

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

SAMSUNG ELECTRONICS CO. LTD. and SAMSUNG ELECTRONICS
AMERICA, INC.,
Petitioners,

v.

OS-NEW HORIZON PERSONAL COMPUTING SOLUTIONS LTD.,
Patent Owner

IPR2025-00613
U.S. Patent 8,401,875

**PETITION FOR *INTER PARTES* REVIEW OF
U.S. PATENT NO. 8,401,875**

Mail Stop PATENT BOARD
Patent Trial and Appeal Board
U.S. Patent & Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

TABLE OF CONTENTS

I.	Grounds for Standing.....	1
II.	Identification of Challenge	1
	A. Prior Art.....	1
	B. Grounds For Challenge	2
III.	The '875 Patent.....	2
	A. Patent Overview	2
	B. Technical Background.....	3
	C. Level of Ordinary Skill	4
	D. Prosecution History	4
	1. USPTO Examiner and Applicant Agree Multi-Biometric Authentication Was Known.....	4
	2. European Counterpart Application Never Issues Because of Fadell	5
	E. Claim Construction.....	6
	1. “first storage unit” (Claim 1)	6
	2. “second storage unit” (Claim 1).....	7
	3. “authentication unit” (Claim 1).....	7
	4. “communication and data connection means for communicating with an external device, said communication and data connection means being controlled by and in communication with said processor” (Claim 4)	8
IV.	GROUND 1: Fadell-Moran Combination Renders Obvious Claims 1, 4, 7, 10, 14, and 19.....	9
	A. Combination Overview	9

1.	Fadell.....	9
2.	Moran	11
3.	Motivation to Combine	12
B.	Independent Claim 1	16
1.	Preamble [1P].....	16
2.	Integrated Biometric Sensors [1A]	18
3.	Life Signs Detector [1B]	21
4.	First Storage Unit [1C].....	23
5.	Authentication Unit [1D]	24
a)	Integrated Authentication System	25
b)	“pre-recorded set of personal biological biometric identification parameters”	26
c)	Second Storage Unit	26
d)	Authentication Unit	28
e)	Authentication Unit Comprising the Second Storage Unit	31
6.	Processor [1E]	31
7.	Matching Personal Biological Biometric Identification Parameters [1F]	33
8.	Critical Level Detection [1G]	34
C.	Claims 4 and 7	35
D.	Claim 10	37
E.	Claim 14	38
F.	Claim 19	39

V.	GROUND 2: Fadell-Moran-Rosenblatt Combination Renders Obvious Claims 15 and 18.....	41
A.	Overview of the Combination.....	42
1.	Rosenblatt.....	42
2.	Motivation to Combine.....	43
B.	Claim 15	47
C.	Claim 18	50
VI.	GROUND 3: Kohinata-Mizusawa Combination Render Obvious Claims 1 and 4	50
A.	Overview of the Combination.....	50
1.	Kohinata	50
2.	Mizusawa	51
3.	Motivation to Combine	52
B.	Independent Claim 1	56
1.	Preamble [1P]: “Apparatus”	56
2.	Integrated Biometric Sensors [1A]	57
3.	Life Signs Detector [1B].....	59
4.	First Storage Unit [1C].....	61
5.	Authentication Unit [1D]	62
a)	Authentication Module	62
b)	“pre-recorded set of personal biological biometric identification parameters”	65
c)	Second Storage Unit	66
d)	Authentication Unit	67

e)	Authentication Unit Comprising the Second Storage Unit.....	70
6.	Processor [1E].....	70
7.	Matching of Personal Biological Biometric Identification Parameters [1F].....	72
8.	Critical Level Detection [1G]	73
C.	Claim 4	74
VII.	GROUND 4: Kohinata-Mizusawa-Rosenblatt Combination Render Obvious Claims 15 and 18.....	76
A.	Motivation to Combine	77
B.	Claim 15	79
C.	Claim 18	82
VIII.	Discretionary Denial is Not Appropriate.....	82
A.	35 U.S.C. §314(a).....	82
B.	35 U.S.C. §325(d).....	83
IX.	Mandatory Notices.....	84
A.	Real Party In Interest.....	84
B.	Related Matters.....	84
C.	Notice of Counsel and Service Information.....	84
X.	Conclusion	85

