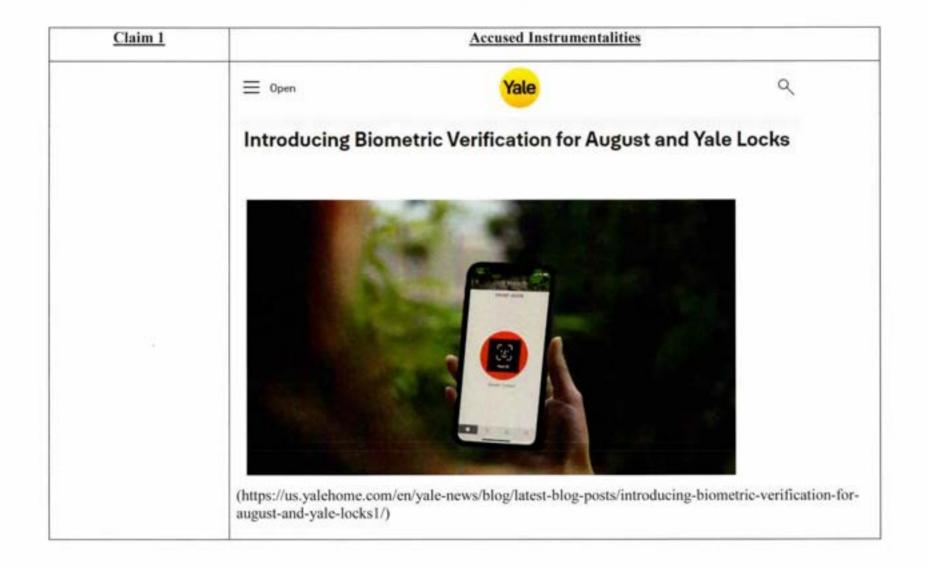
Exhibit I

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.

Claim 1	Accused Instrumentalities	
A system for providing secure access to a	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.	
controlled item, the system comprising:	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.	
	"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/)	



Claim 1	Accused Instrumentalities
	1 2 3 4 5 6 7 8 9 V 0 0
	(https://www.apple.com/shop/product/HPAR2ZM/A/yale-assure-lock-sl-touchscreen-deadbolt-black)

<u>Claim 1</u>	Accused Instrumentalities		
	The Accused Instrumentalities compatible with Yale Smart Locks are shown below: Compatibility		
	iPhone Models iPhone 12 Pro iPhone 12 Pro Max iPhone 12 iPhone 12 iPhone 12 iPhone 12 iPhone 11 iPhone 12 iPhone 11		
1a. a memory comprising a database of biometric signatures;			

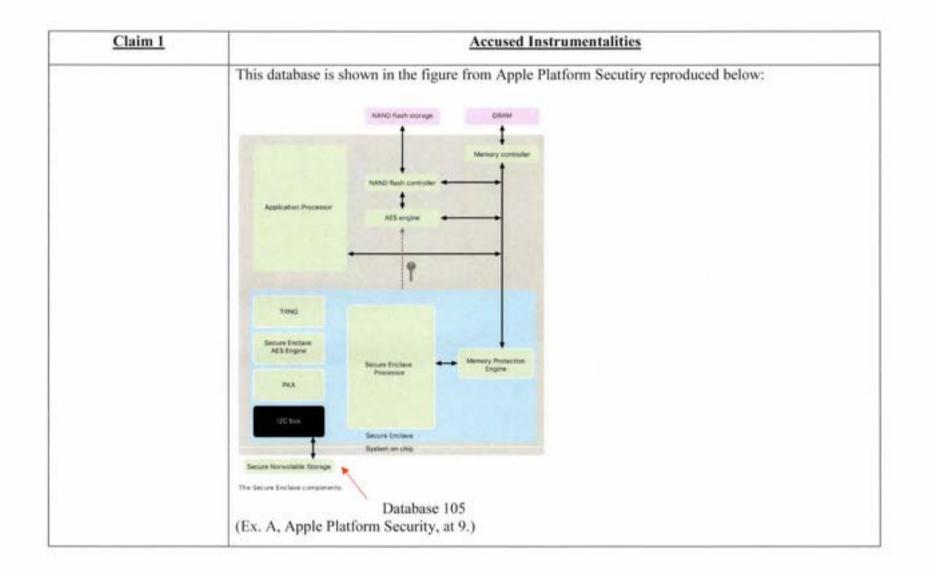
Claim 1	Accused Instrumentalities	
	More specifically, the iPhone allows multiple biometric signatures to be entered into a database on the iPhone: Touch ID	
	The iPhone allows the registration of multiple fingerprints:	
	Fig. from https://support.apple.com/en-us/HT201371 under Manage Touch ID Settings. In the second bullet, it literally says:	
	"Register up to five fingerprints."	
	"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."	

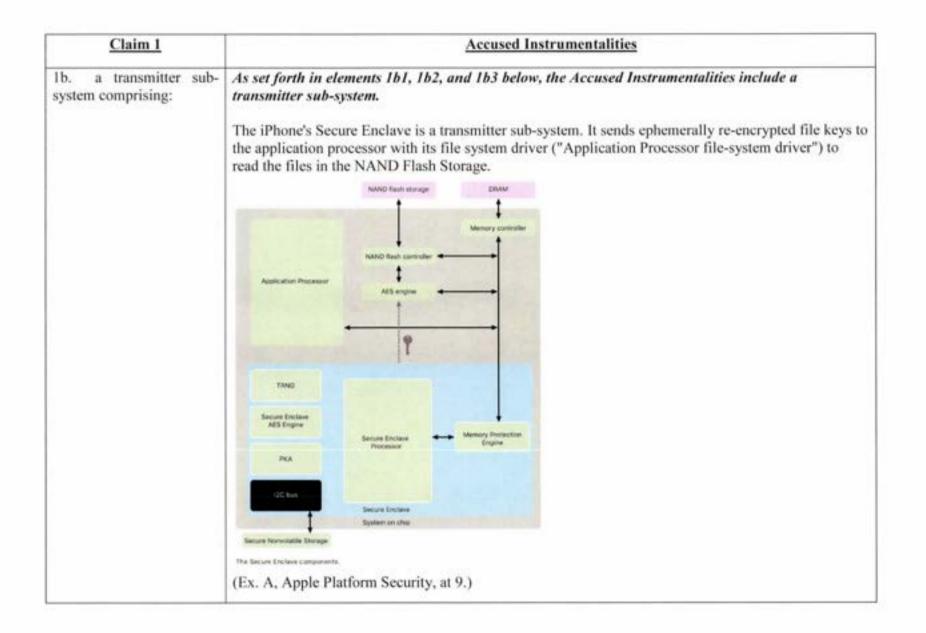
Claim 1	Accused Instrumentalities
	(https://support.apple.com/en-us/HT204587) "Touch ID can read multiple fingerprints and recognize fingerprints at any orientation of the finger. The system then creates a mathematical representation of your fingerprint and compares it to the registered fingerprint data to determine a match and unlock your device." (https://support.apple.com/en-us/HT204587)
	Face ID
	The iPhone allows the registration of multiple faces:
	Bewengs dien Kapf langsaan im Kreis, um ihn zu schließen.
	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 https://support.apple.com/en-us/HT208109 in the second section "Configure Face ID", there also the figure shown above.

Claim 1	Accused Instrumentalities
	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; https://www.macworld.co.uk/how-to/second-face-id-3803421/), a second face is registered by the iPhone in the same way as the first face. "Set up Face ID or add another face. • Select "Settings" > "Face ID & Code" > "Configure alternate appearance" if you want to configure another face to be recognized by Face ID." (https://support.apple.com/de-de/guide/iphone/iph6d162927a/ios)

Claim 1	Accused Instrumentalities		
	(2)		
	(4)		
	subject of PDH		
	(Turnets App Store		
	Apple		
	Passw: utoFill		
	Other Ap A Apply 1		
	Printer can a fee fire project, Printer-disconnected feetings of an inter-security automotion for proper unit disconnection for the printer and disconnection for the printer an		
	Set Up an Alternative Approximation		
	In addition in community learning tree you, Face III for recognise an alternative appropriate		
	Reset face (i)		
	MITMENTAL CONTRACTOR OF THE PROPERTY OF THE PR		
	Require Attention for Face ID		
	The page How To Add A Second Face To Face ID - Macworld UK		
	(https://www.macworld.co.uk/how-to/second-face-id-3803421/) literally states:		
	"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.		
	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."		
	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:		

Claim 1	Accused Instrumentalities
	"The Secure Enclave is a system on chip (SoC) that is included on all recent iPhone, devices" (Ex. A, Apple Platform Security, at 7.)
	"The Secure Enclave is a dedicated secure subsystem integrated into Apple systems on chip (SoCs)." (<i>Id.</i> , at 9.)
	The Secure Enclave Processor provides the main computing power for the Secure Enclave." (<i>Id.</i> , at 10.)
	"During enrollment, the Secure Enclave processes, encrypts, and stores the corresponding Touch ID and Face ID template data." (<i>Id.</i> , at 19.)
	The Secure Enclave has access to a memory assigned to it and accessible only to it:
	Secure nonvolatile storage "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." (Id., at 15.)
	This memory serves as a database for storing the biometric signatures:
	"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:
	 Adding or removing a Touch ID fingerprint or Face ID face".
	(Id., at 16.)





	Accused Instru	amentanties	
"sepOS can then use the ephen Processor file-system driver. wrapped key to the AES Eng (Id., at 14.) "All wrapped file key handling the Application Processor. [] the ephemeral key and sent ba (Id., at 85.)	when the file-system ine. " coccurs in the Secure I When the Secure Enc	driver reads or v Enclave; the file ke lave unwraps a file	ey is never directly exposed to
The file system driver of the ap	oplication processor is	an NVME driver:	
Filesystem Da	ta Protectio	n	
User	Kernel		SEP
apen("Saatxi",)	Fetch waspeed Te key from metadata	F5 Kiry S	2. Unierap file Jey using keybag key
	4. Send IO command with epitemesally misoped file, key	Oriver AES En	Wrap frir_key using ephermonal_key, return ephermonally wrapped file_key to kernel
Hardware			phemeral Key shished on boot
4	The second secon	Hardware NAND	Hardware NAND Controller

Claim 1	Accused Instrumentalities		
1b1. a biometric sensor configured to receive a biometric signal;	The Accused Instrumentalities include a biometric sensor configured to receive a biometric signal. 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.		
	Touch ID		
	"Apple devices with a Touch ID sensor can be unlocked using a fingerprint." (Ex. A, Apple Platform Security, at 19.)		
	"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.)		
	"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." (Id.)		
	The biometric sensor for Touch ID is located below the home button:		
	"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)		

Claim 1	Accused Instrumentalities
	Laser-cut sapphire crystal Stainless steel detection ring Touch ID sensor Tactile switch
	Biometric sensor 121
	"Where is the Touch ID sensor located?
	The Touch ID sensor is located either in the home button or - on the iPad Air (4th generation) - in the top button.
	(https://support.apple.com/en-us/HT201371)
	The image sensor captures an 88-by-88-pixel, 500 PPI raster scan:
	"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."

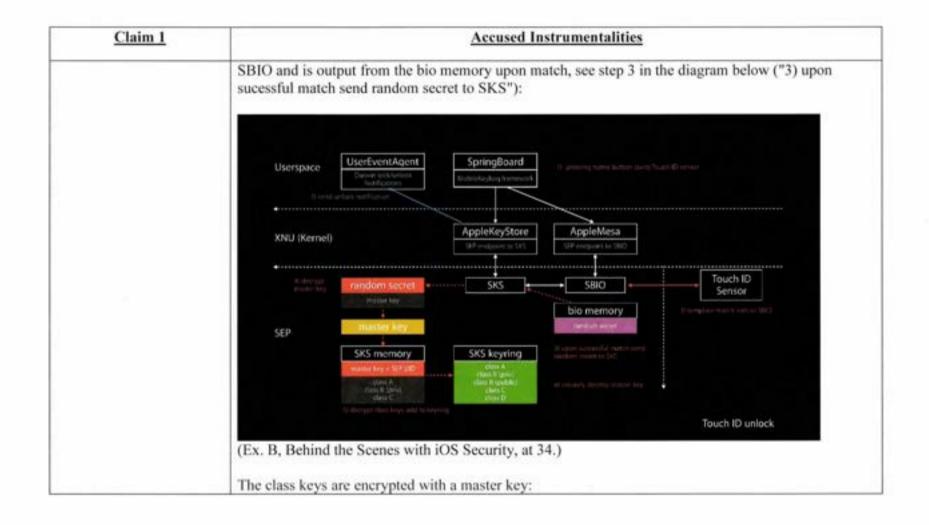
Claim 1	Accused Instrumentalities	
	(Ex. C, iOS Security white paper, at 8.)	
	Face ID	
	The biometric sensor for facial biometrics is a camera system ("TrueDepth camera system") with an image sensor.	
	"With a simple glance, Face ID securely unlocks supported Apple devices. It provides intuitive and 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.)	
	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.	
	"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 sequence of 2D images and depth maps, 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." (Id.)	
	The camera system includes a biometric image sensor, namely a "CMOS image" sensor from Sony, to perform facial biometrics:	

Claim 1	Accused Instrumentalities				
	Structured light receiver Module: Hen-hall Sharp Chical Indian Interest In	TOP If your state of the state	Ambient light sensor Module AMS	Module: Hon-hal, Cowell, O-Rim DA/OS image sector (RMS) Serry Darts RAT Limpson, Gerviss Systems Kycoers, NTK	Connection Connec
	(https://appleinsiderreport)	r.com/articles/17	Active oil gement	rkings-of-apples-f	Admir algorited southwest
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	More specifically, t Processor (SEP) or biometric signal wi	the iPhone's Syst a Secure Neural th elements of the	tem on Chip (SO Engine containe the biometric sign the chip (SoC) that	C), i.e. the Secure of therein, is a measure database.	gured to emit a secure access bute. Enclave with its Secure Enclave ins (103) to check a match of the recent iPhone, devices"

Claim 1	Accused Instrumentalities
	"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). " (<i>Id.</i> , at 19.)
	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.
	For Touch ID, the Secure Enclave match verification is performed as follows:
	"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.)
	"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.)
	"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. " (https://support.apple.com/en-us/HT204587)
	"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." (https://support.apple.com/de-de/HT204587)

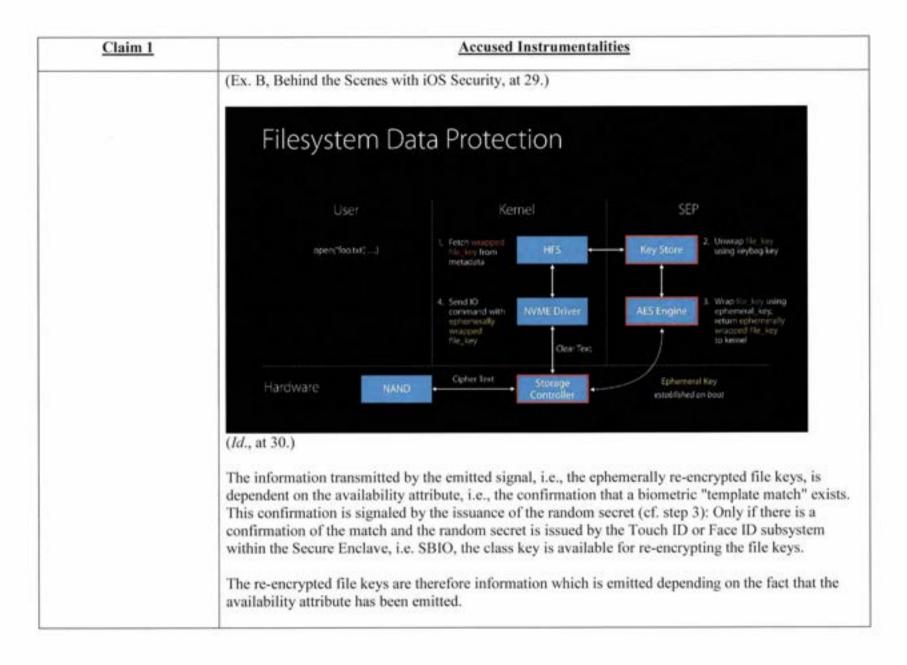
Claim 1	Accused Instrumentalities
	For Face ID , the Secure Enclave has a neural network protected by it, i.e., a Secure Neural Engine, which is used to verify the match:
	"Face ID uses neural networks for determining attention, matching , and antispoofing, so a user can unlock their phone with a glance." (Ex. A, Apple Platform Security, at 20.)
	"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>).
	"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." (Id. at 23.)
	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").
	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:
	"During matching, the Secure Enclave compares incoming data from the biometric sensor against the stored templates to determine whether to unlock the device []." (Id. at 19.)

Claim 1	Accused Instrumentalities
	"Uses for Touch ID and Face ID
	Unlocking a device or user account
	[] keys for the highest class of Data Protection-which are held in the Secure Enclave [].
	With Touch ID or Face ID enabled, the keys aren't discarded when the device or account locks; instead, they're wrapped with a key that's given to the Touch ID or Face ID subsystem inside the Secure Enclave. When 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. 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.)
	"The class key is protected with the hardware UID and, for some classes, the user's passcode." (<i>Id.</i> at 85.)
	"Complete Protection
	(NSFileProtectionComplete): 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, 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."
	(Id. at 86.)
	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

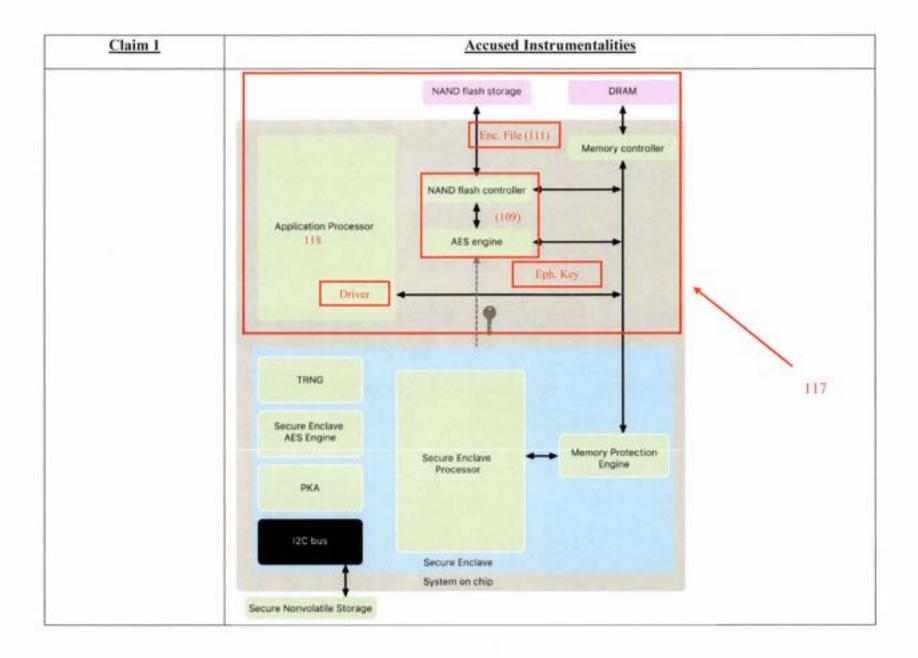


Claim 1	Accused Instrumentalities
	User Keybags
	User Keybags Background
	Sets of keys generated for each user to protect their data at rest
	Keys wrapped by master key derived from user passcode and SEP UID
	After 10 incorrect passcode entries, SEP will not process any further attempts
	Different policy associated with each keybag key—Usage, availability
	(Id., at 25.)
	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.
1b3. a transmitter configured to emit a secure access signal conveying	The Accused Instrumentalities include a transmitter configured to emit a secure access signal conveying information dependent upon said accessibility attribute.
information dependent upon said accessibility	For example, the Secure Enclave emits a signal with ephemerally re-encrypted file keys:
attribute; and	"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."

