bars until the capture of the biometric entry in question is complete:</p> <div data-bbox="1115 431 1391 992" data-label="Image"> </div> <p>When the required duration is reached, the iPhone vibrates after an entry of the biometric signal is received or it issues a prompt to the user to lift the finger. The user then lifts the finger in question and replaces the same finger so that the iPhone receives a series of biometric signal entries of sufficient duration for that finger. The process is repeated for the same finger for as long as required according to the iPhone's user guidance.</p> <p>This is shown in the Apple YouTube video (32) How to set up Touch ID on your iPhone or iPad - Apple Support - YouTube (<a href="https://www.youtube.com/watch?v=xTZ2LALWZlg">https://www.youtube.com/watch?v=xTZ2LALWZlg</a>):</p>

<u>Claim 17</u>	<u>Accused Instrumentalities</u>
	 <p>Both the number of entries, i.e. the number of repetitions for placing the finger on the screen, and their respective duration are specified by the iPhone via the user guidance.</p>

<u>Claim 17</u>	<u>Accused Instrumentalities</u>
	<p><b>Face ID</b></p> <p>The user moves his face in front of the camera to strike different poses, and the camera system with image sensor continuously captures a large number of biometric entries, i.e. here the 2D images with depth information, in a row.</p> <p>"This enrolled facial data is itself a mathematical representation of the user's face captured across a variety of poses." (Ex. A, Apple Platform Security, at 20.)</p> <p>The sufficient duration of an entry for a pose, i.e. an angular position of the head specified via the user interface of the iPhone, is indicated to the user by the transformation of a gray line into a green line:</p>  <p>(Individual images taken from: <a href="https://support.apple.com/en-us/HT208109">https://support.apple.com/en-us/HT208109</a>)</p>

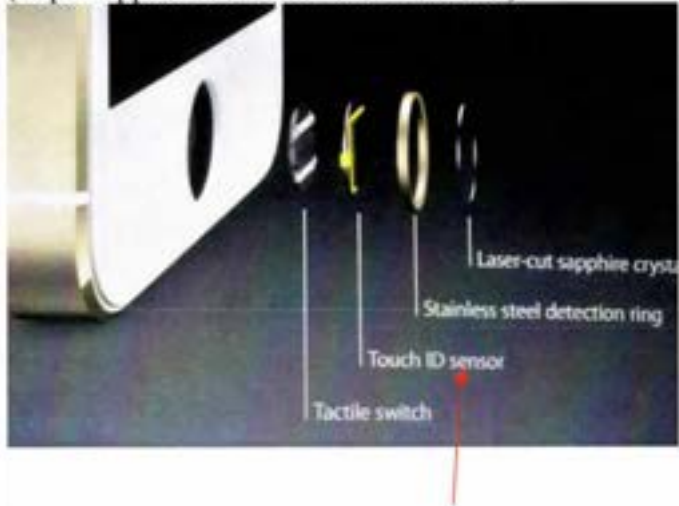
<u>Claim 17</u>	<u>Accused Instrumentalities</u>
17a2. determining at least one of the number of said entries and a duration of each said entry;	<p><b><i>The Accused instrumentalities are configured to populate the database of biometric signatures by: determining at least one of the number of said entries and a duration of each said entry.</i></b></p> <p>More specifically, as discussed above, both Face ID and Touch ID require a specific number of entries to enroll a Touch ID or Face ID. The Accused Instrumentalities must determine that the specific number of entries have been input. Likewise, while not necessary for the claim, upon information and belief, the Accused Instrumentalities determine that each input of either facial or fingerprint data is of a sufficient duration. Again, when setting up Touch ID in the Accused Instrumentalities, the users are required to touch the home button with their finger several times for a certain duration. Similarly, the users need to scan their face twice, and each scan requires the users to move their head in a circle for a certain duration for Face ID.</p> <p>Touch ID: Register a fingerprint for Apple Touch ID by the user tapping a finger several times on the home button to record the fingerprint data. (<a href="https://video.search.yahoo.com/yhs/search?fr=yhs-pty-pty_converter&amp;hsimp=yhs-pty_converter&amp;hspart=pty&amp;p=registering+fingerprint+apple+touch+id+on+screen+instructions#id=1&amp;vid=156de65ae06ca453643009fc0ea9cf79&amp;action=click">https://video.search.yahoo.com/yhs/search?fr=yhs-pty-pty_converter&amp;hsimp=yhs-pty_converter&amp;hspart=pty&amp;p=registering+fingerprint+apple+touch+id+on+screen+instructions#id=1&amp;vid=156de65ae06ca453643009fc0ea9cf79&amp;action=click</a>)</p> <p>Touch ID: The user's finger must remain on the home button long enough for the data to be recorded. "Touch the Touch ID sensor with your finger, but don't press it. Hold it there until you feel a quick vibration, or until you're asked to lift your finger." "Continue to lift and rest your finger slowly, making small adjustments to the position of your finger each time." (<a href="https://support.apple.com/en-au/HT201371">https://support.apple.com/en-au/HT201371</a>)</p> <p>Touch ID: "you shouldn't tap too quickly or move your finger around" (<a href="https://support.apple.com/en-us/HT207537">https://support.apple.com/en-us/HT207537</a>)</p> <p>Face ID: Setting up Face ID requires two scans of the user's face. Each scan asks users to move their head slowly in a circle to register different angles of the user's face. (<a href="https://www.imore.com/how-set-face-id-iphone">https://www.imore.com/how-set-face-id-iphone</a>)</p>