EXHIBIT LIST

Exhibit	Description
1001	U.S. Patent 8,401,875 to Fish et al. (the “’875 patent”)
1002	Prosecution History of U.S. Patent 8,401,875 (“’875 PH”)
1003	Declaration of Dr. Andrew Wolfe in Support of Petition for <i>Inter Partes</i> Review of U.S. Patent 8,401,875
1004	Curriculum Vitae of Dr. Andrew Wolfe
1005	Prosecution History of European Patent Office Patent Application No. 11/752,936.2 (“EPO PH”)
1006	Anil K. Jain et al., “ <i>An Introduction to Biometric Recognition</i> ” (2004) (“Jain”)
1007	U.S. Patent App. Pub. No 2009/0083847 to Fadell et al. (“Fadell”)
1008	U.S. Patent No. 6,539,380 to Moran (“Moran”)
1009	U.S. Patent No. 6,788,928 to Kohinata et al. (“Kohinata”)
1010	U.S. Publication No. 2010/0082490 to Rosenblatt et al. (“Rosenblatt”)
1011	Japanese Patent App. Pub. No. P2001-109855A to Mizusawa et al.
1012	Certified Translation of Japanese Patent App. Pub. No. P2001-109855A to Mizusawa et al. (“Mizusawa”)
1013	U.S. Patent No. 8,495,020 to Nasserbakht et al. (“Nasserbakht”)
1014	U.S. Patent No. 7,313,825 to Redlich et al. (“Redlich”)
1015	U.S. Patent No. 7,587,595 to Scarlata et al. (“Scarlata”)
1016	PO’s Infringement Contentions for the ’875 patent in <i>OS-New Horizon Personal Computing Solutions v. Samsung Electronics Co., Ltd.</i> , No. 2:24-cv-00634-JRG-RSP (E.D. Tex.) (“OSNH v. Samsung – OSNH’s ’875 Patent Infringement Contentions”)

Exhibit	Description
1017	Bruce Schneier, “ <i>Applied Cryptography</i> ” 2nd ed. 2006 (“Applied Cryptography”)
1018	Excerpt from Bryan Pfaffenberger, “ <i>Webster’s New World Computer Dictionary</i> ” 10th ed. 2003 (“Webster’s Computer Dictionary”)
1019	Ross Anderson, “ <i>Security Engineering</i> ” 2nd ed. 2008 (“Anderson”)
1020	Excerpt from Richard E. Smith, “ <i>Authentication From Passwords to Public Keys</i> ” (2002) (“Smith”)
1021	U.S. Publication No. 2007/0241861 to Venkatanna et al. (“Venkatanna”)
1022	U.S. Publication No. 2010/0115607 to Pratt et al. (“Pratt”)
1023	U.S. Publication No. 2008/0037001 to Yokoyama et al. (“Yokoyama”)
1024	U.S. Patent No. 5,719,950 to Osten et al. (“Osten”)
1025	Excerpt from Microsoft Corporation, “ <i>Microsoft Computer Dictionary</i> ,” 5th ed. 2002 (“Microsoft Dictionary”)
1026	R. Ricci et al., “ <i>THE ‘SECUREPHONE’ A Mobile Phone with Biometric Authentication and e-Signature Support for Dealing Secure Transactions on the Fly</i> ” (2006) (“SecurePhone”)
1027	ISO/IEC 18092, First Edition Information technology—Telecommunications and information exchange between systems—Near Field Communication—Interface and Protocol (NFCIP-1) (April 1, 2004) (“ISO/IEC 18092”)
1028	ISO/IEC 21481, First Edition – Information technology—Telecommunications and information exchange between systems—Near Field Communication Interface and Protocol -2 (NFCIP-2) (January 15, 2005) (“ISO/IEC 21481”)
1029	U.S. Patent No. 8,199,719 to Taneja (“Taneja”)

Exhibit	Description
1030	Behzad Razavi, “ <i>RF Microelectronics</i> ,” (1998) (“Razavi”)
1031	Anil K. Jain et al. “ <i>Handbook of Biometrics</i> ,” (2008) (“Biometrics Handbook”)
1032	U.S. Publication No. 2008/0233880 to Rofougaran et al. (“Rofougaran”)
1033	U.S. Publication No. 2003/0115490 to Russo et al. (“Russo”)
1034	Excerpt from Jochen Schiller et al. “ <i>Location Based Services</i> ” (2004) (“Schiller”)
1035	U.S. Patent No. 7,762,469 to Sueoka et al. (“Sueoka”)

Samsung Electronics Co. Ltd. and Samsung Electronics America, Inc.