Claim 1	Accused Instrumentalities
	(Ex. A, Apple Platform Security, at 14.)
	"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." (Id. at 85.)
	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:
	"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." (Id.)
	Filesystem Data Protection
	Overview
	File blocks are encrypted using AES-XTS with 128-bit keys
	Each file on the user partition is encrypted using a unique random key chosen by SE
	Raw file keys are never exposed to the AP
	 Wrapped with a key from the user keybag for long-term storage
	 Wrapped with an ephemeral key while in use, bound to boot session

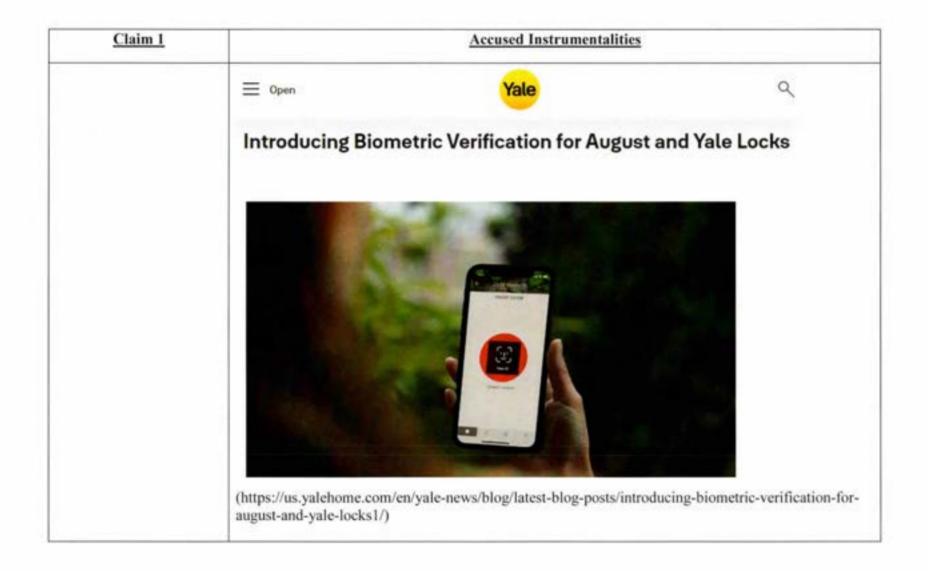


Claim 1	Accused Instrumentalities		
1c. a receiver sub-system comprising:	As set forth in elements 1c1 and 1c2 below, the Accused Instrumentalities include a receiver subsystem.		
	The receiver subsystem is the part of the system outside the Secure Enclave that is responsible for reading encrypted files from the NAND Flash Storage and receives ephemerally re-encrypted file keys from the Secure Enclave for this purpose:		



Claim 1	Accused Instrumentalities					
	(Ex. A, Apple Platform Security, at 9.)					
lc1. a receiver sub-system controller configured to: receive the transmitted secure access signal; and	The Accused Instrumentalities include a receiver sub-system controller configured to: receive the transmitted secure access signal. 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: Filesystem Data Protection					
	User	Ke	mel	SEP		
	open("foo.tist";3	Fetch waspoold file, key from metadata	HFS	Key Store	Unwrap file, key using keybog key	
		Send KO command with ephemerally wrapped	NVME Driver	AES Engine	3. Whap fire key using ephemeral key, seturn ephemerally wrapped file, key	
		file_key	Clear Text		to kernel	

Claim 1	Accused Instrumentalities
	"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.) "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." (Id., at 85.)
1c2. provide conditional access to the controlled item dependent upon said information;	The Accused Instrumentalities include a receiver sub-system configured to provide conditional access to the controlled item dependent upon said information. 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.
	"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/)



Claim 1	Accused Instrumentalities
	1 2 3 4 5 6 7 8 9 V 0 0
	(https://www.apple.com/shop/product/HPAR2ZM/A/yale-assure-lock-sl-touchscreen-deadbolt-black)

Claim 1	Accused Instrumentalities		
1d. wherein the transmitter sub-system controller is further configured to:	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.		
1d1. receive a series of entries of the biometric signal, said series being characterized according to	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.		
at least one of the number of said entries and a duration of each said entry;	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.		
, , , , , , , , , , , , , , , , , , ,	"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.)		
	Touch ID		
	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.		
	"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." (Id.)		
	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.		
	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.		

Claim 1	Accused Instrumentalities
	Set up Touch ID
	Before you can set up Touch ID, you must first create a <u>code</u> for your device,* then follow these steps: 1. Make sure the Touch ID sensor and your finger are clean and dry.
	Tap Settings > Touch ID & Code, and then enter your code.
	Tap "Add fingerprint" and hold the device as you normally would when touching the Touch ID sensor.
	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. Place Your Finger In and total part from the town to th
	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.

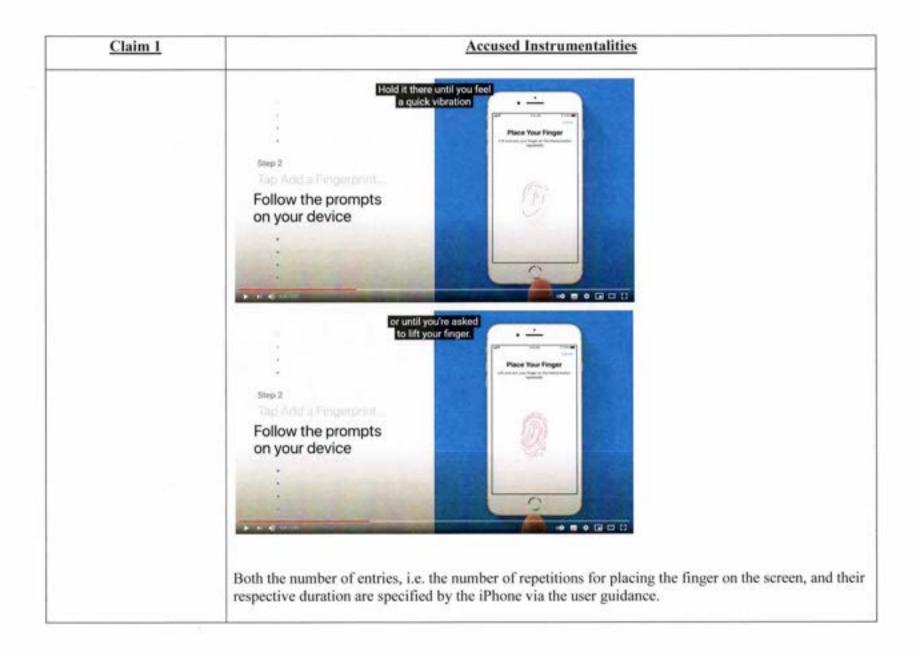
<u>Claim 1</u>	Accused Instrumentalities
	6. The next screen will ask you to change your finger position. Hold your device as you normally would when unlocking it. Touch the Touch ID sensor with the outer edges of your fingertip instead of the middle part as you would during the first scan."
	(https://support.apple.com/en-us/HT201371)
	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.
	Face ID
	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").
	"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 sequence of 2D images and depth maps, 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." (Ex. A, Apple Platform Security, at 20.)
	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

Claim 1	Accused Instrumentalities
	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.
	Using Face ID on iPhone
	1. Tap Settings > Face ID & Code. Enter your code when prompted.
	2. Tap on "Configure Face ID".
	3. Hold the device in portrait mode in front of your face and tap "Let's go".
	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".
	5. After performing the first Face ID scan, tap "Next".
	6. Again, slowly describe a circle with your head until it is completed.
	7. Tap "Done."
	(https://support.apple.com/en-us/HT208109)
	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).
	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 https://www.macworld.co.uk/how-to/second-face-id-3803421/, a second face is registered by the iPhone in the same way as the first face.

Claim 1	Accused Instrumentalities
	< Setting: Face ID & Passcode (□□)
	#Phone Unitods
	Throat App Store
	Appl
	Passwo LutoFill
	Other Apr 4 April 4
	Officer (24) A Constitution of State contract of State contract of State contract of State Constitution of Sta
	Set Up an Alternative Appearance
	To autilities to continuously, transmit from your leaf. Face: If you property an alternative approximate.
	Reset Face ID
	ACTEMOTOR
	Require Attention for Face ID
	The series of entries of the biometric signal is identified on the iPhone by both the number and duration of each such entry.
	Touch ID
	According to step 5 of the instructions https://support.apple.com/en-us/HT201371 , for the enrollment of a single finger, the user has to repeatedly place the respective finger on the sensor and thus a numbe 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.

Claim 1	Accused Instrumentalities
	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.
	Set up Touch ID
	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.
	Curice Place Your Finger Uit and rest your frager on the Hone
	bution repeatedly.
	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.
	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.
	(https://support.apple.com/en-us/HT201371)

Claim 1	Accused Instrumentalities
	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:
	Place Your Finger Lift and rest your finger on the Home button repeatedly.
	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. This is shown in the Apple You Tube video (32) How to set up Touch ID on your iPhone or iPad - Apple Support - YouTube (https://www.youtube.com/watch?v=xTZ2LALWZlg):



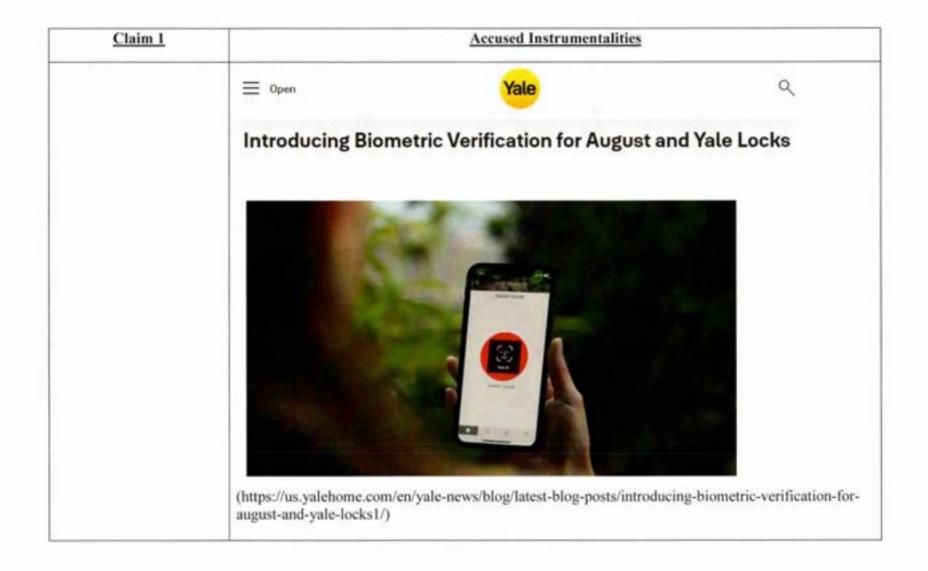
Claim 1	Accused Instrumentalities
	Face ID The user moves his face in front of the camera to strike different poses, and the camera system with image sensor continuously captures a large number of biometric entries, i.e. here the 2D images with depth information, in a row.
	"This enrolled facial data is itself a mathematical representation of the user's face captured across a variety of poses." (Ex. A, Apple Platform Security, at 20.)
	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:
	Move your hand storely to complete the circle. Individual images taken from: https://support.apple.com/en-us/HT208109)

<u>Claim 1</u>	Accused Instrumentalities	
1d2. map said series into an instruction; and	The Accused Instrumentalities include a transmitter sub-system controller configured to map said series into an instruction.	
	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").	
	"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.)	
	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." (Id., at 10.)	
	Touch ID	
	The instruction here involves the processing of under-the-skin fingerprint characteristics and their encrypted storage.	
	"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.)	
	Face ID	

Claim 1	Accused Instrumentalities
	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.
	"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.)
	"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: • The mathematical representations of a user's face calculated during enrollment
	(<i>Id.</i> , at 23.)

<u>Claim 1</u>	Accused Instrumentalities
1d3. populate the database according to instruction,	se The Accused Instrumentalities include a transmitter sub-system controller configured to populate the database according to the instruction.
mstruction,	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":
	"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:
	•
į	 Adding or removing a Touch ID fingerprint or Face ID face". (Ex. A, Apple Platform Security, at 16.)
	"During enrollment, the Secure Enclave processes, encrypts, and stores the corresponding Touch ID and Face ID template data." (Id., at 19.)
	Touch ID
	"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" (Id.)
	Face ID
	The following Face ID data is saved, encrypted only for use by the Secure Enclave, during normal operation:
	• The mathematical representations of a user's face calculated during enrollment". (Id., at 23.)

Claim 1	Accused Instrumentalities
wherein the controlled item is one of: a locking mechanism of a physical access structure or an	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.
electronic lock on an electronic computing device.	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.
	"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/)



Claim 1	Accused Instrumentalities
	1 2 3 4 5 6 7 8 9 V 0 0
	(https://www.apple.com/shop/product/HPAR2ZM/A/yale-assure-lock-sl-touchscreen-deadbolt-black)

Claim 2	Accused Instrumentalities
The system according to claim 1, wherein the transmitter sub-system	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.

Claim 2	Accused Instrumentalities	
controller is further configured to:		
2a. provide a signal for directing input of the series of entries of the biometric	Upon information and belief, the Accused Instrumentalities are configure to provide a signal for directing input of the series of entries of the biometric signal.	
signal;	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.	
	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.	
	(https://video.search.yahoo.com/yhs/search?fr=yhs-pty_converter&hsimp=yhs-pty_converter&hspart=pty&p=registering+fingerprint+apple+touch+id+on+screen+instructions#id=1&vid=156de65ae06ca453643009fc0ea9cf79&action=click.)	
	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." (https://support.apple.com/en-au/HT201371)	
	Touch ID: "you shouldn't tap too quickly or move your finger around" (https://support.apple.com/en-us/HT207537)	
	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. (https://www.imore.com/how-set-face-id-iphone)	

Claim 2	Accused Instrumentalities	
	Place Your Finger Lift and rest your finger on the Home button repositedly.	
	(https://support.apple.com/en-us/HT201371)	

Claim 2	Accused Instrumentalities
	More your head showly to complete the circle. (https://support.apple.com/en-us/HT208109)
2b. incorporate into the secure access signal an identification field identifying the biometric signal if the signal matches a member of the database; and	Upon information and belief, the Accused Instrumentalities are configure to incorporate into the secure access signal an identification field identifying the biometric signal if the signal matches a member of the database. 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. "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." (https://support.apple.com/ko-kr/guide/security/sec067eb0c9e/1/web/1)

Claim 2	Accused Instrumentalities
	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.)
2c. construct an audit trail of biometric signals provided to the biometric sensor in order to access the controlled item.	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. 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.
	"Touch ID will incrementally update the mathematical representation of enrolled fingerprints over time to improve matching accuracy." (https://support.apple.com/en-us/HT204587)
	"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." (https://support.apple.com/en-us/HT208108)
	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.

Claim 4 Accused Instrumentalities 4. The system according to The Accused Instrumentalities includes a biometric sensor that is responsive to one of voice, retinal claim 1, wherein the 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. biometric sensor is responsive to one of voice, More specifically, the Accused Instrumentalities include a CMOS image sensor in the front camera of retinal pattern, iris pattern, the iPhones that is responsive to face pattern of the user. Upon information and belief, the Secure face pattern, and palm Nonvolatile Storage is a memory including a database of the face data. configuration, and/or the database of biometric Face ID signatures is located in at The biometric sensor for facial biometrics is a camera system ("TrueDepth camera system") with an least one of the transmitter image sensor. sub-system and the "With a simple glance, Face ID securely unlocks supported Apple devices. It provides intuitive and receiver sub-system. 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.) (https://appleinsider.com/articles/17/09/09/inner-workings-of-apples-face-id-camera-detailed-inreport)

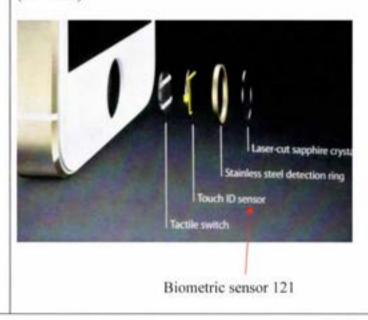
The Accused Instrumentalities includes a biometric sensor that is further configured to authenticate the identity of a user. More specifically, the iPhones uses Face ID and Touch ID to authenticate the user's identity. Face ID The biometric sensor for facial biometrics is a camera system ("TrueDepth 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.)
Andwert fant Received And Part Print camera Committee Consent of the Consent

"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.)



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

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.

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.

"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."

(https://us.yalehome.com/en/yale-news/blog/latest-blog-posts/introducing-biometric-verification-for-august-and-yale-locks1/)

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.

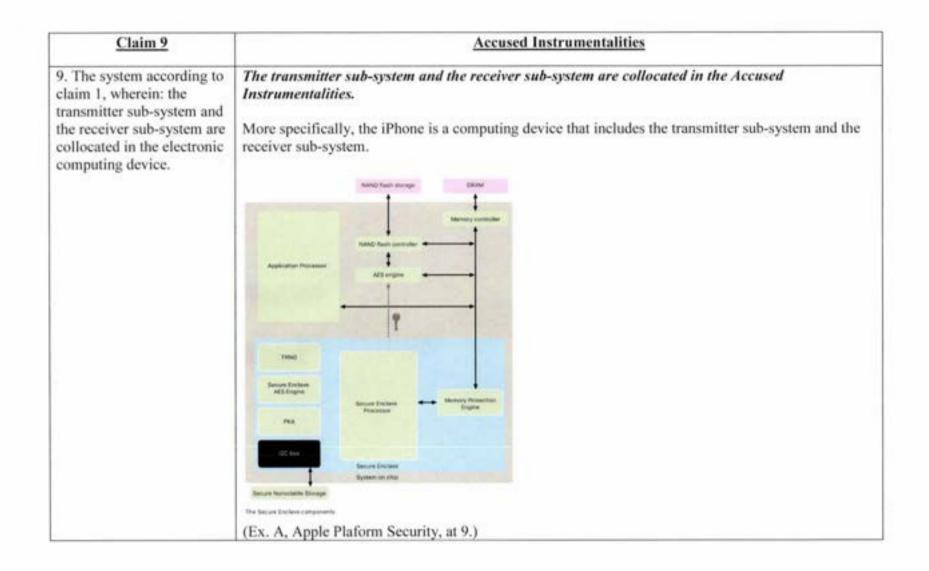
More specifically, upon information and belief, the Yale Home Smart Lock is configured to receive information allowing its unlocking from the Secure Enclave of the iPhone.