<u>Claim 17</u>	<u>Accused Instrumentalities</u>
<p>17a3. mapping said series into an instruction; and</p>	<p><b><i>The Accused Instrumentalities include a transmitter sub-system controller configured to map said series into an instruction.</i></b></p> <p>More specifically, the Secure Enclave of the iPhone contains means to assign the received row to an instruction: The Secure Enclave, after receiving the full set of entries of the biometric signal, assigns this set to an instruction for processing, encrypting and storing the biometric signature ("Touch ID and Face ID template data").</p> <p>"The sensor captures the biometric image and securely transmits it to the Secure Enclave. During enrollment, the Secure Enclave processes, encrypts, and stores the corresponding Touch ID and Face ID template data." (Ex. A, Apple Platform Security, at 19.)</p> <p>To carry out this instruction, the Secure Enclave has its own processor: "The Secure Enclave Processor provides the main computing power for the Secure Enclave." (<i>Id.</i>, at 10.)</p> <p><b>Touch ID</b></p> <p>The instruction here involves the processing of under-the-skin fingerprint characteristics and their encrypted storage.</p> <p>"The analysis uses subdermal ridge flow angle mapping, a lossy process that discards "finger minutiae data" that would be required to reconstruct the user's actual fingerprint. During enrollment, the resulting map of nodes is stored in an encrypted format that can be read only by the Secure Enclave as a template to compare against for future matches, but without any identity information." (<i>Id.</i>, at 19.)</p> <p><b>Face ID</b></p>




<u>Claim 17</u>	<u>Accused Instrumentalities</u>
	<p>The instruction involves the transformation of the set of entries of the biometric signal captured via the Face ID scans into a mathematical representation, i.e. the biometric signature of the face in question by the Secure Neural Engine of the Secure Enclave, as well as its encryption and storage.</p> <p>"A portion of the Secure Neural Engine-protected within the Secure Enclave-transforms this data into a mathematical representation and compares that representation to the enrolled facial data. This enrolled facial data is itself a mathematical representation of the user's face captured across a variety of poses. " (<i>Id.</i>, at 20.)</p> <p>"Face ID data, including mathematical representations of a user's face, is encrypted and available only to the Secure Enclave. This data never leaves the device. It's not sent to Apple, nor is it included in device backups. The following Face ID data is saved, encrypted only for use by the Secure Enclave, during normal operation:</p> <ul style="list-style-type: none"> <li>• The mathematical representations of a user's face calculated during enrollment</li> <li>• ..."</li> </ul> <p>(<i>Id.</i>, at 23.)</p>
<p>17a4. populating the database according to the instruction;</p>	<p><b><i>The Accused Instrumentalities include a transmitter sub-system controller configured to populate the database according to the instruction.</i></b></p> <p>More specifically, the Secure Enclave stores the biometric signature, i.e. the encrypted mathematical representation of the fingerprint or face, in the database 105, i.e. the "secure nonvolatile storage":</p> <p>"The secure nonvolatile storage is used for all anti-replay services in the Secure Enclave. Anti-replay services on the Secure Enclave are used for revocation of data over events that mark anti-replay boundaries including, but not limited to, the following:</p> <ul style="list-style-type: none"> <li>• ...</li> <li>• ...</li> <li>• Adding or removing a Touch ID fingerprint or Face ID face".</li> </ul> <p>(Ex. A, Apple Platform Security, at 16.)</p>