(“Petitioners”) petition for *inter partes* review of claims 1, 4, 7, 10, 14, 15, 18 and 19 of U.S. Patent 8,401,875 (“the ’875 patent”; EX-1001).

I. Grounds for Standing

Petitioners certify the ’875 patent is available for IPR; Petitioners are not barred or estopped.

II. Identification of Challenge

A. Prior Art

The ’875 patent, filed August 4, 2010, claims priority to Provisional 61/313,145 filed March 12, 2010. Petitioners do not acquiesce the ’875 patent is entitled to priority of the provisional. Regardless, each applied reference was filed or published before March 12, 2010.

1. **U.S. Publication 2009/0083847 to Fadell, et al.** (“Fadell”; EX-1007), published March 26, 2009, is prior art under 35 U.S.C. §102(a).

2. **U.S. Patent 6,539,380 to Moran** (“Moran”; EX-1008), published March 25, 2003, is prior art under 35 U.S.C. §102(b).

3. **U.S. Patent 6,788,928 to Kohinata, et al.** (“Kohinata”; EX-1009), published September 7, 2004, is prior art under 35 U.S.C. §102(b).

4. **U.S. Publication 2010/0082490 to Rosenblatt et al.** (“Rosenblatt”; EX-1010), filed September 30, 2008, is prior art under 35 U.S.C. §102(e).

5. **JP2001-109855 to Mizusawa** (“Mizusawa”; EX-1012), published

April 20, 2001, is prior art under 35 U.S.C. §102(b).

B. Grounds For Challenge

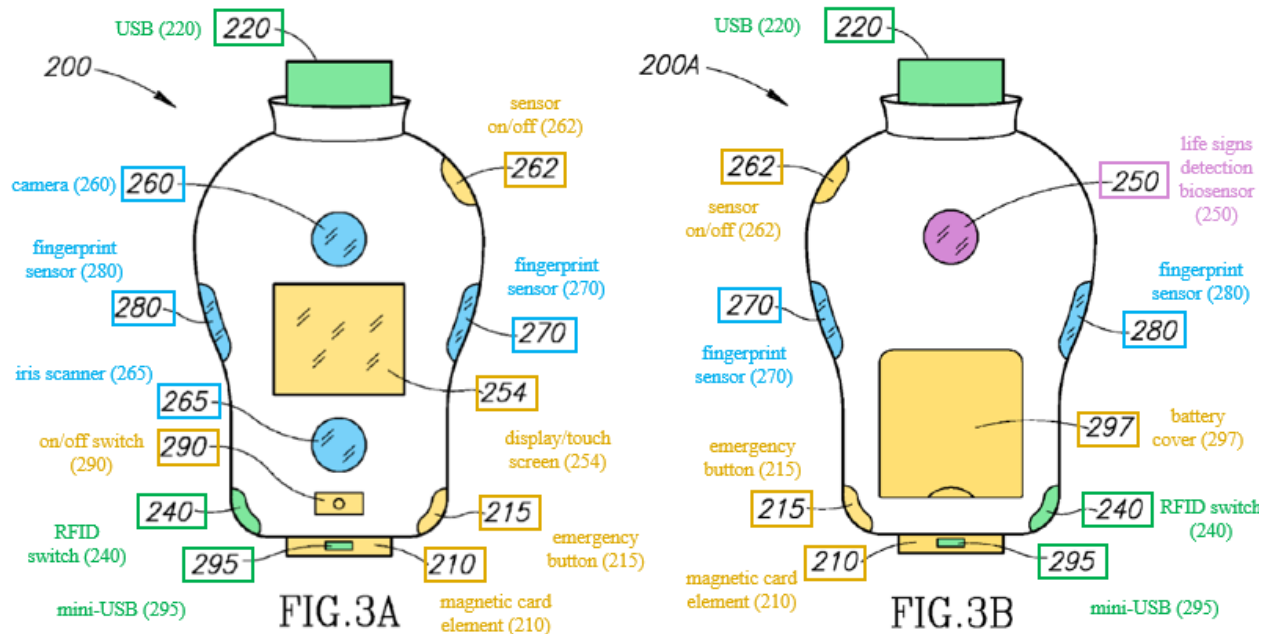
Ground		Claims	Prior Art
1	103	1, 4, 7, 10, 14, 19	Fadell, Moran
2	103	15, 18	Fadell, Moran, Rosenblatt
3	103	1, 4	Kohinata, Mizusawa
4	103	15, 18	Kohinata, Mizusawa, Rosenblatt