"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)



IPR2022-01094

Claim 10	Accused Instrumentalities
10. A transmitter subsystem for operating in a system for providing secure access to a controlled item, wherein the transmitter sub-system comprises:	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.
10a. a biometric sensor configured to receiving a biometric signal;	The Accused Instrumentalities include a biometric sensor configured to receive a biometric signal. 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.
	Touch ID
	"Apple devices with a Touch ID sensor can be unlocked using a fingerprint." (Ex. A, Apple Platform Security, at 19.)
	"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.)
	"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." (Id.)

Claim 10	Accused Instrumentalities
	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 capacitive touch sensor installed underneath the cover: A CMOS chip with small capacitors." (https://appleinsider.com/inside/touch-id) Laser-cut supphire crystal lens. The surrounding stainless steel detection ring Touch ID sensor Touch ID is located below the home button: "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 capacitive touch sensor installed underneath the cover: A CMOS chip with small capacitors." [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 capacitive touch sensor installed underneath the cover: A CMOS chip with small capacitors." [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 capacitive touch sensor installed underneath the cover: A CMOS chip with small capacitors."
	"Where is the Touch ID sensor located?
	The Touch ID sensor is located either in the home button or - on the iPad Air (4th generation) - in the top button.
	(https://support.apple.com/en-us/HT201371)
	The image sensor captures an 88-by-88-pixel, 500 PPI raster scan:

Claim 10	Accused Instrumentalities
	"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.)
	Face ID
	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.)
	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.
	"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 sequence of 2D images and depth maps, 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." (Id.)

Claim 10	Accused Instrumentalities
	The camera system includes a biometric image sensor, namely a "CMOS image" sensor from Song perform facial biometrics:
	Structured light receiver Median How has been Common Structured from Structur
	Active alignment Active alignment Active alignment
	(https://appleinsider.com/articles/17/09/09/inner-workings-of-apples-face-id-camera-detailed-in- report)
10b. a controller configured to match the biometric signal against members of a database of biometric signatures to	The Accused Instrumentalities include a transmitter controller configured to emit a secure accessignal conveying information dependent upon said accessibility attribute.

Claim 10	Accused Instrumentalities
thereby output an accessibility attribute; and	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.
	"The Secure Enclave is a system on chip (SoC) that is included on all recent iPhone, devices" (Ex. A, Apple Platform Security, at 7.)
	"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). " (Id., at 19.)
	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.
	For Touch ID, the Secure Enclave match verification is performed as follows:
	"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.)
	"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.)
	"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. " (https://support.apple.com/en-us/HT204587)

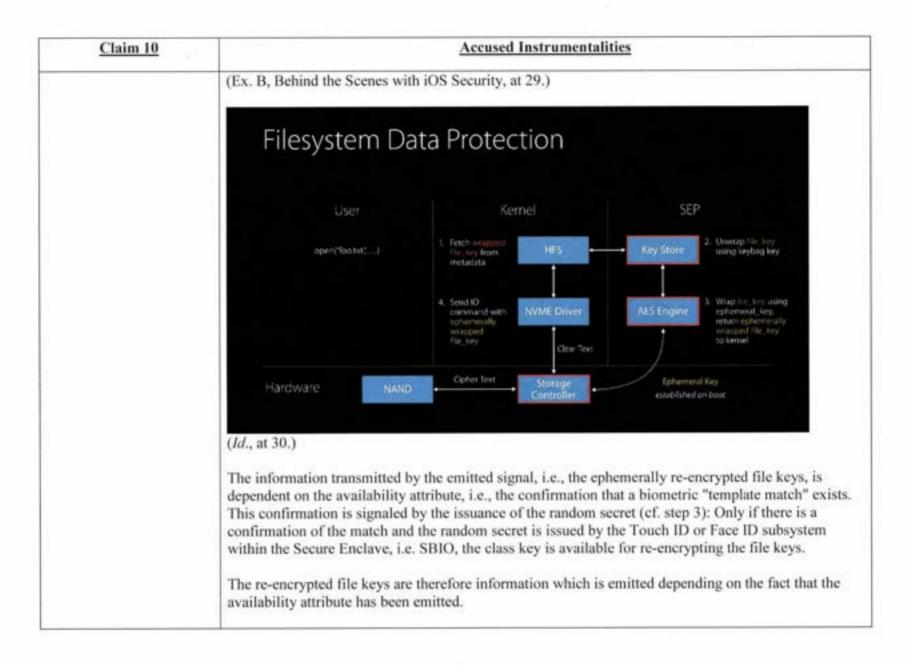
Claim 10	Accused Instrumentalities
	"Touch ID can read multiple fingerprints and recognize fingerprints at any orientation of the finger. The system then creates a mathematical representation of your fingerprint and compares it to the registered fingerprint data to determine a match and unlock your device." (https://support.apple.com/de-de/HT204587)
	For Face ID , the Secure Enclave has a neural network protected by it, i.e., a Secure Neural Engine, which is used to verify the match:
	"Face ID uses neural networks for determining attention, matching , and antispoofing, so a user can unlock their phone with a glance." (Ex. A, Apple Platform Security, at 20.)
	"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>).
	"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." (Id. at 23.)
	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").

Claim 10	Accused Instrumentalities
	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:
	"During matching, the Secure Enclave compares incoming data from the biometric sensor against the stored templates to determine whether to unlock the device []." (Id. at 19.)
	"Uses for Touch ID and Face ID
	Unlocking a device or user account
	[] keys for the highest class of Data Protection-which are held in the Secure Enclave [].
	With Touch ID or Face ID enabled, the keys aren't discarded when the device or account locks; instead, they're wrapped with a key that's given to the Touch ID or Face ID subsystem inside the Secure Enclave. When 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. This process provides additional protection by requiring cooperation between the Data Protection and Touch ID or Face ID subsystems to unlock the device."
	(Id. at 24.)
	"The class key is protected with the hardware UID and, for some classes, the user's passcode." (Id. at 85.)
	"Complete Protection
	(NSFileProtectionComplete): 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, 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."
	(<i>Id.</i> at 86.)

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 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"):
	Userspace UserEventAgent SpringBoard Userspace Indian term foods (Common Indian term foods (Common Indian term foods (Common Indian term foods (Common Indian India
	XNU (Kernel) AppleKeyStore SP andpose to SKS SP andpose to SKS
	random secrets SKS SBIO Touch ID Sensor
	SEP SKS memory SKS keyring Sine to the state of the state
	O der cyal state Anyo, wild be Anyong : Touch ID unlock
	(Ex. B, Behind the Scenes with iOS Security, at 34.) The class keys are encrypted with a master key:

Claim 10	Accused Instrumentalities
	User Keybags
	User Keybags Background
	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
	(Id., at 25.)
	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.
10c. a transmitter configured to emit a secure access signal	The Accused Instrumentalities include a transmitter configured to emit a secure access signal conveying information dependent upon said accessibility attribute.
conveying said information dependent	For example, the Secure Enclave emits a signal with ephemerally re-encrypted file keys:
upon said accessibility attribute;	"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."

Claim 10	Accused Instrumentalities
	(Ex. A, Apple Platform Security, at 14.)
	"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." (Id. at 85.)
	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:
	"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." (Id.)
	Filesystem Data Protection
	Overview
	File blocks are encrypted using AES-XTS with 128-bit keys
	Each file on the user partition is encrypted using a unique random key chosen by SEF
	Raw file keys are never exposed to the AP
	 Wrapped with a key from the user keybag for long-term storage
	 Wrapped with an ephemeral key while in use, bound to boot session



Claim 10	Accused Instrumentalities
10d. wherein the controller is further configured to:	The Accused Instrumentalities include a controller that is configured to be used as set forth in elements 10d1, 10d2, and 10d3 below.
10d1. receive a series of entries of the biometric signal, said series being	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.
characterised according to at least one of the number of said entries and a duration of each said	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.
entry;	"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.)
	Touch ID
	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.
	"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." (Id.)
	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.
	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.

Claim 10	Accused Instrumentalities
	Set up Touch ID
	Before you can set up Touch ID, you must first create a <u>code</u> for your device,* then follow these steps: 7. Make sure the Touch ID sensor and your finger are clean and dry.
	8. Tap Settings > Touch ID & Code, and then enter your code.
	Tap "Add fingerprint" and hold the device as you normally would when touching the Touch ID sensor.
	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. Place Your Finger Lin and met your frogen on the Home Doctor repeasedy.
	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.

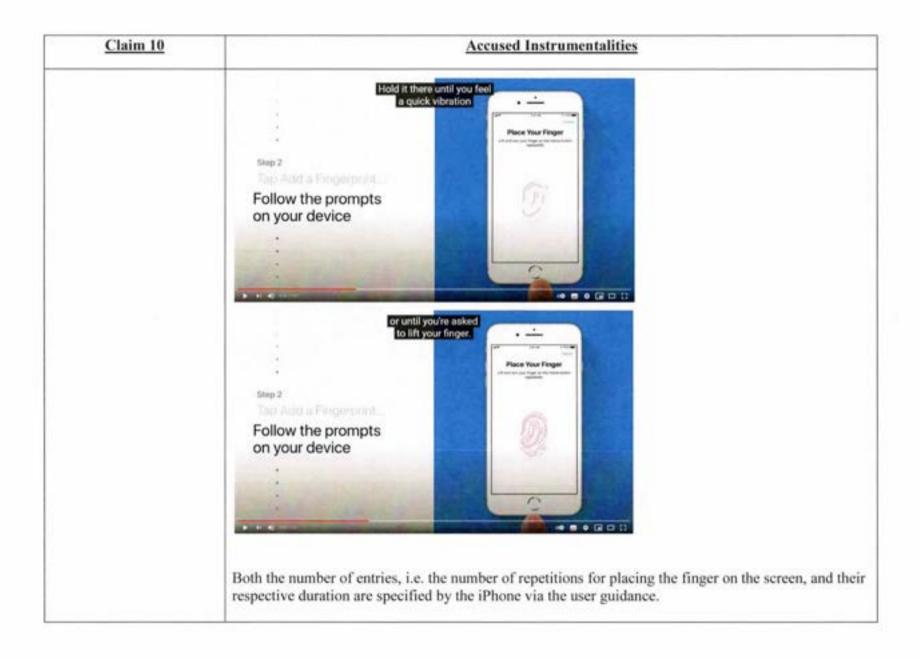
Claim 10	Accused Instrumentalities
	12. The next screen will ask you to change your finger position. Hold your device as you normally would when unlocking it. Touch the Touch ID sensor with the outer edges of your fingertip instead of the middle part as you would during the first scan."
	(https://support.apple.com/en-us/HT201371)
	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.
	Face ID
	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").
	"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 sequence of 2D images and depth maps, 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." (Ex. A, Apple Platform Security, at 20.)
	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

Claim 10	Accused Instrumentalities
	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.
	Using Face ID on iPhone
	1. Tap Settings > Face ID & Code. Enter your code when prompted.
	2. Tap on "Configure Face ID".
	3. Hold the device in portrait mode in front of your face and tap "Let's go".
	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".
	5. After performing the first Face ID scan, tap "Next".
	6. Again, slowly describe a circle with your head until it is completed.
	7. Tap "Done."
	(https://support.apple.com/en-us/HT208109)
	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).
	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 https://www.macworld.co.uk/how-to/second-face-id-3803421/, a second face is registered by the iPhone in the same way as the first face.

Claim 10	Accused Instrumentalities
	< Section Face ID & Passcode
	(3e)
	Phone Unicid
	iTueren App Store
	Appl
	Passw-S utoFill (C)
	Other April 4 April 1
	Principal Laboration and Part Laboration, Williams (Inc.) Authorities of your Authorities distributed to depart and glassing. Laboration (Laboration).
	Set Up an Alternative Appearance
	to addition to confinencing how you program on the confinencing from your time. Face:
	Reset Face (I)
	AFTINION
	Require Attention for Face ID
	The series of entries of the biometric signal is identified on the iPhone by both the number and duration of each such entry.
	Touch ID
	According to step 5 of the instructions https://support.apple.com/en-us/HT201371 , 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.

Claim 10	Accused Instrumentalities
	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.
	Set up Touch ID
	 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.
	-al ♦ 9-4) And 100% mm C.u/x.ts:
	Place Your Finger Lift and rest your finger on the Home button repealedly.
	5. Continue by raising and slowly lowering your finger over and over again, changing the position of your finger just a time.
	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.
	(https://support.apple.com/en-us/HT201371)

Claim 10	Accused Instrumentalities
	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: Place Your Finger Lit and lest your legt on the Home botton repeatedly.
	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. This is shown in the Apple You Tube video (32) How to set up Touch ID on your iPhone or iPad - Apple Support - YouTube (https://www.youtube.com/watch?v=xTZ2LALWZlg):

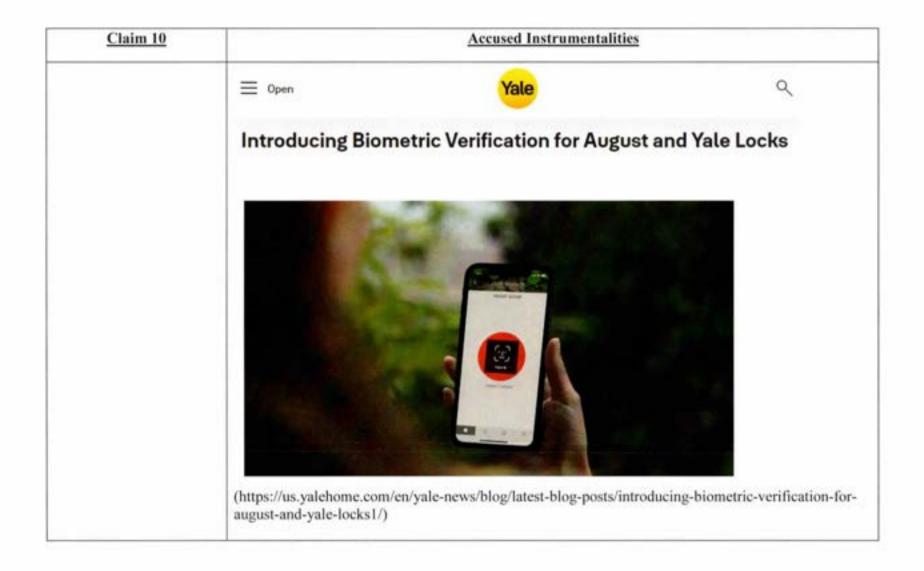


Claim 10	Accused Instrumentalities
Claim 10	Face ID The user moves his face in front of the camera to strike different poses, and the camera system with image sensor continuously captures a large number of biometric entries, i.e. here the 2D images with depth information, in a row. "This enrolled facial data is itself a mathematical representation of the user's face captured across a variety of poses." (Ex. A, Apple Platform Security, at 20.) 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:
	(Individual images taken from: https://support.apple.com/en-us/HT208109)
10d2. map said series into an instruction; and	The Accused Instrumentalities include a transmitter sub-system controller configured to map said series into an instruction.

Claim 10	Accused Instrumentalities
	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").
	"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.)
	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." (Id., at 10.)
	Touch ID
	The instruction here involves the processing of under-the-skin fingerprint characteristics and their encrypted storage.
	"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.)
	Face ID 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.

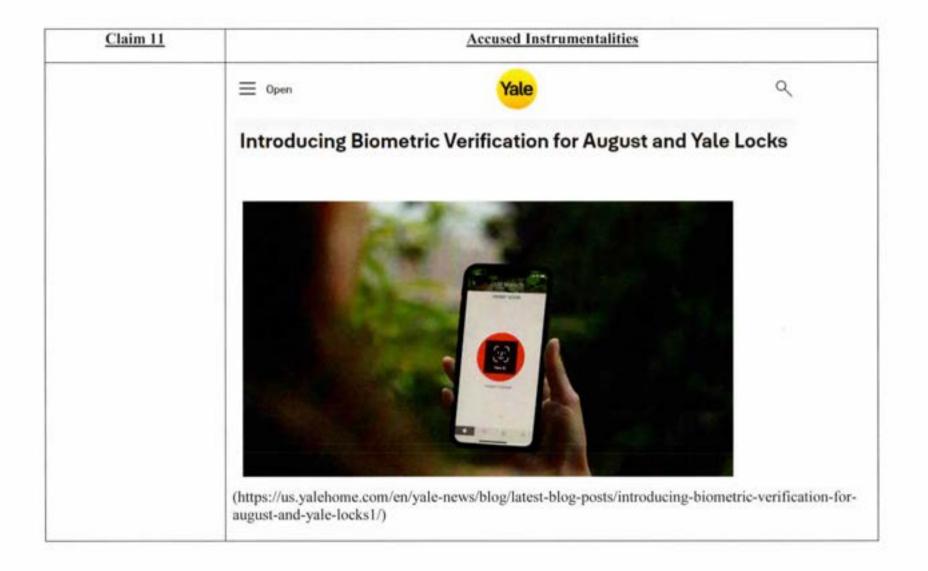
Claim 10	Accused Instrumentalities
	"A portion of the Secure Neural Engine-protected within the Secure Enclave-transforms this data into a mathematical representation and compares that representation to the enrolled facial data. This enrolled facial data is itself a mathematical representation of the user's face captured across a variety of poses. " (Id., at 20.)
	"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:
	 The mathematical representations of a user's face calculated during enrollment " (Id., at 23.)
10d3. populate the database according to the instruction, wherein the	The Accused Instrumentalities include a transmitter sub-system controller configured to populate the database according to the instruction.
controlled item is one of: a locking mechanism of a physical access structure	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":
or an electronic lock on an electronic computing device.	"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:
	•
	• Adding or removing a Touch ID fingerprint or Face ID face". (Ex. A, Apple Platform Security, at 16.)
	"During enrollment, the Secure Enclave processes, encrypts, and stores the corresponding Touch ID and Face ID template data." (Id., at 19.)