<u>Claim 17</u>	<u>Accused Instrumentalities</u>
	<p>"During enrollment, the Secure Enclave processes, encrypts, and stores the corresponding Touch ID and Face ID template data." (<i>Id.</i>, at 19.)</p> <p><b>Touch ID</b></p> <p>"During enrollment, the resulting map of nodes is stored in an encrypted format that can be read only by the Secure Enclave as a template to compare against for future matches...." (<i>Id.</i>)</p> <p><b>Face ID</b></p> <p>The following Face ID data is saved, encrypted only for use by the Secure Enclave, during normal operation:</p> <ul style="list-style-type: none"> <li>• The mathematical representations of a user's face calculated during enrollment".</li> </ul> <p>(<i>Id.</i>, at 23.)</p>
<p>17b. receiving the biometric signal;</p>	<p><b><i>The Accused Instrumentalities are configured to receive the biometric signal.</i></b></p> <p>More specifically, the iPhone has at least one biometric sensor for capturing a fingerprint or a face (Touch ID and/or Face ID), namely a Touch ID sensor and a camera system with image sensor, respectively.</p> <p><b>Touch ID</b></p> <p>"Apple devices with a Touch ID sensor can be unlocked using a fingerprint." (Ex. A, Apple Platform Security, at 19.)</p> <p>"Touch ID is the fingerprint sensing system that makes secure access to supported Apple devices faster and easier. This technology reads fingerprint data from any angle and learns more about a user's fingerprint over time, with the <b>sensor</b> continuing to expand the fingerprint map as additional overlapping nodes are identified with each use."</p>

<u>Claim 17</u>	<u>Accused Instrumentalities</u>
	<p>(<i>Id.</i>)</p> <p>"When the fingerprint sensor detects the touch of a finger, it triggers the advanced imaging array to scan the finger and sends the scan to the Secure Enclave."  (<i>Id.</i>)</p> <p>The biometric sensor for Touch ID is located below the home button:</p> <p>"The Home button is a stack of different materials, capped with a sapphire crystal lens. The surrounding stainless-steel ring works as a ground and detects the user's finger. This action activates a capacitive touch sensor installed underneath the cover: A CMOS chip with small capacitors."  (<a href="https://appleinsider.com/inside/touch-id">https://appleinsider.com/inside/touch-id</a>)</p>  <p style="text-align: center;">Biometric sensor 121</p> <p>"Where is the Touch ID sensor located?"</p>

<u>Claim 17</u>	<u>Accused Instrumentalities</u>
	<p>The Touch ID sensor is located either in the home button or - on the iPad Air (4th generation) - in the top button.</p> <p>(<a href="https://support.apple.com/en-us/HT201371">https://support.apple.com/en-us/HT201371</a>)</p> <p>The image sensor captures an 88-by-88-pixel, 500 PPI raster scan:</p> <p>"The 88-by-88-pixel, 500-ppi raster scan is temporarily stored in encrypted memory within the Secure Enclave while being vectorized for analysis, and then it's discarded. The analysis utilizes subdermal ridge flow angle mapping, which is a lossy process that discards minutia data that would be required to reconstruct the user's actual fingerprint. The resulting map of nodes is stored without any identity information in an encrypted format that can only be read by the Secure Enclave, and is never sent to Apple or backed up to iCloud or iTunes."</p> <p>(Ex. C, iOS Security white paper, at 8.)</p> <p><b>Face ID</b></p> <p>The biometric sensor for facial biometrics is a camera system ("TrueDepth camera system") with an image sensor.</p> <p>"With a simple glance, Face ID securely unlocks supported Apple devices. It provides intuitive and secure authentication enabled by the TrueDepth camera system, which uses advanced technologies to accurately map the geometry of a user's face."</p> <p>(Ex. A, Apple Platform Security, at 20.)</p> <p>To receive a biometric signal, the camera system with image sensor reads over 30,000 infrared points to capture depth information along with a two-dimensional infrared image.</p> <p>"After the TrueDepth camera confirms the presence of an attentive face, it projects and <b>reads over 30,000 infrared dots to form a depth map of the face along with a 2D infrared image.</b> This data is</p>

<u>Claim 17</u>	<u>Accused Instrumentalities</u>
	<p>used to <b>create a sequence of 2D images and depth maps</b>, which are digitally signed and sent to the Secure Enclave. To counter both digital and physical spoofs, the TrueDepth camera randomizes the sequence of 2D images and depth map captures, and projects a device-specific random pattern. A portion of the Secure Neural Engine-protected within the Secure Enclave-transforms this data into a mathematical representation and compares that representation to the enrolled facial data. This enrolled facial data is itself a mathematical representation of the user's face captured across a variety of poses." (<i>Id.</i>, at 20.)</p> <p>The camera system includes a biometric image sensor, namely a "CMOS image" sensor from Sony, to perform facial biometrics:</p>  <p>(<a href="https://appleinsider.com/articles/17/09/09/inner-workings-of-apples-face-id-camera-detailed-in-report">https://appleinsider.com/articles/17/09/09/inner-workings-of-apples-face-id-camera-detailed-in-report</a>)</p>

<u>Claim 17</u>	<u>Accused Instrumentalities</u>
<p>17c. matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute;</p>	<p><i>The Accused Instrumentalities include a transmitter controller configured to emit a secure access signal conveying information dependent upon said accessibility attribute.</i></p> <p>More specifically, the iPhone's System on Chip (SOC), i.e. the Secure Enclave with its Secure Enclave Processor (SEP) or a Secure Neural Engine contained therein, is a means (103) to check a match of the biometric signal with elements of the biometric signature database.</p> <p>"The <i>Secure Enclave</i> is a system on chip (SoC) that is included on all recent iPhone, ... devices" (Ex. A, Apple Platform Security, at 7.)</p> <p>"During <b>matching</b>, the Secure Enclave <b>compares</b> incoming data from the biometric sensor against the stored templates <b>to determine whether to unlock the device</b> or respond that a match is valid (for Apple Pay, in-app, and other uses of Touch ID and Face ID). " (<i>Id.</i>, at 19.)</p> <p>The biometric signal received from the biometric sensor ("incoming data from the biometric sensor") is thus checked by the Secure Enclave and its SEP with the elements of the database of biometric signatures 105, i.e. the "stored templates", for the presence of a match.</p> <p>For Touch ID, the Secure Enclave match verification is performed as follows:</p> <p>"The Secure Enclave is responsible for processing fingerprint data from the Touch ID sensor, determining if there is a match against registered fingerprints, and then enabling access or purchases on behalf of the user ..." (Ex. C, iOS Security white paper, at 7.)</p> <p>"During enrollment, the resulting map of nodes is stored in an encrypted format that can be read only by the Secure Enclave as a template to compare against for future matches...." (Ex. A, Apple Platform Security, at 19.)</p>