Claim 10	Accused Instrumentalities
	Touch ID
	"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" (Id.)
	Face ID
	The following Face ID data is saved, encrypted only for use by the Secure Enclave, during normal operation:
	 The mathematical representations of a user's face calculated during enrollment". (Id., at 23.)
	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.
	"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/)



Claim 10	Accused Instrumentalities
	1 2 3 4 5 6 7 8 9 V 0 0
	(https://www.apple.com/shop/product/HPAR2ZM/A/yale-assure-lock-sl-touchscreen-deadbolt-black

Claim 11	Accused Instrumentalities
11. A method for providing secure access to a controlled item in a	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.
system comprising a database of biometric signatures, a transmitter sub-system comprising a biometric sensor	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.
configured to receive a biometric signal, and a transmitter configured to emit a secure access signal capable of granting access	"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."
to the controlled item, and a receiver sub-system comprising a receiver sub- system controller configured to receive the transmitted secure access	(https://us.yalehome.com/en/yale-news/blog/latest-blog-posts/introducing-biometric-verification-for- august-and-yale-locks1/)
signal, and provide conditional access to the controlled item dependent upon information in said secure access signal, the method comprising:	



Claim 11	Accused Instrumentalities
	1 2 3 4 5 6 7 8 9 V 0 0
Ha. populating the database of biometric	(https://www.apple.com/shop/product/HPAR2ZM/A/yale-assure-lock-sl-touchscreen-deadbolt-black) The Accused Instrumentalities are configured to populate the database of biometric signatures as set forth in elements 11a1, 11a2, and 11a3 below.

Claim 11	Accused Instrumentalities
11a1. receiving a series of entries of the biometric signal;	The Accused Instrumentalities are configured to populate the database of biometric signatures by: receiving a series of entries of the biometric signal.
	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.
	"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.)
	Touch ID
	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.
	"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.)
	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.
	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.
	Set up Touch ID
	Before you can set up Touch ID, you must first create a <u>code</u> for your device,* then follow these steps: 1. Make sure the Touch ID sensor and your finger are clean and dry.

Claim 11	Accused Instrumentalities
	2. Tap Settings > Touch ID & Code, and then enter your code.
	Tap "Add fingerprint" and hold the device as you normally would when touching the Touch ID sensor.
	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. Place Your Finger Lit and test you freque on the terms button repeatedly.
	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.
	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."
	(https://support.apple.com/en-us/HT201371)

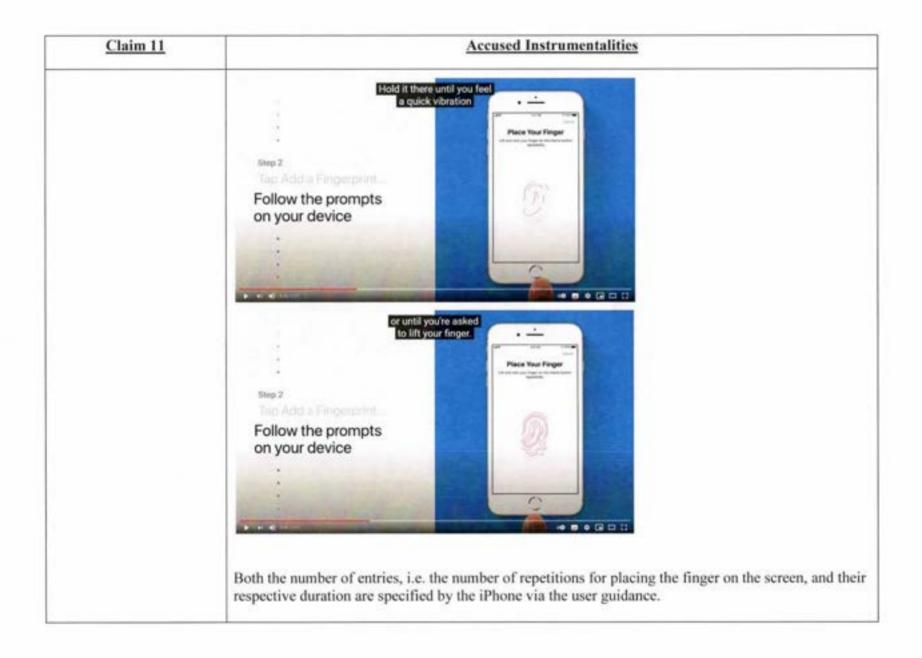
Claim 11	Accused Instrumentalities
N. 1. 2. 2. 2. 2. 2. 2. 2. 2. 2. 2. 2. 2. 2.	Accordingly, the user is prompted to place his finger on the sensor several times, in particular in accordance with step 5. Each time the finger is placed on the sensor, a corresponding biometric entry is generated, i.e. a series of such entries. All these entries, which result from placing the same finger on the sensor, form a series.
	Face ID
	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").
	"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 sequence of 2D images and depth maps, 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." (emphasis added) (Ex. A, Apple Platform Security, at 20.)
	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.
	Using Face ID on iPhone or iPad Pro - Apple Support

Claim 11	Accused Instrumentalities
	Configure Face ID
	Before configuring Face ID, make sure that neither the TrueDepth camera nor your face are covered by anything
	Follow the steps below to configure Face ID:
	1. Tap Settings > Face ID & Code. Enter your code when prompted.
	2. Tap on "Configure Face ID".
	3. Hold the device in portrait mode in front of your face and tap "Let's go".
	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".
	5. After performing the first Face ID scan, tap "Next".
	6. Again, slowly describe a circle with your head until it is completed.
	7. Tap "Done."
	(https://support.apple.com/en-us/HT208109)
	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).
	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 https://www.macworld.co.uk/how-to/second-face-id-3803421/, a second face is registered by the iPhone in the same way as the first face.

Claim 11	Accused Instrumentalities
	Cartiforn Face ID & Passcode
	Life (ACC III 1996)
	Phone Union Appli Passers NutoFill Other Api Passers out for ill Other Api Appli Contract of the service plants of sept. Set Up an Afternative Appearance In all things of the service out of sept. Set Up an Afternative Appearance In all things of the service out of sept. Set Up an Afternative Appearance Application to continuously learning lyon you state, fixing Up are restigence an all properties appearance. Actions to the service out of the sept.
	The series of entries of the biometric signal is identified on the iPhone by both the number and duration of each such entry. Touch ID According to step 5 of the instructions https://support.apple.com/en-us/HT201371, 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

Claim 11	Accused Instrumentalities
	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.
	Set up Touch ID
	 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.
	Place Your Finger Lift and rest your fringer on the Home button repeatedly.
	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.
	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.
	(https://support.apple.com/en-us/HT201371)

Claim 11	Accused Instrumentalities
	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:
	Place Your Finger Lift and rest your finger on the Home button repealedly
	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.
	This is shown in the Apple You Tube video (32) How to set up Touch ID on your iPhone or iPad - Apple Support - YouTube (https://www.youtube.com/watch?v=xTZ2LALWZlg):



Claim 11	Accused Instrumentalities
	Face ID 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. "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.)
	The sufficient duration of an entry for a pose, i.e. an angular position of the head specified via the use interface of the iPhone, is indicated to the user by the transformation of a gray line into a green line:
	Move your friend strong to complete the circle. Move your friend strong to complete the circle. Move your friend strong to complete the circle. First Face ID scan complete.

Claim 11	Accused Instrumentalities
11a2. determining at least one of the number of said entries and a duration of	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.
entries and a duration of each said entry;	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.
	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. (https://video.search.yahoo.com/yhs/search?fr=yhs-pty_pty_converter&hsimp=yhs-pty_converter&hspart=pty&p=registering+fingerprint+apple+touch+id+on+screen+instructions#id=1&vid=156de65ae06ca453643009fc0ea9cf79&action=click)
	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." (https://support.apple.com/en-au/HT201371)
	Touch ID: "you shouldn't tap too quickly or move your finger around" (https://support.apple.com/en-us/HT207537)
	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. (https://www.imore.com/how-set-face-id-iphone)

Claim 11	Accused Instrumentalities
11a3. mapping said series into an instruction; and	The Accused Instrumentalities include a transmitter sub-system controller configured to map said series into an instruction.
	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").
	"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.)
	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." (Id., at 10.)
	Touch ID
	The instruction here involves the processing of under-the-skin fingerprint characteristics and their encrypted storage.
	"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.)
	Face ID

Claim 11	Accused Instrumentalities
	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.
	"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.)
	"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: • The mathematical representations of a user's face calculated during enrollment
	•" (Id., at 23.)
11a4. populating the database according to the instruction;	The Accused Instrumentalities include a transmitter sub-system controller configured to populate the database according to the instruction.
mstruction,	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":
	"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:
	• • Adding or removing a Touch ID fingerprint or Face ID face". (Ex. A, Apple Platform Security, at 16.)

Claim 11	Accused Instrumentalities
	"During enrollment, the Secure Enclave processes, encrypts, and stores the corresponding Touch ID and Face ID template data." (Id., at 19.)
	Touch ID
	"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" (Id.)
	Face ID
	The following Face ID data is saved, encrypted only for use by the Secure Enclave, during normal operation:
	• The mathematical representations of a user's face calculated during enrollment". (<i>Id.</i> , at 23.)
11b. receiving the biometric signal;	The Accused Instrumentalities include a biometric sensor configured to receive the biometric signal.
bioinettie signat,	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.
	Touch ID
	"Apple devices with a Touch ID sensor can be unlocked using a fingerprint." (Ex. A, Apple Platform Security, at 19.)
	"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."

Claim 11	Accused Instrumentalities
	"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." (Id.)
	"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) Laser-cut sapphire cryst. Stainless steel detection ring Touch D sensor Tactile switch Biometric sensor 121
	"Where is the Touch ID sensor located?

Claim 11	Accused Instrumentalities
	The Touch ID sensor is located either in the home button or - on the iPad Air (4th generation) - in the top button.
	(https://support.apple.com/en-us/HT201371)
	The image sensor captures an 88-by-88-pixel, 500 PPI raster scan:
	"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.)
	Face ID
	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.)
	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.
	"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

Accused Instrumentalities
used to create a sequence of 2D images and depth maps, which are digitally signed and sent to 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 mathematical representation and compares that representation to the enrolled facial data. This enrifacial data is itself a mathematical representation of the user's face captured across a variety of potal, at 20.) The camera system includes a biometric image sensor, namely a "CMOS image" sensor from Sortina Compares that representation of the user's face captured across a variety of potal.
Structured light receiver Module How has Sharp CMOS any present of AMS CMOS any present First CMOS any present CMO
Active alignment Active algoriest equipment.

Claim 11	Accused Instrumentalities
11c. matching the biometric signal against members of the database	The Accused Instrumentalities include a transmitter controller configured to emit a secure access signal conveying information dependent upon said accessibility attribute.
of biometric signatures to thereby output an accessibility attribute;	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.
	"The Secure Enclave is a system on chip (SoC) that is included on all recent iPhone, devices" (Ex. A, Apple Platform Security, at 7.)
	"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). " (Id., at 19.)
	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.
	For Touch ID, the Secure Enclave match verification is performed as follows:
	"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.)
	"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.)

Claim 11	Accused Instrumentalities
	"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. " (https://support.apple.com/en-us/HT204587)
	"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." (https://support.apple.com/de-de/HT204587)
	For Face ID , the Secure Enclave has a neural network protected by it, i.e., a Secure Neural Engine, which is used to verify the match:
	"Face ID uses neural networks for determining attention, matching , and antispoofing, so a user can unlock their phone with a glance." (Ex. A, Apple Platform Security, at 20.)
	"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." (Id.).
	"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." (Id. at 23.)
	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

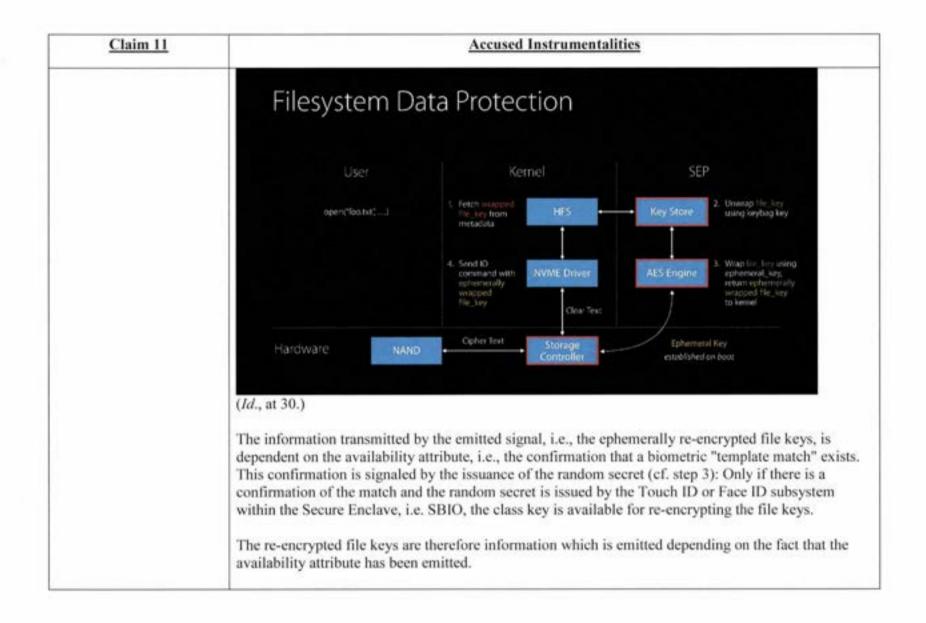
Claim 11	Accused Instrumentalities
	Touch ID or Face ID subsystem. This Touch ID or Face ID subsystem is also referred to as the SBIO. The accessibility attribute confirms that there is a match and that the iPhone is to be unlocked (" determine whether to unlock the device").
	This confirmation of the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

Claim 11	Accused Instrumentalities
	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."
	(Id. at 86.)
	The Touch ID or Face ID subsystem within the Secure Enclave is the SBIO shown below. SBIO is a 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 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"):
	Userspace UserEventAgent SpringBoard SpringBoard Weblefughters Agence Weblefughters Agence to the Board State Stat
	XNU (Kernel) AppleKeyStore SEP endpoint in SES SEP endpoint to SES
	Touch ID Sensor blo memory
	SEP minter key
	SKS memory SKS keyring SKS keyring
	SKS memory SKS keyring

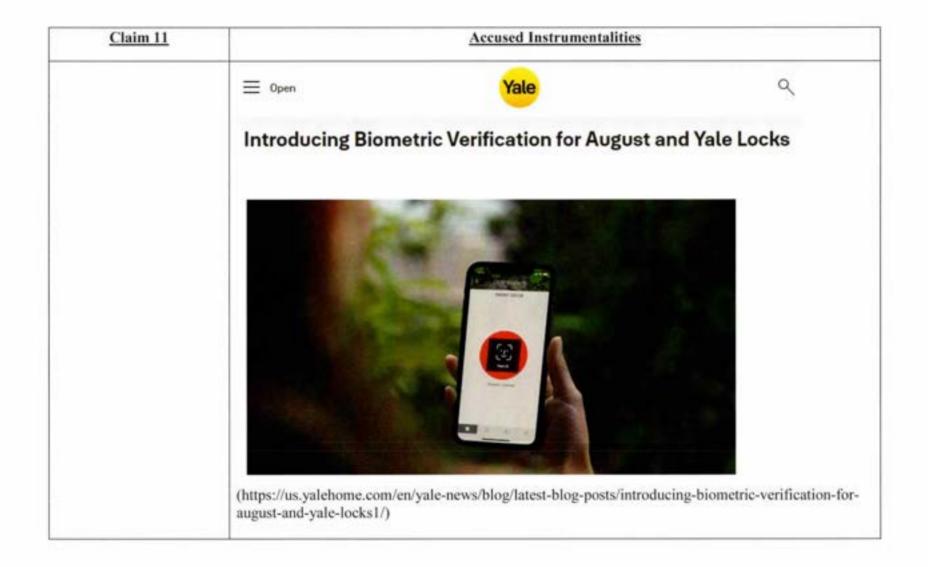
Claim 11	Accused Instrumentalities
	The class keys are encrypted with a master key:
	User Keybags
	Background
	Sets of keys generated for each user to protect their data at rest
	Keys wrapped by master key derived from user passcode and SEP UID
	After 10 incorrect passcode entries, SEP will not process any further attempts
	Different policy associated with each keybag key—Usage, availability
	(Id., at 25.)
	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.
11d. emitting a secure access signal conveying information dependent upon said accessibility attribute; and	The Accused Instrumentalities include a transmitter configured to emit a secure access signal conveying information dependent upon said accessibility attribute. For example, the Secure Enclave emits a signal with ephemerally re-encrypted file keys:

<u>Claim 11</u>	Accused Instrumentalities
	"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.)
	"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." (Id. at 85.)
	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:
	"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." (Id.)

Claim 11	Accused Instrumentalities
	Filesystem Data Protection
	Overview
	File blocks are encrypted using AES-XTS with 128-bit keys
	Each file on the user partition is encrypted using a unique random key chosen by SE
	Raw file keys are never exposed to the AP
	 Wrapped with a key from the user keybag for long-term storage
	 Wrapped with an ephemeral key while in use, bound to boot session (Ex. B, Behind the Scenes with iOS Security, at 29.)



Claim 11	Accused Instrumentalities
11e. providing conditional access to the controlled item dependent upon said information, wherein the	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
controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing	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.
device.	"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/)



Claim 11	Accused Instrumentalities
	1 2 3 4 5 6 7 8 9 V 0 0
	(https://www.apple.com/shop/product/HPAR2ZM/A/yale-assure-lock-sl-touchscreen-deadbolt-black)

Claim 12	Accused Instrumentalities
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:	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.
12a. receiving a biometric signal; and	The Accused Instrumentalities include a biometric sensor configured to receive the biometric signal.
	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. Touch ID
	"Apple devices with a Touch ID sensor can be unlocked using a fingerprint." (Ex. A, Apple Platform Security, at 19.)
	"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.)
	"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."

Claim 12	Accused Instrumentalities
	(Id.)
	The biometric sensor for Touch ID is located below the home button:
	"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) Laser-cut sapphire cryst. Stainless steel detection trig
	Touch ID sensor Tactile switch
	Biometric sensor 121
	"Where is the Touch ID sensor located?
	The Touch ID sensor is located either in the home button or - on the iPad Air (4th generation) - in the top button.
	(https://support.apple.com/en-us/HT201371)

Claim 12	Accused Instrumentalities
	The image sensor captures an 88-by-88-pixel, 500 PPI raster scan: "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.)
	Face ID 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.)
	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.
	"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 sequence of 2D images and depth maps, 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

Claim 12	Accused Instrumentalities
	mathematical representation and compares that representation to the enrolled facial data. This enrolle facial data is itself a mathematical representation of the user's face captured across a variety of poses. (Id., at 20.) The camera system includes a biometric image sensor, namely a "CMOS image" sensor from Sony, to perform facial biometrics:
	Structured light - System Commission - Ambient light - Front camera - Structure light
	Module: Horizon Harry Caronic Page Frage Caronic Page Caronic
	(https://appleinsider.com/articles/17/09/09/inner-workings-of-apples-face-id-camera-detailed-in-report)
12b. enrolling the biometric signal as an administrator signature in response to the database of	The Accused instrumentalities are configured to enroll the biometric signal as an administrator signature in response to the database of biometric signatures being empty. 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

Claim 12	Accused Instrumentalities
biometric signatures being empty.	signature enrolled upon the initial set up of the iOS device will be required to add additional fingerprints or faces on the device.
	Set up Face ID or Touch ID and create a passcode
	On some devices, you can set up Face ID or Touch ID. 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."
	Next, set a six-digit passcode to help protect your data. You need a passcode to use features like Face ID, Touch ID, and Apple Pay. If you'd like a four-digit passcode, custom passcode, or no passcode, tap "Passcode Options."
	Face ID Phone can recognize the unique, three-dimensional features of your face to unique, automatically, use Apple Pay, make painthases, or subscribe to services from Apple. Create a Passcode Face ID provides convenient and secure access by recognizing your face. Occasionally your passcode will be required for validation. Passacide Options
	(https://support.apple.com/en-us/HT202033)

Claim 14	Accused Instrumentalities
14. A non-transitory computer readable storage medium storing a computer program comprising instructions, which when executed by processors causes the processors to:	The Accused Instrumentalities are non-transitory computer readable storage medium storing a computer program comprising instructions as set forth below.
14a. receive a series of entries of a biometric signal;	The Accused Instrumentalities include a transmitter sub-system controller configured to receive a series of entries of the biometric signal.
Signat,	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.
	"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.)
	Touch ID
1	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.
	"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." (Id.)
	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.

Claim 14	Accused Instrumentalities
	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.
	Set up Touch ID
	Before you can set up Touch ID, you must first create a <u>coxic</u> for your device,* then follow these steps: 13. Make sure the Touch ID sensor and your finger are clean and dry.
	 Tap Settings > Touch ID & Code, and then enter your code.
	Tap "Add fingerprint" and hold the device as you normally would when touching the Touch ID sensor.
	16. Touch the Touch ID sensor with one finger, but do not press. Keep your finger on the button unti- you feel a quick vibration or are prompted to lift your finger. Place Your Finger Ut and rate mer frager on the turns Utter receaseds.

Claim 14	Accused Instrumentalities
	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.
	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."
	(https://support.apple.com/en-us/HT201371)
	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.
	Face ID
	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").
	"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 sequence of 2D images and depth maps, 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." (Ex. A, Apple Platform Security, at 20.)

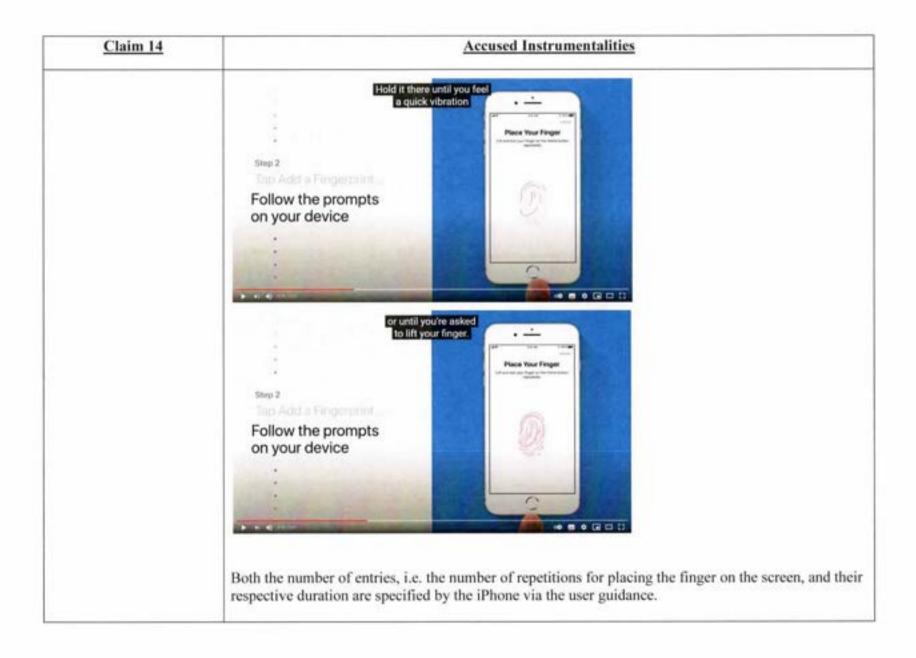
Claim 14	Accused Instrumentalities
	Each entry of the biometric signal thus contains a two-dimensional infrared image with 30,000 infrared points for capturing depth information. By continuously capturing such infrared images into a Face ID scan while the user moves his head into different poses, a series 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.
	Using Face ID on iPhone
	1. Tap Settings > Face ID & Code. Enter your code when prompted.
	2. Tap on "Configure Face ID".
	3. Hold the device in portrait mode in front of your face and tap "Let's go".
	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".
	5. After performing the first Face ID scan, tap "Next".
	6. Again, slowly describe a circle with your head until it is completed.
	7. Tap "Done."
	(https://support.apple.com/en-us/HT208109)
	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).
	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 https://www.macworld.co.uk/how-to/second-face-id-3803421/, a second face is registered by the iPhone in the same way as the first face.

Claim 14	Accused Instrumentalities
	< ∫ettinus Face ID & Passcode
	(2c)
	LUIZ FACS ID FOR.
	Phone Unlock
	(Tunger App Store
	Applia V
	Passwo utoFill (
	Other Agents 4 Agents
	Process part in the owners and the service of the s
	Set Up an Alternative Appearance
	In addition to combinately deserving from you have, Parce III ster recognise an alternative against level.
	Reset Face ©
	arrayatan
	Require Attention for Face ID
	The series of entries of the biometric signal is identified on the iPhone by both the number and duration of each such entry.
	Touch ID
	According to step 5 of the instructions https://support.apple.com/en-us/HT201371 , 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.

Claim 14	Accused Instrumentalities
	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.
	Set up Touch ID
	 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.
	Place Your Finger
	Lift and rest your finger on the Home butlion repeatedly.
	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.
	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.
	(https://support.apple.com/en-us/HT201371)

IPR2022-01094

Claim 14	Accused Instrumentalities
	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:
	Place Your Finger Lift and rest your linguer on the Home button repeatedly.
	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.
	This is shown in the Apple You Tube video (32) How to set up Touch ID on your iPhone or iPad - Apple Support - YouTube (https://www.youtube.com/watch?v=xTZ2LALWZlg):



Claim 14	Accused Instrumentalities
	Face ID 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. "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.) The sufficient duration of an entry for a pose, i.e. an angular position of the head specified via the use interface of the iPhone, is indicated to the user by the transformation of a gray line into a green line:
	Move your hand shorty to gargainte the simile. Move your hand shorty to gargainte the simile. Move your hand shorty to gargainte the simile.
14b. determine at least of a number of said entr	

<u>Claim 14</u>	Accused Instrumentalities
and a duration of each of said entries;	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.
	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.
	(https://video.search.yahoo.com/yhs/search?fr=yhs-pty-pty_ converter&hsimp=yhs- pty_converter&hspart=pty&p=registering+
	fingerprint+apple+touch+id+on+screen+instructions#id=1&vid=156de65ae06ca453643009fc0ea9cf79&action=click)
	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." (https://support.apple.com/en-au/HT201371)
	Touch ID: "you shouldn't tap too quickly or move your finger around" (https://support.apple.com/en-us/HT207537)
	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. (https://www.imore.com/how-set-face-id-iphone)
14c. map said series into an instruction;	The Accused Instrumentalities include a transmitter sub-system controller configured to map said series into an instruction.

Claim 14	Accused Instrumentalities
	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").
	"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.)
	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." (Id., at 10.)
	Touch ID
	The instruction here involves the processing of under-the-skin fingerprint characteristics and their encrypted storage.
	"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.)
	Face ID 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.

Claim 14	Accused Instrumentalities
	"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.)
	"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:
	• The mathematical representations of a user's face calculated during enrollment •" (Id., at 23.)
14d. populate a database of biometric signatures according to the	The Accused Instrumentalities include a transmitter sub-system controller configured to populate the database according to the instruction.
instruction;	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":
	"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:
	•
	• Adding or removing a Touch ID fingerprint or Face ID face". (Ex. A, Apple Platform Security, at 16.)
	"During enrollment, the Secure Enclave processes, encrypts, and stores the corresponding Touch ID and Face ID template data." (Id., at 19.)

Claim 14	Accused Instrumentalities
	Touch ID
	"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" (Id.)
	Face ID
	The following Face ID data is saved, encrypted only for use by the Secure Enclave, during normal operation:
	• The mathematical representations of a user's face calculated during enrollment". (<i>Id.</i> , at 23.)
14e. receive the biometric signal;	The Accused Instrumentalities include a biometric sensor configured to receive the biometric signal.
Signal,	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.
	Touch ID
	"Apple devices with a Touch ID sensor can be unlocked using a fingerprint." (Ex. A, Apple Platform Security, at 19.)
	"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.)
	"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."

Claim 14	Accused Instrumentalities
	(Id.)
	The biometric sensor for Touch ID is located below the home button:
	"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) Laser-out supphire crystal Stainless steel detection ring
	Touch ID sensor Tactile switch
	Biometric sensor 121
	"Where is the Touch ID sensor located?
	The Touch ID sensor is located either in the home button or - on the iPad Air (4th generation) - in the top button.
	(https://support.apple.com/en-us/HT201371)

Claim 14	Accused Instrumentalities
	The image sensor captures an 88-by-88-pixel, 500 PPI raster scan: "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.)
	Face ID 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.)
	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.
	"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 sequence of 2D images and depth maps, 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

	Accused Instrumentalities
	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. (Id., at 20.) The camera system includes a biometric image sensor, namely a "CMOS image" sensor from Sony, to perform facial biometrics:
	Structured light receiver Column Structured light receiver Column Structured Structur
	Active alignment Active alignment Ash Pacific
	(https://appleinsider.com/articles/17/09/09/inner-workings-of-apples-face-id-camera-detailed-in-report)
4f. match the biometric signal against members of the database of biometric signatures to thereby	The Accused Instrumentalities include a transmitter controller configured to emit a secure access signal conveying information dependent upon said accessibility attribute.

Claim 14	Accused Instrumentalities
output an accessibility attribute;	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.
	"The Secure Enclave is a system on chip (SoC) that is included on all recent iPhone, devices" (Ex. A, Apple Platform Security, at 7.)
	"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). " (Id., at 19.)
	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.
	For Touch ID, the Secure Enclave match verification is performed as follows:
	"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.)
	"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.)
	"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. " (https://support.apple.com/en-us/HT204587)

Claim 14	Accused Instrumentalities
	"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." (https://support.apple.com/de-de/HT204587)
	For Face ID , the Secure Enclave has a neural network protected by it, i.e., a Secure Neural Engine, which is used to verify the match:
	"Face ID uses neural networks for determining attention, matching , and antispoofing, so a user can unlock their phone with a glance." (Ex. A, Apple Platform Security, at 20.)
	"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>).
	"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." (Id. at 23.)
	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").

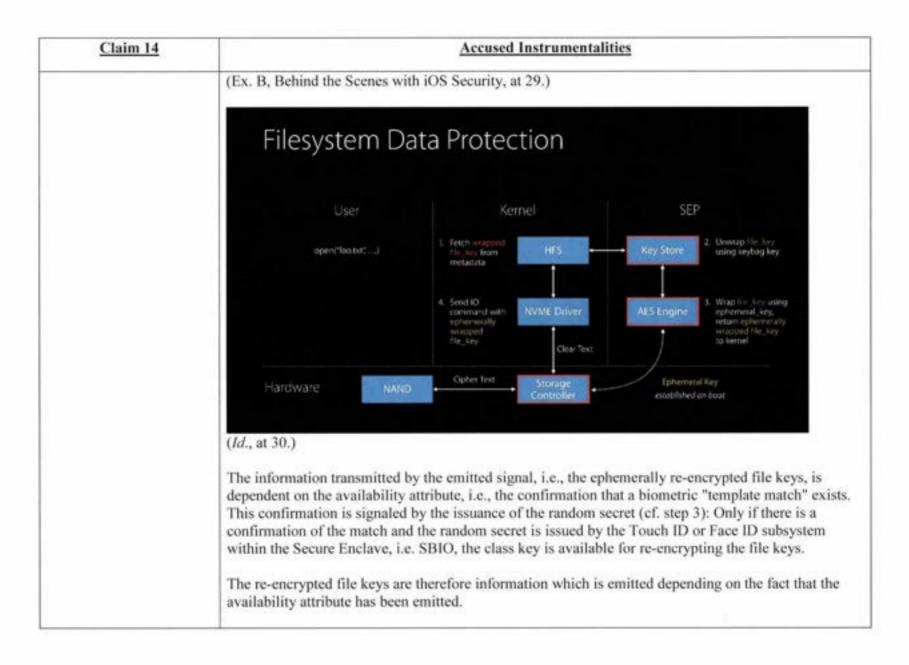
IPR2022-01094

Claim 14	Accused Instrumentalities
	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:
	"During matching, the Secure Enclave compares incoming data from the biometric sensor against the stored templates to determine whether to unlock the device []." (Id. at 19.)
	"Uses for Touch ID and Face ID
	Unlocking a device or user account
	[] keys for the highest class of Data Protection-which are held in the Secure Enclave [].
	With Touch ID or Face ID enabled, the keys aren't discarded when the device or account locks; instead, they're wrapped with a key that's given to the Touch ID or Face ID subsystem inside the Secure Enclave. When 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. This process provides additional protection by requiring cooperation between the Data Protection and Touch ID or Face ID subsystems to unlock the device."
	(Id. at 24.)
	"The class key is protected with the hardware UID and, for some classes, the user's passcode." (Id. at 85.)
	"Complete Protection
	(NSFileProtectionComplete): 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, 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."
	(<i>Id.</i> at 86.)

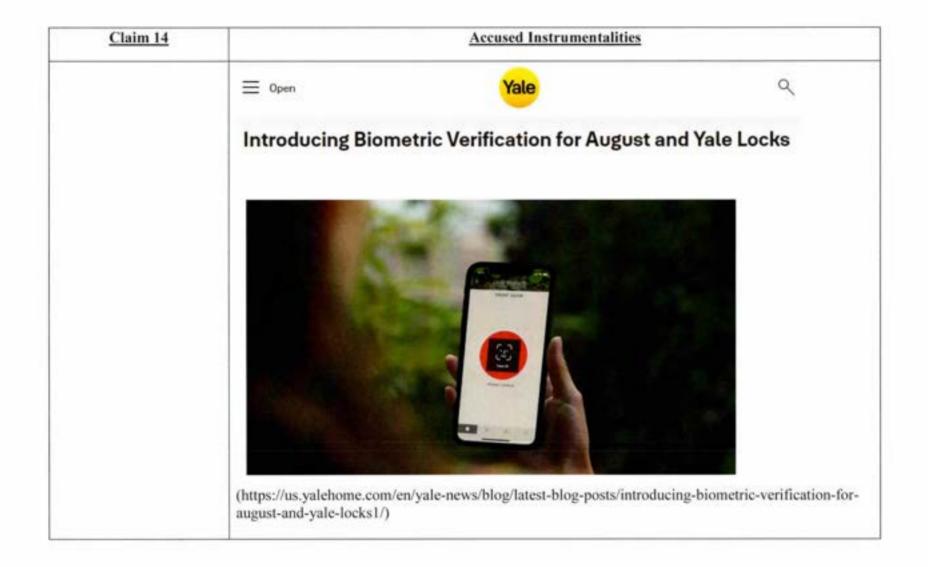
Claim 14	Accused Instrumentalities
	The Touch ID or Face ID subsystem within the Secure Enclave is the SBIO shown below. SBIO is an application that runs within the Secure Enclave on the SEP and is responsible for checking the match of biometric features. SBIO receives the corresponding biometric data from a biometric sensor, such a 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"):
	Userspace UserEventAgent SpringBoard N unguring home button some Brook Kingboard Short SpringBoard Spr
	XNU (Kernel) AppleKeyStore AppleMesa SIF analyses to SIES
	SEP SKS SBIO Touch ID Sensor
	SKS memory SKS keyring Close A Close
	Touch ID unlock
	(Ex. B, Behind the Scenes with iOS Security, at 34.) The class keys are encrypted with a master key:

Claim 14	Accused Instrumentalities
	User Keybags
	User Keybags Background
	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
	(Id., at 25.)
	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.
14g. emit a secure access signal conveying information dependent upon said accessibility attribute; and	The Accused Instrumentalities include a transmitter configured to emit a secure access signal conveying information dependent upon said accessibility attribute.
	For example, the Secure Enclave emits a signal with ephemerally re-encrypted file keys:
	"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."

Claim 14	Accused Instrumentalities
	(Ex. A, Apple Platform Security, at 14.)
	"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." (Id. at 85.)
	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:
	"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." (Id.)
	Filesystem Data Protection
	Overview
	File blocks are encrypted using AES-XTS with 128-bit keys
	Each file on the user partition is encrypted using a unique random key chosen by SEI
	Raw file keys are never exposed to the AP
	Wrapped with a key from the user keybag for long-term storage
	Wrapped with an ephemeral key while in use, bound to boot session



Claim 14	Accused Instrumentalities
14h. provide conditional access to a controlled item dependent upon said information, wherein the	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.
controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing	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.
device.	"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/)



Claim 14	Accused Instrumentalities
	1 2 3 4 5 6 7 8 9 V 0 0
	(https://www.apple.com/shop/product/HPAR2ZM/A/yale-assure-lock-sl-touchscreen-deadbolt-black)

Claim 15	Accused Instrumentalities
15. A system for providing secure access to a controlled item, the system comprising:	The Accused Instrumentalities are non-transitory computer readable storage medium storing a computer program comprising instructions as set forth below.
15a. a memory comprising a database of biometric signatures;	The Accused Instrumentalities include a memory comprising a database of biometric signatures. More specifically, the iPhone allows multiple biometric signatures to be entered into a database on the iPhone: Touch ID The iPhone allows the registration of multiple fingerprints:

Claim 15	Accused Instrumentalities
	"Register up to five fingerprints."
	"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. " (https://support.apple.com/en-us/HT204587)
	"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." (https://support.apple.com/en-us/HT204587)
	Face ID The iPhone allows the registration of multiple faces:

Claim 15	Accused Instrumentalities
	Benverge den Kopf langsam im Arek, um ibn zu sichließen.
	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 https://support.apple.com/en-us/HT208109 in the second section "Configure Face ID", there also the figure shown above.
	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; https://www.macworld.co.uk/how-to/second-face-id-3803421/), a second face is registered by the iPhone in the same way as the first face.
	"Set up Face ID or add another face. • Select "Settings" > "Face ID & Code" > "Configure alternate appearance" if you want to configure another face to be recognized by Face ID."

Claim 15	Accused Instrumentalities
	(https://support.apple.com/de-de/guide/iphone/iph6d162927a/ios)
	< <u>Continue</u> Face ID & Pesscode
	(a) (b) (c) (c) (c) (c) (c) (c) (c) (c) (c) (c
	iPhone Unlock
	iTunges App Stone
	Passws world
	Other Act A Appro A
	Process can in the State of St
	Set Up an Alternative Appnierance
	In addition to continuously learning free, you tree, free. C) can recognise an alternative against even.
	Reset Face (C)
	all transcores
	Require Attention for Face ID
	The page How To Add A Second Face To Face ID - Macworld UK (https://www.macworld.co.uk/how-to/second-face-id-3803421/) literally states:
	"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.