<u>Claim 17</u>	<u>Accused Instrumentalities</u>
	<p>"Touch ID can read multiple fingerprints, and it can read fingerprints in 360-degrees of orientation. It then creates a mathematical representation of your fingerprint and compares this to your enrolled fingerprint data to identify a match and unlock your device. " (<a href="https://support.apple.com/en-us/HT204587">https://support.apple.com/en-us/HT204587</a>)</p> <p>"Touch ID can read multiple fingerprints and recognize fingerprints at any orientation of the finger. The system then creates a mathematical representation of your fingerprint and compares it to the registered fingerprint data to determine a match and unlock your device." (<a href="https://support.apple.com/de-de/HT204587">https://support.apple.com/de-de/HT204587</a>)</p> <p>For <b>Face ID</b>, the Secure Enclave has a neural network protected by it, i.e., a Secure Neural Engine, which is used to verify the match:</p> <p>"Face ID uses neural networks for determining attention, <b>matching</b>, and antispoofing, so a user can unlock their phone with a glance." (Ex. A, Apple Platform Security, at 20.)</p> <p>"A portion of the Secure Neural Engine-protected within the Secure Enclave-transforms this data into a mathematical representation and compares that representation to the enrolled facial data. This enrolled facial data is itself a mathematical representation of the user's face captured across a variety of poses." (<i>Id.</i>).</p> <p>"Facial matching security Facial matching is performed within the Secure Enclave using neural networks trained specifically for that purpose... Face ID data, including mathematical representations of a user's face, is encrypted and available only to the Secure Enclave. This data never leaves the device." (<i>Id.</i> at 23.)</p> <p>When the Secure Enclave, or more precisely the Touch ID or Face ID subsystem within the Secure Enclave, has determined that a match exists, an accessibility attribute is issued by the corresponding</p>

<u>Claim 17</u>	<u>Accused Instrumentalities</u>
	<p>Touch ID or Face ID subsystem. This Touch ID or Face ID subsystem is also referred to as the SBIO. The accessibility attribute confirms that there is a match and that the iPhone is to be unlocked ("... determine whether to unlock the device ...").</p> <p>This confirmation of the match is signaled by the SBIO by issuing a random secret to which only the Touch ID or Face ID subsystem within the Secure Enclave has access:</p> <p>"During matching, the Secure Enclave compares incoming data from the biometric sensor against the stored templates to determine whether to unlock the device [...]." (<i>Id.</i> at 19.)</p> <p>"Uses for Touch ID and Face ID</p> <p><b>Unlocking a device or user account</b></p> <p>[...] <b>keys for the highest class of Data Protection-which are held in the Secure Enclave [...].</b></p> <p>With Touch ID or Face ID enabled, the keys aren't discarded when the device or account locks; instead, <b>they're wrapped with a key that's given to the Touch ID or Face ID subsystem inside the Secure Enclave.</b> When a user attempts to unlock the device or account, <b>if the device detects a successful match, it provides the key for unwrapping the Data Protection keys,</b> and the device or account is unlocked. This process provides additional protection by requiring cooperation between the Data Protection and Touch ID or Face ID subsystems to unlock the device." (<i>Id.</i> at 24.)</p> <p>"The class key is protected with the hardware UID and, for some classes, the user's passcode." (<i>Id.</i> at 85.)</p> <p><b>"Complete Protection</b></p> <p>(<i>NSFileProtectionComplete</i>): The class key is protected with a key derived from the user passcode or password and the device UID. Shortly after the user locks a device (10 seconds, if the Require</p>



Claim 17	Accused Instrumentalities
	<p>Password setting is Immediately), the decrypted class key is discarded, <b>rendering all data in this class inaccessible until the user enters the passcode again or unlocks (logs in to) the device using Touch ID or Face ID.</b>"</p> <p>(<i>Id.</i> at 86.)</p> <p>The Touch ID or Face ID subsystem within the Secure Enclave is the SBIO shown below. SBIO is an application that runs within the Secure Enclave on the SEP and is responsible for checking the match of biometric features. SBIO receives the corresponding biometric data from a biometric sensor, such as the Touch ID sensor. The random secret is stored in a memory ("bio memory") associated with the SBIO and is output from the bio memory upon match, see step 3 in the diagram below ("3) upon successful match send random secret to SKS"): </p> <p>(Ex. B, Behind the Scenes with iOS Security, at 34.)</p>