Claim 15	Accused Instrumentalities
	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."
	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:
	"The Secure Enclave is a system on chip (SoC) that is included on all recent iPhone, devices" (Ex. A, Apple Platform Security, at 7.)
	"The Secure Enclave is a dedicated secure subsystem integrated into Apple systems on chip (SoCs)." (<i>Id.</i> , at 9.)
	The Secure Enclave Processor provides the main computing power for the Secure Enclave." (<i>Id.</i> , at 10.)
	"During enrollment, the Secure Enclave processes, encrypts, and stores the corresponding Touch ID and Face ID template data." (<i>Id.</i> , at 19.)
	The Secure Enclave has access to a memory assigned to it and accessible only to it:
	Secure nonvolatile storage "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." (Id., at 15.)
	This memory serves as a database for storing the biometric signatures:

Claim 15	Accused Instrumentalities
	"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:
	 Adding or removing a Touch ID fingerprint or Face ID face".
	(Id., at 16.)
	This database is shown in the figure from Apple Platform Secutiry reproduced below:

Claim 15	Accused Instrumentalities
	NANO flash storage CRAM
	Namery controller NAND Static controller Application Processor ALS engine
	Secure Entitive AEE Engine Secure Entitive Proposition Engine
	Secure Nonvolatile Shirage The Secure Enclare companients.
	Database 105 (Ex. A, Apple Platform Security, at 9.)
5b. a transmitter sub- system comprising:	As set forth in elements 15b1, 15b2, and 15b3 below, the Accused Instrumentalities include a transmitter subsystem
15b1. a biometric sensor capable of receiving a biometric signal;	The Accused Instrumentalities include a biometric sensor configured to receive a biometric signal.

Claim 15	Accused Instrumentalities
	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.
	Touch ID
	"Apple devices with a Touch ID sensor can be unlocked using a fingerprint." (Ex. A, Apple Platform Security, at 19.)
	"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.)
	"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." (Id.)
	The biometric sensor for Touch ID is located below the home button:
	"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)

Claim 15	Accused Instrumentalities
	Laser-cut sapphire crystal Stainless steel detection ring Touch ID sensor Tactile-switch
	Biometric sensor 121
	"Where is the Touch ID sensor located?
	The Touch ID sensor is located either in the home button or - on the iPad Air (4th generation) - in the top button.
	(https://support.apple.com/en-us/HT201371)
	The image sensor captures an 88-by-88-pixel, 500 PPI raster scan:
	"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."

Claim 15	Accused Instrumentalities
	(Ex. C, iOS Security white paper, at 8.)
	Face ID
	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.)
	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.
	"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 sequence of 2D images and depth maps, 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." (Id.)
	The camera system includes a biometric image sensor, namely a "CMOS image" sensor from Sony, to perform facial biometrics:

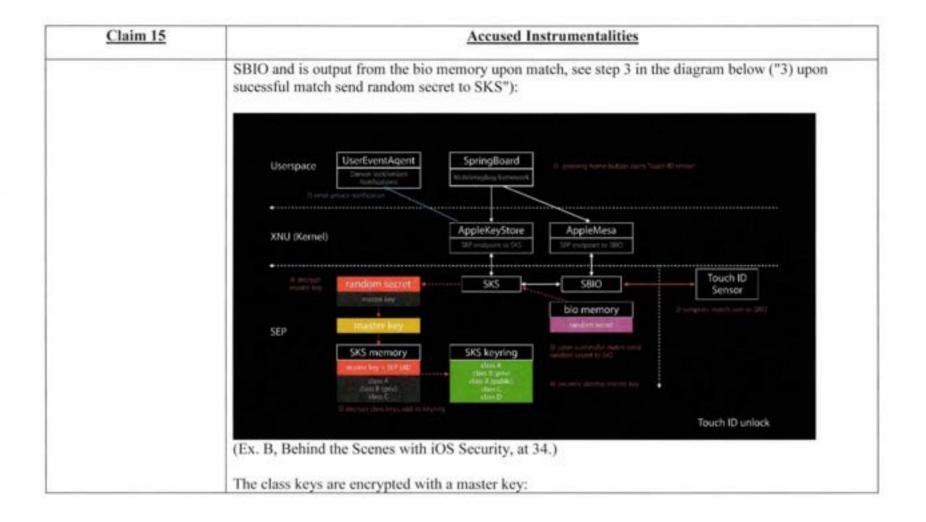
Claim 15	Accused Instrumentalities		
	Structured light received Moore Hon-hall, Sharp Child spearuserms (J. MPS) STM Child spearuserms (J. MPS) State Up and State		
	Active alignment Active asymmetric asymmetric ASM Pacific		
	(https://appleinsider.com/articles/17/09/09/inner-workings-of-apples-face-id-camera-detailed-in-report)		
15b2. a transmitter sub- system controller capable of matching the biometric	The Accused Instrumentalities include a transmitter controller configured to emit a secure access signal conveying information dependent upon said accessibility attribute.		
signal against members of the database of biometric signatures to thereby output an accessibility	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.		
attribute; and	"The Secure Enclave is a system on chip (SoC) that is included on all recent iPhone, devices" (Ex. A, Apple Platform Security, at 7.)		

Claim 15	Accused Instrumentalities
	"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). " (Id., at 19.)
	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.
	For Touch ID, the Secure Enclave match verification is performed as follows:
	"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.)
	"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.)
	"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. " (https://support.apple.com/en-us/HT204587)
	"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." (https://support.apple.com/de-de/HT204587)

Claim 15	Accused Instrumentalities
	For Face ID , the Secure Enclave has a neural network protected by it, i.e., a Secure Neural Engine, which is used to verify the match:
	"Face ID uses neural networks for determining attention, matching , and antispoofing, so a user can unlock their phone with a glance." (Ex. A, Apple Platform Security, at 20.)
	"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>).
	"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." (Id. at 23.)
	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").
	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:
	"During matching, the Secure Enclave compares incoming data from the biometric sensor against the stored templates to determine whether to unlock the device []." (Id. at 19.)

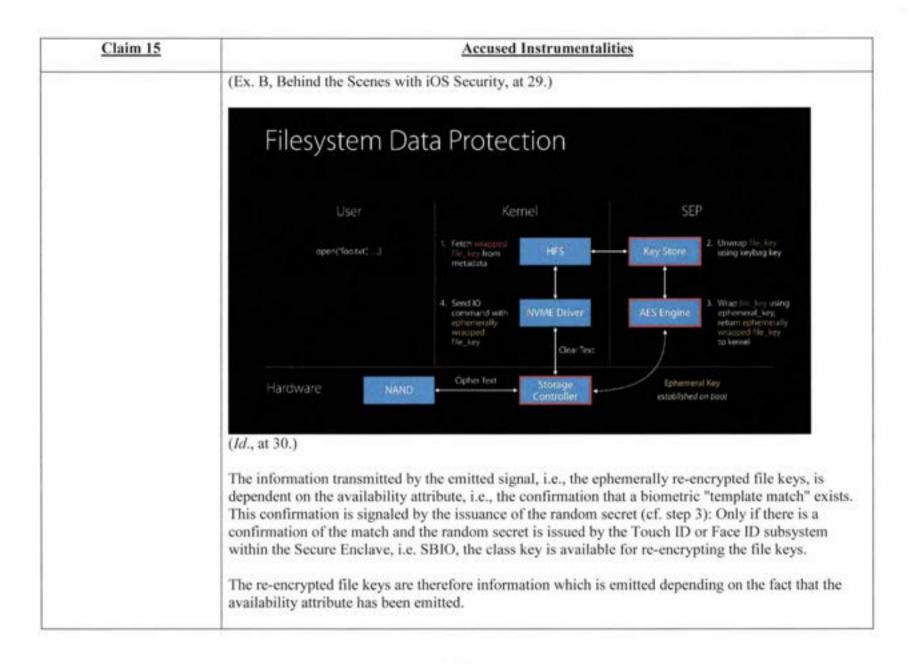
IPR2022-01094

Claim 15	Accused Instrumentalities
	"Uses for Touch ID and Face ID
	Unlocking a device or user account
	[] keys for the highest class of Data Protection-which are held in the Secure Enclave [].
	With Touch ID or Face ID enabled, the keys aren't discarded when the device or account locks; instead, they're wrapped with a key that's given to the Touch ID or Face ID subsystem inside the Secure Enclave. When 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. This process provides additional protection by requiring cooperation between the Data Protection and Touch ID or Face ID subsystems to unlock the device."
	(Id. at 24.)
	"The class key is protected with the hardware UID and, for some classes, the user's passcode." (Id. at 85.)
	"Complete Protection
	(NSFileProtectionComplete): 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, 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."
	(Id. at 86.)
	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



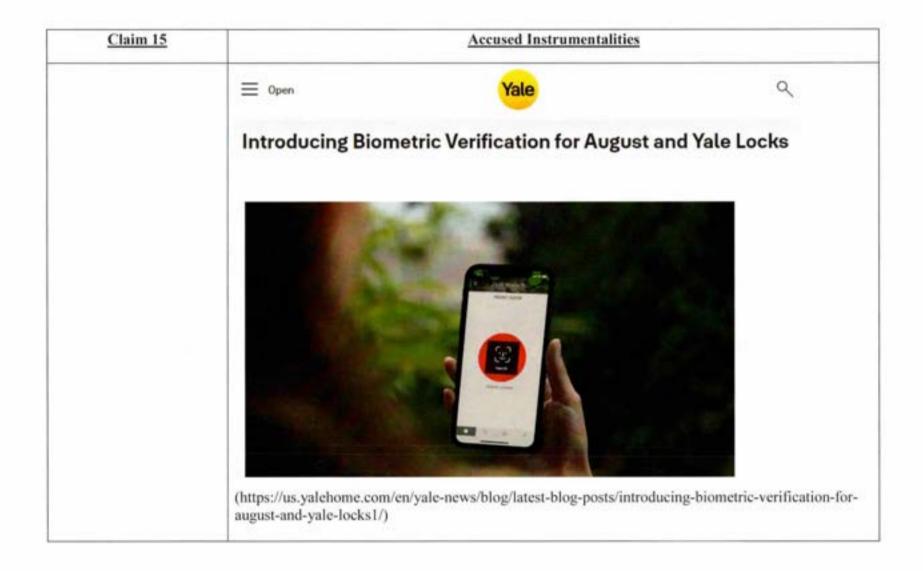
Claim 15	Accused Instrumentalities
	User Keybags
	Background
	Sets of keys generated for each user to protect their data at rest
	Keys wrapped by master key derived from user passcode and SEP UID
	After 10 incorrect passcode entries, SEP will not process any further attempts
	Different policy associated with each keybag key—Usage, availability
	(Id., at 25.)
	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.
15b3. a transmitter capable of emitting a secure access signal	The Accused Instrumentalities include a transmitter configured to emit a secure access signal conveying information dependent upon said accessibility attribute.
conveying information dependent upon said accessibility attribute; and	For example, the Secure Enclave emits a signal with ephemerally re-encrypted file keys:
	"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."

Claim 15	Accused Instrumentalities
	(Ex. A, Apple Platform Security, at 14.)
	"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." (Id. at 85.)
	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:
	"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." (Id.)
	Filesystem Data Protection
	Overview
	File blocks are encrypted using AES-XTS with 128-bit keys
	Each file on the user partition is encrypted using a unique random key chosen by SEP
	Raw file keys are never exposed to the AP
	 Wrapped with a key from the user keybag for long-term storage
	 Wrapped with an ephemeral key while in use, bound to boot session



Claim 15	Accused Instrumentalities				
15c. a receiver sub-system comprising:	As set forth in elements 15c1 and 15c2 below, the Accused Instrumentalities include a receiver suit system.			es include a receiver sub-	
15c1. a receiver sub- system controller capable of: receiving the transmitted secure access signal; and	The Accused Instrumentalitic transmitted secure access signal An application processor (118 file key. To read files from the signal by creating a read come ephemerally wrapped file_key with AES engine). This read to read and decrypt the encryption of the encryptio	nal. 8) with file system e NAND Flash sto mand with the eph y") and sends it to command provides pted file from the 1	driver, which rage, the appli emerally wrap the storage con the storage con NAND flash storage	receives the ep cation process ped file key (" ntroller (109) (ontroller with a	ohemerally re-encrypted or processes the received IO command with NAND Flash controller
	User	Ken	nel	SEP	
	apen("foo.txt";)	I. Fetch waspend his key from metaclata	HFS	Key Store	Uniwrap file, key using seybag key
		Send IO command with ephermously wrapped file_lary	NVME Driver	AES Engine	What he key using ephemeral_key, return ephemerally visaged file_key to kernel
	Hardware NANO	- Cipher Text	Storage Controller	Ephemeni essablished	

Claim 15	Accused Instrumentalities
	"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.) "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."
15c2. providing conditional access to the controlled item dependent upon said information;	The Accused Instrumentalities include a receiver sub-system configured to provide conditional access to the controlled item dependent upon said information. 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.
	"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/)



Claim 15	Accused Instrumentalities
	1 2 3 4 5 6 7 8 9 V 0 0
	(https://www.apple.com/shop/product/HPAR2ZM/A/yale-assure-lock-sl-touchscreen-deadbolt-black)
15d. wherein the transmitter sub-system controller is further capable of:	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.

Claim 15	Accused Instrumentalities
15d1. receiving a series of entries of the biometric signal, said series being characterised according to	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.
at least one of the number of said entries and a duration of each said	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.
duration of each said entry;	"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.)
	Touch ID
	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.
	"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." (Id.)
	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.
	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.
	Set up Touch ID
	Before you can set up Touch ID, you must first create a code for your device,* then follow these steps:

Claim 15	Accused Instrumentalities
	19. Make sure the Touch ID sensor and your finger are clean and dry.
	20. Tap Settings > Touch ID & Code, and then enter your code.
	 Tap "Add fingerprint" and hold the device as you normally would when touching the Touch ID sensor.
	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. Place Your Finger Lift and rest your froger on the Horse Dutton recentedly.
	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.
	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."
	(https://support.apple.com/en-us/HT201371)

Claim 15	Accused Instrumentalities
	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.
	Face ID
	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").
	"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 sequence of 2D images and depth maps, 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." (Ex. A, Apple Platform Security, at 20.)
	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.
	Using Face ID on iPhone
	1. Tap Settings > Face ID & Code. Enter your code when prompted.
	2. Tap on "Configure Face ID".

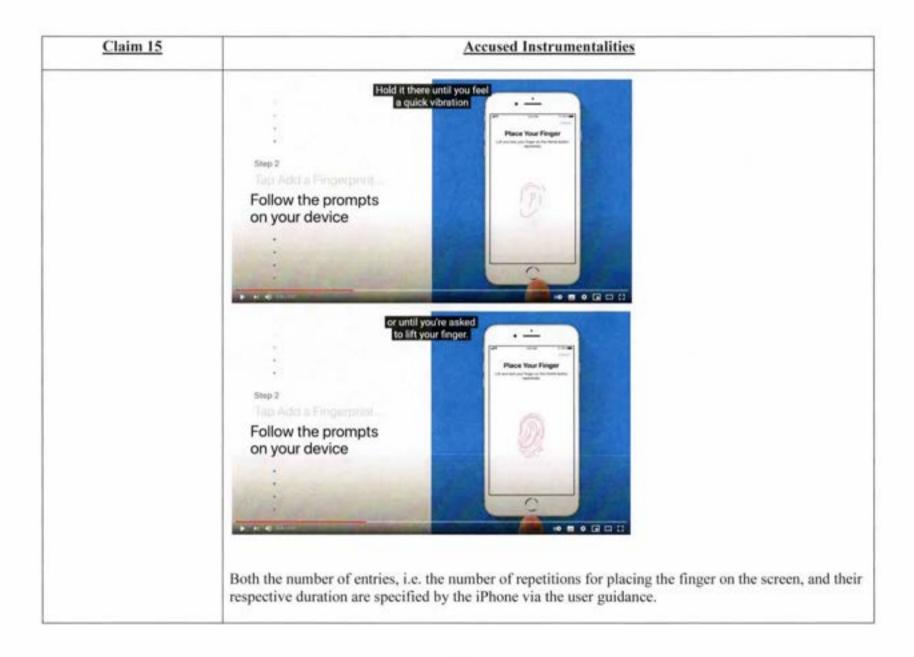
IPR2022-01094

Claim 15	Accused Instrumentalities
	3. Hold the device in portrait mode in front of your face and tap "Let's go".
	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".
	5. After performing the first Face ID scan, tap "Next".
	6. Again, slowly describe a circle with your head until it is completed.
	7. Tap "Done."
	(https://support.apple.com/en-us/HT208109)
	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).
	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 https://www.macworld.co.uk/how-to/second-face-id-3803421/, a second face is registered by the iPhone in the same way as the first face.

Claim 15	Accused Instrumentalities
	< Setting: Face ID & Passcode (2)
	UNIX FACE ID FOR
	Phone Unlock
	Ture App Store
	Appli
	Parowo MoFili
	Other Add 4 Approx 1 Others call of the limited defined defin
	Set Up an Alternative Appearance
	to admitted to communically learning from you had, Faces © can recognize an after other approximation
	Perset Faces (C)
	armetical
	Require Attention for Face ID
	The series of entries of the biometric signal is identified on the iPhone by both the number and duration of each such entry.
	Touch ID
	According to step 5 of the instructions https://support.apple.com/en-us/HT201371 , for the enrollment of a single finger, the user has to repeatedly place the respective finger on the sensor and thus a numb 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 finger must remain on the sensor for a predetermined duration for each entry of the biometric signal is order to capture the biometric signal during this time.

Claim 15	Accused Instrumentalities
	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.
	Set up Touch ID
	 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.
	Place Your Finger
<u>.</u>	Lift and rest your finger on the Home button repeatedly.
	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.
	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.
	(https://support.apple.com/en-us/HT201371)

Claim 15	Accused Instrumentalities
	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: Place Your Finger Ut and rest your frequence on the stone botton repeatedly.
	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. This is shown in the Apple You Tube video (32) How to set up Touch ID on your iPhone or iPad - Apple Support - YouTube (https://www.youtube.com/watch?v=xTZ2LALWZlg):

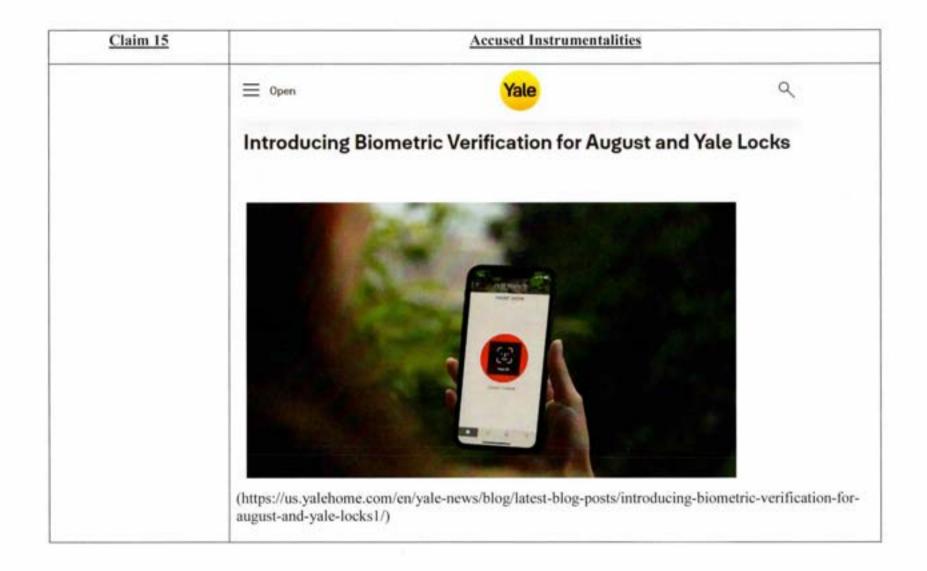


Claim 15	Accused Instrumentalities
	Face ID The user moves his face in front of the camera to strike different poses, and the camera system with image sensor continuously captures a large number of biometric entries, i.e. here the 2D images with depth information, in a row.
	"This enrolled facial data is itself a mathematical representation of the user's face captured across a variety of poses." (Ex. A, Apple Platform Security, at 20.)
	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:
	Mover your head slowly to gorgiste the circle. Mover your head slowly to gorgiste the circle. House your head slowly to gorgiste the circle.
5d2. mapping said serie	(Individual images taken from: https://support.apple.com/en-us/HT208109) S The Accused Instrumentalities include a transmitter sub-system controller configured to map said series into an instruction.

Claim 15	Accused Instrumentalities
	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").
	"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.)
	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." (Id., at 10.)
	Touch ID
	The instruction here involves the processing of under-the-skin fingerprint characteristics and their encrypted storage.
	"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.)
	Face ID 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.

Claim 15	Accused Instrumentalities
	"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.)
	"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:
	• The mathematical representations of a user's face calculated during enrollment •" (Id., at 23.)
15d3. populating the data base according to the instruction,	The Accused Instrumentalities include a transmitter sub-system controller configured to populate the database according to the instruction.
industrial,	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":
	"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: •
	 Adding or removing a Touch ID fingerprint or Face ID face". (Ex. A, Apple Platform Security, at 16.)
	"During enrollment, the Secure Enclave processes, encrypts, and stores the corresponding Touch ID and Face ID template data." (Id., at 19.)

Claim 15	Accused Instrumentalities
	"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" (Id.) Face ID The following Face ID data is saved, encrypted only for use by the Secure Enclave, during normal operation: • The mathematical representations of a user's face calculated during enrollment".
wherein the controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing device.	(Id., at 23.) 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. 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.
	"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/)



Claim 15	Accused Instrumentalities
	7 8 9
	(https://www.apple.com/shop/product/HPAR2ZM/A/yale-assure-lock-sl-touchscreen-deadbolt-blades)

Claim 16	Accused Instrumentalities
16. A transmitter subsystem for operating in a system for providing secure access to a controlled item, wherein the transmitter sub-system comprises:	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.
16a. a biometric sensor capable of receiving a biometric signal;	The Accused Instrumentalities include a biometric sensor configured to receive a biometric signal. 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. Touch ID "Apple devices with a Touch ID sensor can be unlocked using a fingerprint." (Ex. A, Apple Platform Security, at 19.) "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.) "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." (Id.)
	The biometric sensor for Touch ID is located below the home button:

Claim 16	Accused Instrumentalities
	"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) Laser cut sapphire crystal Laser cut sapphire crystal lens. The surrounding stainless steel detection ring Touch ID sensor Tactile switch
	Biometric sensor 121
	"Where is the Touch ID sensor located?
	The Touch ID sensor is located either in the home button or - on the iPad Air (4th generation) - in the top button.
	(https://support.apple.com/en-us/HT201371)
	The image sensor captures an 88-by-88-pixel, 500 PPI raster scan:
	"The 88-by-88-pixel, 500-ppi raster scan is temporarily stored in encrypted memory within the Secur- Enclave while being vectorized for analysis, and then it's discarded. The analysis utilizes subdermal

Accused Instrumentalities
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.)
Face ID
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.)
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.
"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 sequence of 2D images and depth maps, 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." (Id.)

Claim 16	Accused Instrumentalities
	The camera system includes a biometric image sensor, namely a "CMOS image" sensor from Sony, perform facial biometrics:
	Structured right receiver. Module: Honorial, Sharp: Child Sensor and Sensor
16b. a controller capable	(https://appleinsider.com/articles/17/09/09/inner-workings-of-apples-face-id-camera-detailed-in-report) The Accused Instrumentalities include a transmitter controller configured to emit a secure access
of matching the biometric signal against members of a database of biometric signatures to thereby output an accessibility attribute; and	More specifically, the iPhone's System on Chip (SOC), i.e. the Secure Enclave with its Secure Encla Processor (SEP) or a Secure Neural Engine contained therein, is a means (103) to check a match of t biometric signal with elements of the biometric signature database.

Claim 16	Accused Instrumentalities
	"The Secure Enclave is a system on chip (SoC) that is included on all recent iPhone, devices" (Ex. A, Apple Platform Security, at 7.)
	"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). " (<i>Id.</i> , at 19.)
	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.
	For Touch ID, the Secure Enclave match verification is performed as follows:
	"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.)
	"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.)
	"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." (https://support.apple.com/en-us/HT204587)
	"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."

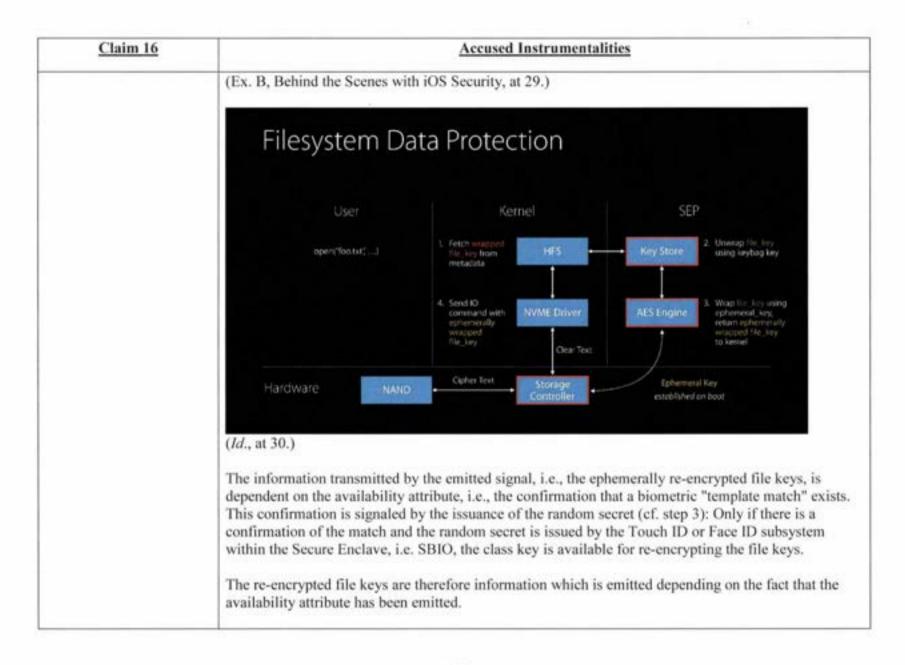
Claim 16	Accused Instrumentalities
	(https://support.apple.com/de-de/HT204587)
	For Face ID , the Secure Enclave has a neural network protected by it, i.e., a Secure Neural Engine, which is used to verify the match:
	"Face ID uses neural networks for determining attention, matching , and antispoofing, so a user can unlock their phone with a glance." (Ex. A, Apple Platform Security, at 20.)
	"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>).
	"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." (Id. at 23.)
	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").
	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:

Claim 16	Accused Instrumentalities
	"During matching, the Secure Enclave compares incoming data from the biometric sensor against the stored templates to determine whether to unlock the device []." (Id. at 19.)
	"Uses for Touch ID and Face ID
	Unlocking a device or user account
	[] keys for the highest class of Data Protection-which are held in the Secure Enclave [].
	With Touch ID or Face ID enabled, the keys aren't discarded when the device or account locks; instead, they're wrapped with a key that's given to the Touch ID or Face ID subsystem inside the Secure Enclave. When 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. This process provides additional protection by requiring cooperation between the Data Protection and Touch ID or Face ID subsystems to unlock the device."
	(Id. at 24.)
	"The class key is protected with the hardware UID and, for some classes, the user's passcode." (Id. at 85.)
	"Complete Protection
	(NSFileProtectionComplete): 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, 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."
	(<i>Id.</i> at 86.)
	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

Claim 16	Accused Instrumentalities
	of biometric features. SBIO receives the corresponding biometric data from a biometric sensor, such 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 sucessful match send random secret to SKS"):
	Userspace UserEventAgent SpringBoard Nobletsylang terrenoork
	XNU (Kernel) AppleKeyStore AppleMesa SR endpoint to SRS AppleMesa SR endpoint to SRS
	SKS S8IO Touch ID Sensor
	SKS memory SKS keyring
	(Ex. B, Behind the Scenes with iOS Security, at 34.)
	The class keys are encrypted with a master key:

Claim 16	Accused Instrumentalities
	User Keybags
	Background
	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
	(Id., at 25.)
	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.
16c. a transmitter capable of emitting a secure access signal conveying said	The Accused Instrumentalities include a transmitter configured to emit a secure access signal conveying information dependent upon said accessibility attribute.
information dependent upon said accessibility	For example, the Secure Enclave emits a signal with ephemerally re-encrypted file keys:
attribute;	"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."

Claim 16	Accused Instrumentalities
	(Ex. A, Apple Platform Security, at 14.)
	"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 wit the ephemeral key and sent back to the Application Processor." (Id. at 85.)
	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:
	"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 ar sent back to the Application Processor." (Id.)
	Filesystem Data Protection
	Overview
	File blocks are encrypted using AES-XTS with 128-bit keys
	Each file on the user partition is encrypted using a unique random key chosen by S
	Raw file keys are never exposed to the AP
	 Wrapped with a key from the user keybag for long-term storage
	· Wrapped with an ephemeral key while in use, bound to boot session



IPR2022-01094

Claim 16	Accused Instrumentalities
16d. wherein the controller is further capable of:	The Accused Instrumentalities include a controller that has capabilities as set forth in elements 16d1, 16d2, and 16d3 below.
16d1. receiving a series of entries of the biometric signal, said series being	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.
characterised according to at least one of the number of said entries and a duration of each said	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.
entry;	"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.)
	Touch ID
	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.
	"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." (Id.)
	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.
	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.

Claim 16	Accused Instrumentalities
	Set up Touch ID
	Before you can set up Touch ID, you must first create a <u>code</u> for your device,* then follow these steps: 25. Make sure the Touch ID sensor and your finger are clean and dry.
	26. Tap Settings > Touch ID & Code, and then enter your code.
	Tap "Add fingerprint" and hold the device as you normally would when touching the Touch ID sensor.
	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. Place Your Finger In and the part but the button until your finger.
	 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.

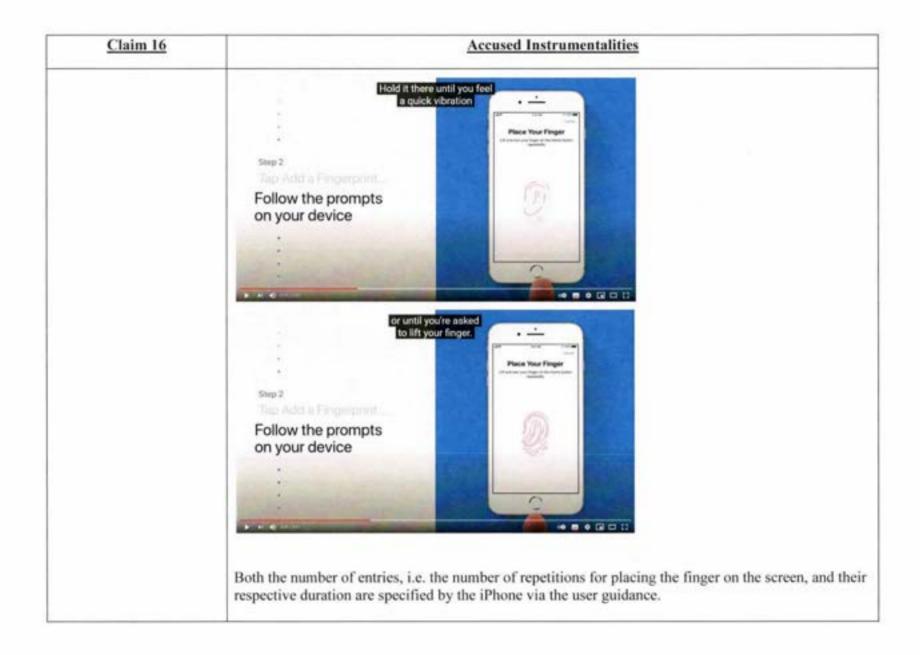
Claim 16	Accused Instrumentalities
	30. The next screen will ask you to change your finger position. Hold your device as you normally would when unlocking it. Touch the Touch ID sensor with the outer edges of your fingertip instead of the middle part as you would during the first scan."
	(https://support.apple.com/en-us/HT201371)
	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.
	Face ID
	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").
	"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 sequence of 2D images and depth maps, 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." (Ex. A, Apple Platform Security, at 20.)
	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

Claim 16	Accused Instrumentalities
	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.
	Using Face ID on iPhone
	1. Tap Settings > Face ID & Code. Enter your code when prompted.
	2. Tap on "Configure Face ID".
	3. Hold the device in portrait mode in front of your face and tap "Let's go".
	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".
	5. After performing the first Face ID scan, tap "Next".
	6. Again, slowly describe a circle with your head until it is completed.
	7. Tap "Done."
	(https://support.apple.com/en-us/HT208109)
	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).
	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 https://www.macworld.co.uk/how-to/second-face-id-3803421/, a second face is registered by the iPhone in the same way as the first face.

Claim 16	Accused Instrumentalities
	< Settom Face tO & Passcode (□)
	USB FINDS 20 POR
	Phone Unlock
	(Tunes App Store
	Aces
	Passed MoFill (C)
	Other Act 4 Acquir III
	Primary can be a fire unique. To reaction to experiment of the control of the con
	Set Up an Alternative Appearance
	In addition by continuously warring how you look, face. If can recognise an alternative appropriate.
	Reset Face ID
	ettiseton
	Require Attention for Face ID
	The series of entries of the biometric signal is identified on the iPhone by both the number and duration of each such entry.
	Touch ID
	According to step 5 of the instructions https://support.apple.com/en-us/HT201371, for the enrollment of a single finger, the user has to repeatedly place the respective finger on the sensor and thus a numb 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.

Claim 16	Accused Instrumentalities
	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.
	Set up Touch ID
	 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.
	AT 100 000
	Place Your Finger Ut and and your frage on the force before repeatedly.
	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.
	 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.
	(https://support.apple.com/en-us/HT201371)

<u>Claim 16</u>	Accused Instrumentalities
	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:
	Place Your Finger Lift and rest your finger on the Home button repeatedly.
	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.
	This is shown in the Apple You Tube video (32) How to set up Touch ID on your iPhone or iPad - Apple Support - YouTube (https://www.youtube.com/watch?v=xTZ2LALWZlg):

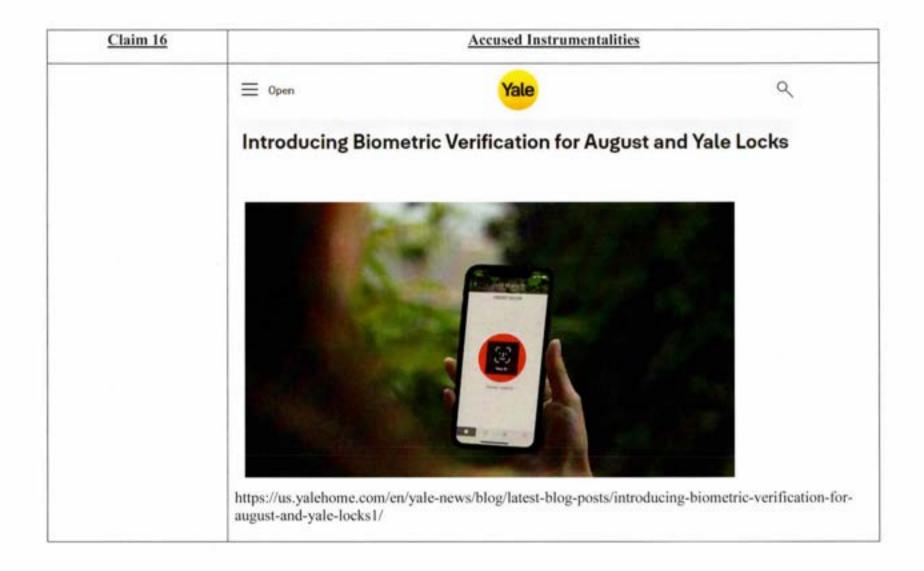


Claim 16	Accused Instrumentalities
	Face ID The user moves his face in front of the camera to strike different poses, and the camera system with image sensor continuously captures a large number of biometric entries, i.e. here the 2D images with depth information, in a row.
	"This enrolled facial data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

Claim 16	Accused Instrumentalities
	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").
	"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.)
	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." (Id., at 10.)
	Touch ID
	The instruction here involves the processing of under-the-skin fingerprint characteristics and their encrypted storage.
	"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.)
	Face ID 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.