<u>Claim 17</u>	<u>Accused Instrumentalities</u>
	<p>The class keys are encrypted with a master key:</p> <div data-bbox="619 345 1825 824" style="background-color: black; color: white; padding: 10px;"> <p><b>User Keybags</b> Background</p> <p>Sets of keys generated for each user to protect their data at rest Keys wrapped by master key derived from user passcode and SEP UID After 10 incorrect passcode entries, SEP will not process any further attempts Different policy associated with each keybag key—Usage, availability</p> </div> <p>(<i>Id.</i>, at 25.)</p> <p>The random secret is issued to SKS. SKS is a Secure Key Service application which is located within the Secure Enclave on the SEP and is responsible for decrypting class keys. The random secret provided by SBIO is used to decrypt a master key ("4) decrypt master key"). The master key is concatenated with the UID of the SEP and thus class keys are decrypted and added to the SKS keyring ("5) decrypt class keys, add to keyring") for further use by the Secure Enclave. The decrypted class keys include, for example, the class key of class A.</p>
<p>17d. emitting a secure access signal conveying information dependent upon said accessibility attribute; and</p>	<p><i>The Accused Instrumentalities include a transmitter configured to emit a secure access signal conveying information dependent upon said accessibility attribute.</i></p> <p>For example, the Secure Enclave emits a signal with ephemerally re-encrypted file keys:</p>


<u>Claim 17</u>	<u>Accused Instrumentalities</u>
	<p>“sepOS can then use the ephemeral wrapping key to wrap file keys for use by the Application Processor file-system driver. When the file-system driver reads or writes a file, it sends the wrapped key to the AES Engine.” (Ex. A, Apple Platform Security, at 14.)</p> <p>"All wrapped file key handling occurs in the Secure Enclave; the file key is never directly exposed to the Application Processor. [...] When the Secure Enclave unwraps a file's keys, they're rewrapped with the ephemeral key and sent back to the Application Processor." (<i>Id.</i> at 85.)</p> <p>The signal with the ephemerally re-encrypted file keys is a secure signal because it comes from the Secure Enclave and thus from a secure environment. Furthermore, the signal is secure because the transmitted information is encrypted. The emitted file keys are encrypted with the ephemeral key:</p> <p>"All wrapped file key handling occurs in the Secure Enclave; the file key is never directly exposed to the Application Processor. At startup, the Secure Enclave negotiates an ephemeral key with the AES Engine. When the Secure Enclave unwraps a file's keys, they're rewrapped with the ephemeral key and sent back to the Application Processor." (<i>Id.</i>)</p>

<u>Claim 17</u>	<u>Accused Instrumentalities</u>
	<p data-bbox="612 279 1415 354">Filesystem Data Protection</p> <p data-bbox="612 370 840 425">Overview</p> <p data-bbox="612 483 1478 522">File blocks are encrypted using AES-XTS with 128-bit keys</p> <p data-bbox="612 544 1898 587">Each file on the user partition is encrypted using a unique random key chosen by SEP</p> <p data-bbox="612 609 1244 652">Raw file keys are never exposed to the AP</p> <ul data-bbox="612 673 1638 776" style="list-style-type: none"><li data-bbox="612 673 1564 717">• Wrapped with a key from the user keybag for long-term storage</li><li data-bbox="612 734 1638 776">• Wrapped with an ephemeral key while in use, bound to boot session</li></ul> <p data-bbox="612 782 1266 815">(Ex. B, Behind the Scenes with iOS Security, at 29.)</p>