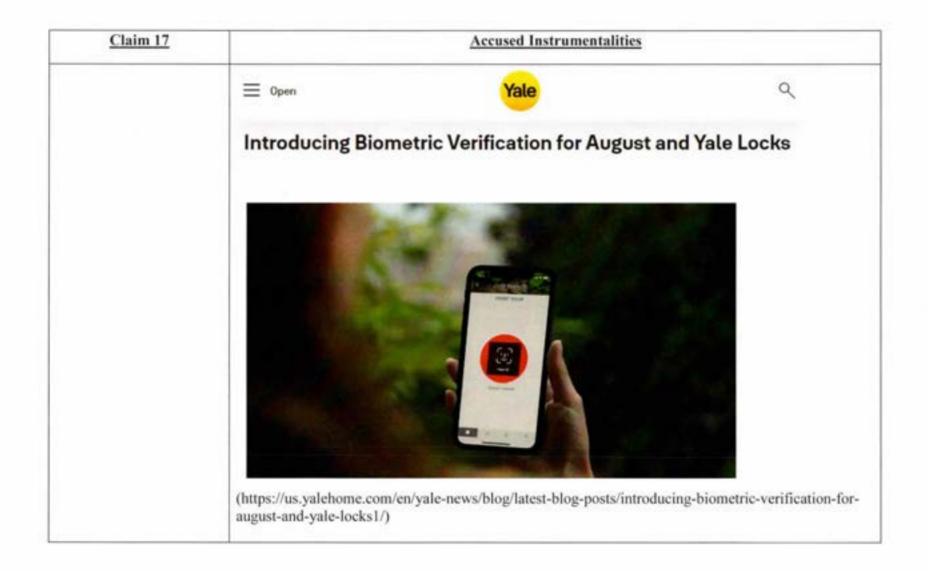
Claim 16	Accused Instrumentalities
	"A portion of the Secure Neural Engine-protected within the Secure Enclave-transforms this data into a mathematical representation and compares that representation to the enrolled facial data. This enrolled facial data is itself a mathematical representation of the user's face captured across a variety of poses. " (<i>Id.</i> , at 20.)
	"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:
	• The mathematical representations of a user's face calculated during enrollment •" (Id., at 23.)
16d3. populating the database according to the instruction,	The Accused Instrumentalities include a transmitter sub-system controller configured to populate the database according to the instruction.
	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":
	"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:
	•
	• Adding or removing a Touch ID fingerprint or Face ID face". (Ex. A, Apple Platform Security, at 16.)
	"During enrollment, the Secure Enclave processes, encrypts, and stores the corresponding Touch ID and Face ID template data." (Id., at 19.)

Claim 16	Accused Instrumentalities
	"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" (Id.) Face ID The following Face ID data is saved, encrypted only for use by the Secure Enclave, during normal operation: • The mathematical representations of a user's face calculated during enrollment".
wherein the controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing device.	(Id., at 23.) 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. 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.
	"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/



Claim 16	Accused Instrumentalities
	1 2 3 4 5 6 7 8 9 V 0 0
	https://www.apple.com/shop/product/HPAR2ZM/A/yale-assure-lock-sl-touchscreen-deadbolt-black

Claim 17	Accused Instrumentalities
Claim 17 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	Accused Instrumentalities 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. 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. "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/)



Claim 17	Accused Instrumentalities
	1 2 3 4 5 6 7 8 9 V 0 0
	(https://www.apple.com/shop/product/HPAR2ZM/A/yale-assure-lock-sl-touchscreen-deadbolt-black)
17a. populating the database of biometric signatures by:	The Accused Instrumentalities are configured to populate the database of biometric signatures as set forth in elements 17a1 to 17a4 below.

Claim 17	Accused Instrumentalities
17a1. receiving a series of entries of the biometric signal;	The Accused Instrumentalities are configured to populate the database of biometric signatures by: receiving a series of entries of the biometric signal.
Signal,	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.
	"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.)
	Touch ID
	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.
	"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.) 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.
	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; https://support.apple.com/en-us/HT201371
	literally described as follows:
	Set up Touch ID

Accused Instrumentalities
Before you can set up Touch ID, you must first create a code for your device,* then follow these steps: 1. Make sure the Touch ID sensor and your finger are clean and dry.
2. Tap Settings > Touch ID & Code, and then enter your code.
Tap "Add fingerprint" and hold the device as you normally would when touching the Touch ID sensor.
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. Place Your Finger Ut and rest your finger on the forms button respectedly.
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.
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."

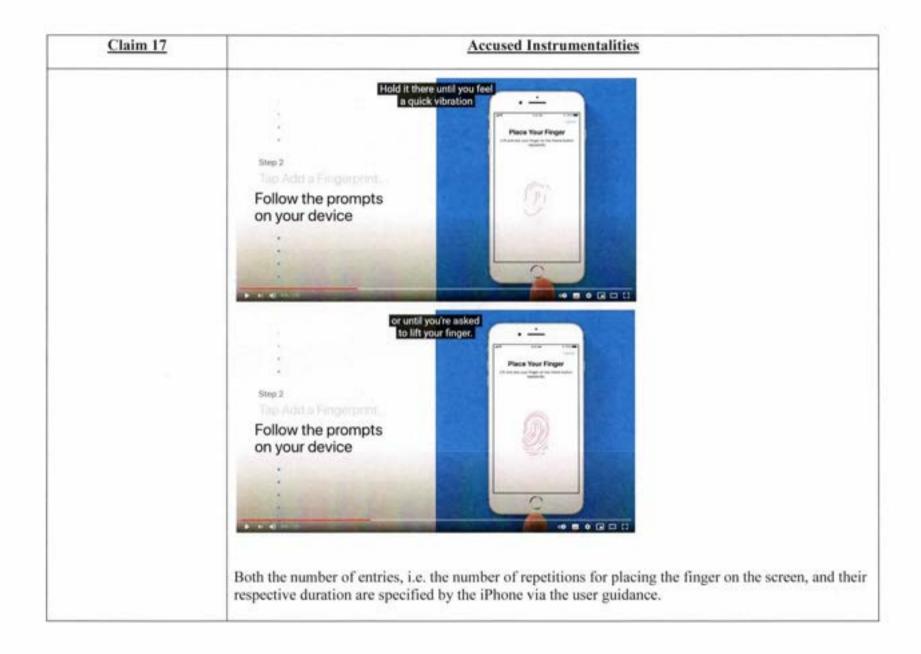
Claim 17	Accused Instrumentalities
	Accordingly, the user is prompted to place his finger on the sensor several times, in particular in accordance with step 5. Each time the finger is placed on the sensor, a corresponding biometric entry is generated, i.e. a series of such entries. All these entries, which result from placing the same finger on the sensor, form a series.
	Face ID
	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").
	"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 sequence of 2D images and depth maps, 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." (Ex. A, Apple Platform Security, at 20.)
	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.
	Under Using Face ID on iPhone or iPad Pro - Apple Support; https://support.apple.com/en-us/HT208109 , the creation of a set of entries is described as follows:

Claim 17	Accused Instrumentalities
	Configure Face ID
	Before configuring Face ID, make sure that neither the TrueDepth camera nor your face are covered by anything
	Follow the steps below to configure Face ID:
	1. Tap Settings > Face ID & Code. Enter your code when prompted.
	2. Tap on "Configure Face ID".
	3. Hold the device in portrait mode in front of your face and tap "Let's go".
	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".
	5. After performing the first Face ID scan, tap "Next".
	6. Again, slowly describe a circle with your head until it is completed.
	7. Tap "Done."
	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).
	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 https://www.macworld.co.uk/how-to/second-face-id-3803421/, a second face is registered by the iPhone in the same way as the first face.

Claim 17	Accused Instrumentalities
	Circlician Face ID & Passcode
	Phone Unlock
	Huser & App Stone Appl
	Other Api A Apics A Apics A Provincia of the Company, Three discovered for apics with pages of all apics and pages of the control of the
	Set Up an Alternative Appearance
	In addition to continuously instrume that you had, have all over management at other sold and the sold of the sold
	Reset Face C)
	ATTOMORY
	Require Attention for Face ID
	The series of entries of the biometric signal is identified on the iPhone by both the number and duration of each such entry.
	Touch ID
	According to step 5 of the instructions https://support.apple.com/en-us/HT201371, 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.

Claim 17	Accused Instrumentalities
	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 (https://support.apple.com/en-us/HT201371)
	literally described as follows:
	Set up Touch ID
	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.
	Place Your Finger Lift and rest your finges on the Home button repeatedly.
	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.
	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.

Claim 17	Accused Instrumentalities
	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:
	Place Your Finger Lift and rest your finger on the Horne button repeatedly.
	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.
	This is shown in the Apple You Tube video (32) How to set up Touch ID on your iPhone or iPad - Apple Support - YouTube (https://www.youtube.com/watch?v=xTZ2LALWZlg):



Claim 17	Accused Instrumentalities
	Face ID 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.
	"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.)
	The sufficient duration of an entry for a pose, i.e. an angular position of the head specified via the use interface of the iPhone, is indicated to the user by the transformation of a gray line into a green line:
	Move your head showly to somplete the sinste. Move your head showly to complete the circle. Move your head showly to complete the circle. Scorr complete.
	(Individual images taken from: https://support.apple.com/en-us/HT208109)

Claim 17	Accused Instrumentalities
17a2. determining at least one of the number of said	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.
entries and a duration of each said entry;	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.
	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. (https://video.search.yahoo.com/yhs/search?fr=yhs-pty-pty_ converter&hsimp=yhs-pty_converter&hspart=pty&p=registering+fingerprint+apple+touch+id+on+screen+instructions#id=1&vid=156de65ae06ca453643009fc0ea9cf79&action=click)
	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." (https://support.apple.com/en-au/HT201371)
	Touch ID: "you shouldn't tap too quickly or move your finger around" (https://support.apple.com/en-us/HT207537)
	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. (https://www.imore.com/how-set-face-id-iphone)

Claim 17	Accused Instrumentalities
17a3. mapping said series into an instruction; and	The Accused Instrumentalities include a transmitter sub-system controller configured to map said series into an instruction.
	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").
	"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.)
	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." (Id., at 10.)
	Touch ID
	The instruction here involves the processing of under-the-skin fingerprint characteristics and their encrypted storage.
	"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.)
	Face ID

Claim 17	Accused Instrumentalities
	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.
	"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.)
	"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: • The mathematical representations of a user's face calculated during enrollment
	•" (Id., at 23.)
17a4. populating the database according to the instruction;	The Accused Instrumentalities include a transmitter sub-system controller configured to populate the database according to the instruction.
msu detion,	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":
	"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:
	 Adding or removing a Touch ID fingerprint or Face ID face". (Ex. A, Apple Platform Security, at 16.)

Claim 17	Accused Instrumentalities
	"During enrollment, the Secure Enclave processes, encrypts, and stores the corresponding Touch ID and Face ID template data." (Id., at 19.)
	Touch ID
	"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" (Id.)
	Face ID
	The following Face ID data is saved, encrypted only for use by the Secure Enclave, during normal operation:
	• The mathematical representations of a user's face calculated during enrollment". (<i>Id.</i> , at 23.)
17b. receiving the biometric signal;	The Accused Instrumentalities are configured to receive the biometric signal.
,	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.
	Touch ID
	"Apple devices with a Touch ID sensor can be unlocked using a fingerprint." (Ex. A, Apple Platform Security, at 19.)
	"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."

Claim 17	Accused Instrumentalities
	"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." (Id.)
	The biometric sensor for Touch ID is located below the home button:
	"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) Laser-cut supphire cryst. Stainless steel detection ring Touch ID sensor
	Biometric sensor 121
	"Where is the Touch ID sensor located?

Claim 17	Accused Instrumentalities
	The Touch ID sensor is located either in the home button or - on the iPad Air (4th generation) - in the top button.
	(https://support.apple.com/en-us/HT201371)
	The image sensor captures an 88-by-88-pixel, 500 PPI raster scan:
	"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.)
	Face ID
	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.)
	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.
	"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

Accused Instrumentalities
used to create a sequence of 2D images and depth maps, which are digitally signed and sent to 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 mathematical representation and compares that representation to the enrolled facial data. This enrolled data is itself a mathematical representation of the user's face captured across a variety of post (Id., at 20.) The camera system includes a biometric image sensor, namely a "CMOS image" sensor from Song
Structured light receiver. Most light sensor. Most light light light light sensor. Most light light light light light sensor. Most light light light light light light light sensor. Most light lig
Active_alignment Active_alignment Active_alignment automost.
(https://appleinsider.com/articles/17/09/09/inner-workings-of-apples-face-id-camera-detailed-in-

Claim 17	Accused Instrumentalities
17c. matching the biometric signal against members of the database	The Accused Instrumentalities include a transmitter controller configured to emit a secure access signal conveying information dependent upon said accessibility attribute.
of biometric signatures to thereby output an accessibility attribute;	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.
	"The Secure Enclave is a system on chip (SoC) that is included on all recent iPhone, devices" (Ex. A, Apple Platform Security, at 7.)
	"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). " (<i>Id.</i> , at 19.)
	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.
	For Touch ID, the Secure Enclave match verification is performed as follows:
	"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.)
	"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.)

Claim 17	Accused Instrumentalities
	"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." (https://support.apple.com/en-us/HT204587)
	"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." (https://support.apple.com/de-de/HT204587)
	For Face ID , the Secure Enclave has a neural network protected by it, i.e., a Secure Neural Engine, which is used to verify the match:
	"Face ID uses neural networks for determining attention, matching , and antispoofing, so a user can unlock their phone with a glance." (Ex. A, Apple Platform Security, at 20.)
	"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>).
	"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." (Id. at 23.)
	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

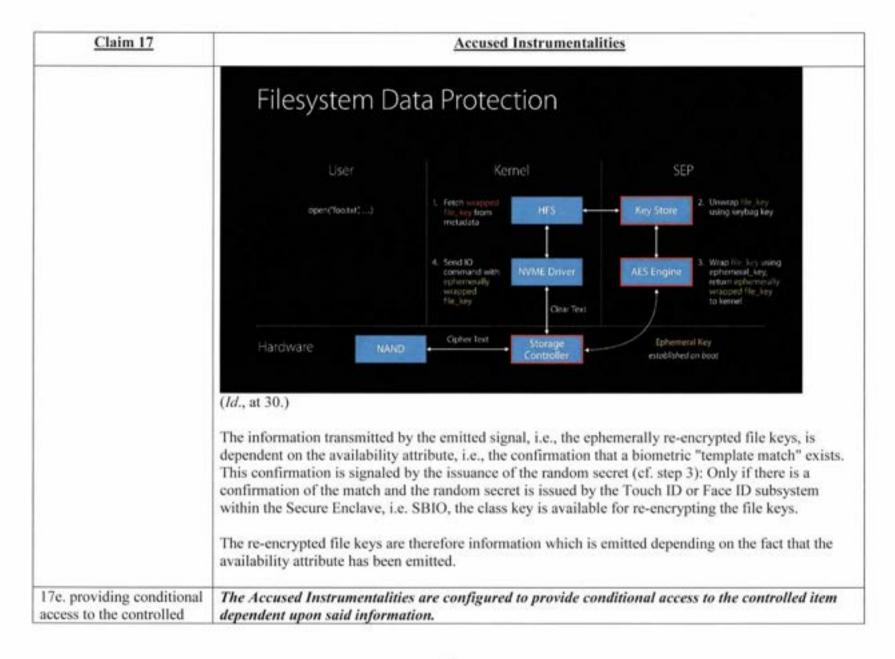
Claim 17	Accused Instrumentalities
	Touch ID or Face ID subsystem. This Touch ID or Face ID subsystem is also referred to as the SBIO. The accessibility attribute confirms that there is a match and that the iPhone is to be unlocked (" determine whether to unlock the device").
	This confirmation of the 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:
	"During matching, the Secure Enclave compares incoming data from the biometric sensor against the stored templates to determine whether to unlock the device []." (Id. at 19.)
	"Uses for Touch ID and Face ID
	Unlocking a device or user account
	[] keys for the highest class of Data Protection-which are held in the Secure Enclave [].
	With Touch ID or Face ID enabled, the keys aren't discarded when the device or account locks; instead, they're wrapped with a key that's given to the Touch ID or Face ID subsystem inside the Secure Enclave. When 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. 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.)
	"The class key is protected with the hardware UID and, for some classes, the user's passcode." (<i>Id.</i> at 85.)
	"Complete Protection
	(NSFileProtectionComplete): 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

Claim 17	Accused Instrumentalities
	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."
	(Id. at 86.)
	The Touch ID or Face ID subsystem within the Secure Enclave is the SBIO shown below. SBIO is a 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 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"):
	UserEventAgent Danner sock under SpringBoard Motivatory from National Spring Board Motivatory from National Spring Board
	XNU (Kernel) AppleKeyStore AppleMesa ISP endpoint to ISIC
	random scoret SKS SBIO Touch ID Sensor
	bio memory August 1973
	SEP SKS memory SKS keyring
	SEP SKS memory SKS keyring

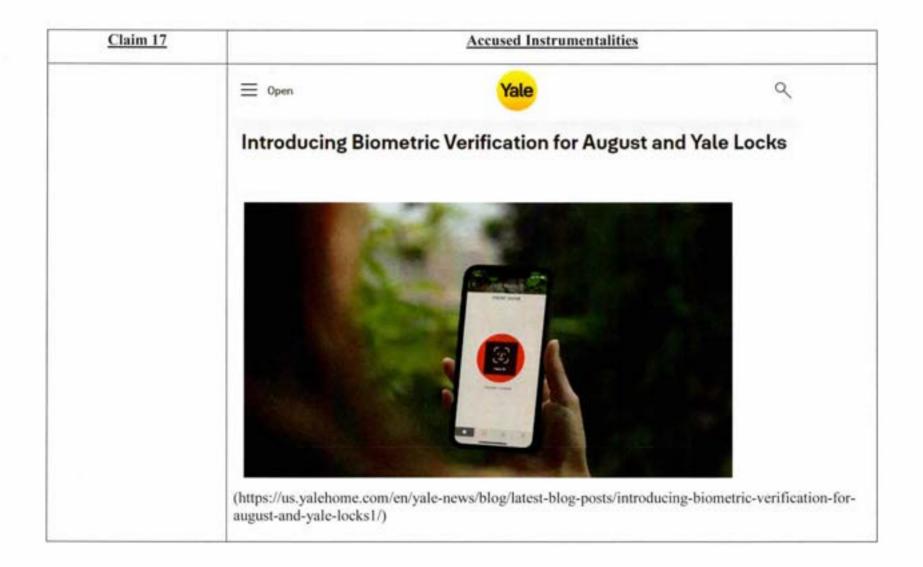
Claim 17	Accused Instrumentalities
	The class keys are encrypted with a master key:
	User Keybags Background
	Background
	Sets of keys generated for each user to protect their data at rest
	Keys wrapped by master key derived from user passcode and SEP UID
	After 10 incorrect passcode entries, SEP will not process any further attempts
	Different policy associated with each keybag key—Usage, availability
	(Id., at 25.)
	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.
17d. emitting a secure access signal conveying information dependent upon said accessibility attribute; and	The Accused Instrumentalities include a transmitter configured to emit a secure access signal conveying information dependent upon said accessibility attribute. For example, the Secure Enclave emits a signal with ephemerally re-encrypted file keys:

Claim 17	Accused Instrumentalities
	"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.)
	"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.)
	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:
	"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." (Id.)

Claim 17	Accused Instrumentalities
	Filesystem Data Protection
	Overview
	File blocks are encrypted using AES-XTS with 128-bit keys
	Each file on the user partition is encrypted using a unique random key chosen by S
	Raw file keys are never exposed to the AP
	 Wrapped with a key from the user keybag for long-term storage
	 Wrapped with an ephemeral key while in use, bound to boot session (Ex. B, Behind the Scenes with iOS Security, at 29.)



Claim 17	Accused Instrumentalities
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	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.
electronic computing device.	"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/)



Claim 17	Accused Instrumentalities
	(https://www.apple.com/shop/product/HPAR2ZM/A/yale-assure-lock-sl-touchscreen-deadbolt-black