<u>Claim 17</u>	<u>Accused Instrumentalities</u>
	<div data-bbox="612 279 1783 928" style="background-color: black; color: white; padding: 20px;"> <h2 style="text-align: center;">Filesystem Data Protection</h2> <p>The diagram illustrates the process of filesystem data protection across four layers: User, Kernel, SEP (Secure Enclave), and Hardware.          <ul style="list-style-type: none"> <li><b>User:</b> Initiates the process with <code>open("foo.txt", ...)</code>.</li> <li><b>Kernel:</b> <ol style="list-style-type: none"> <li>Fetches wrapped file key from metadata (HPS).</li> <li>Communicates with the Key Store.</li> <li>Communicates with the AES Engine.</li> <li>Sends an ID command with an ephemerally wrapped file key (via the NVME Driver).</li> </ol> </li> <li><b>SEP:</b> <ol style="list-style-type: none"> <li>Unwraps the file key using a keybag key.</li> <li>Wraps the file key using an ephemerally wrapped key, returning it to the kernel.</li> </ol> </li> <li><b>Hardware:</b> <ul style="list-style-type: none"> <li>NAND stores the data.</li> <li>Storage Controller receives clear text from the NVME Driver and sends cipher text to the NAND.</li> <li>An Ephemeral Key is established on boot.</li> </ul> </li> </ul> </p> </div> <p><i>(Id., at 30.)</i></p> <p>The information transmitted by the emitted signal, i.e., the ephemerally re-encrypted file keys, is dependent on the availability attribute, i.e., the confirmation that a biometric "template match" exists. This confirmation is signaled by the issuance of the random secret (cf. step 3): Only if there is a confirmation of the match and the random secret is issued by the Touch ID or Face ID subsystem within the Secure Enclave, i.e. SBIO, the class key is available for re-encrypting the file keys.</p> <p>The re-encrypted file keys are therefore information which is emitted depending on the fact that the availability attribute has been emitted.</p>
17e. providing conditional access to the controlled	<i>The Accused Instrumentalities are configured to provide conditional access to the controlled item dependent upon said information.</i>

<u>Claim 17</u>	<u>Accused Instrumentalities</u>
<p>item dependent upon said information, wherein the controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing device.</p>	<p>More specifically, the controlled item is a locking mechanism of the door lock of the user's home. The Accused Instrumentalities are configured to provide secure access to the user's home via Yale Smart Locks when the user provides biometric signal to the Accused Instrumentalities via Touch ID or Face ID.</p> <p>"When the "Secure Remote Access" feature is turned on, the app will use your phone's built-in authentication tools to prompt fingerprint or facial recognition before you can unlock or lock your home remotely (note: if your phone does not have these features, it will prompt you to use your PIN code). This further ensures that your door is only operated by the right people at the time you intend for it."</p> <p>(<a href="https://us.yalehome.com/en/yale-news/blog/latest-blog-posts/introducing-biometric-verification-for-august-and-yale-locks/">https://us.yalehome.com/en/yale-news/blog/latest-blog-posts/introducing-biometric-verification-for-august-and-yale-locks/</a>)</p>

<u>Claim 17</u>	<u>Accused Instrumentalities</u>
	 <p>The screenshot shows a mobile application interface for Yale. At the top, there is a yellow circular logo with the word "Yale" in black. To the left of the logo is a hamburger menu icon and the word "Open". To the right is a magnifying glass search icon. Below the navigation bar, the text "Introducing Biometric Verification for August and Yale Locks" is displayed in a bold, black font. Underneath the text is a photograph of a hand holding a smartphone. The phone's screen displays a biometric verification interface with a red circular camera overlay and a black square in the center containing a white "16" and a camera icon. Below the photograph, the URL <a href="https://us.yalehome.com/en/yale-news/blog/latest-blog-posts/introducing-biometric-verification-for-august-and-yale-locks1/">https://us.yalehome.com/en/yale-news/blog/latest-blog-posts/introducing-biometric-verification-for-august-and-yale-locks1/</a> is provided in a smaller black font.</p>

<u>Claim 17</u>	<u>Accused Instrumentalities</u>
	 <p>(<a href="https://www.apple.com/shop/product/HPAR2ZM/A/yale-assure-lock-sl-touchscreen-deadbolt-black">https://www.apple.com/shop/product/HPAR2ZM/A/yale-assure-lock-sl-touchscreen-deadbolt-black</a>)</p>