III. The '875 Patent

A. Patent Overview

The challenged claims are directed to an apparatus “for managing highly secured personal data” using a plurality of standard biometric authentication systems (EX-1001, Abstract) and a “life signs detector” that prevents data access if a critical level of a life signs parameter is detected (EX-1001, 18:22-27). Figures 3A and 3B¹ show the front and rear of a “preferred embodiment” (EX-1001, 24:21-24), that includes biometric sensors (blue), data/communication means (green), life sign detector (purple) and other components (brown). (EX-1001, 24:25-26:19; EX-1003, ¶¶37-60.)

¹ All emphasis and figure annotations added unless otherwise noted.



B. Technical Background

The use of biometric authentication systems in handheld devices was well known by 2008. For example, the image below shows “[a] cell-phone that validated authorized users using fingerprints and allows them access to functionalities such as mobile-banking.” (EX-1031, 14; EX-1003, ¶¶30-34.)



Biometrics Handbook, Figure 1.5(e)

Also well-known was the fact that biometrics could be “spoof[ed]” using a counterfeit, such as by placing a “latent fingerprint on a sensor, reactivated by

breathing on it.” (EX-1031, 405.) As was the fact that “[t]he act of sensing vitality (‘liveness’) signs such as pulse [was] one method of spoof detection” and that liveness detection can take place in parallel with biometric data processing. (EX-1031, 405; EX-1003, ¶¶35-36; *see also*, EX-1003, ¶¶26-30.)

C. Level of Ordinary Skill

A person of ordinary skill in the art (“POSITA”) would have had a bachelor’s degree in electrical engineering, computer engineering, or a similar field, together with at least two years of practical experience in the research, design, or development of data security, with additional education substituting for practical experience and vice versa. (EX-1003, ¶62.)

D. Prosecution History

1. USPTO Examiner and Applicant Agree Multi-Biometric Authentication Was Known

During prosecution, the Examiner rejected the pending claims over U.S. Publication 2009/0062887 to Mass in view of Moran. (EX-1002, 161-84.) Specifically, the Examiner found the combination disclosed the claimed multi-biometric authentication, noting the combination teaches “stor[ing] a pre-recorded set of personal biological identification parameters uniquely associated with the specific user, wherein said authentication unit is configured to compare the plurality of personal biological identification parameters of the user holding the apparatus with the pre-recorded set of personal biological identification parameters

stored in” a second storage unit wherein access is granted only if each of the plurality of parameters matches a “pre-recorded set.” (EX-1002, 162-63.)

Applicant did not dispute these features were disclosed. Instead, Applicant amended claim 1 to add the “life signs detector” [1B] and “critical level” [1G] limitations. (EX-1002, 192-93.) The Examiner subsequently allowed the claims, stating the prior art failed to disclose the “life signs detector” limitation. (EX-1002, 222-23.)

2. European Counterpart Application Never Issues Because of Fadell

On March 10, 2011, PO entered the counterpart International Application into the European phase. (EX-1005, 87.) Before examination, Applicant amended the pending claims to match claims 1-15 of the ’875 patent. (EX-1005, 144-175.) After issuance of the U.S. claims, the EP Examiner rejected pending claims 1-15 for lack of inventive step over Fadell. (EX-1005, 188-92.) Fadell was not considered during U.S. prosecution of the ’875 patent. (EX-1001, (56) References Cited.)

In response, Applicant alleged that Fadell “fails to disclose each and every” limitation in the claim, without further explanation. (EX-1005, 204-05.) The Examiner “carefully re-considered the arguments” from its previous communication and concluded that claim 1 lacked an inventive concept in view of Fadell and “matter[s] of general knowledge” that “cannot represent a single general

inventive concept.” (EX-1005, 239-41.) Applicant abandoned the claims. (EX-1005, 713.)

E. Claim Construction

The terms “*first storage unit*,”² “*second storage unit*,” “*authentication unit*,” and “*communication and data connection means*” require construction in this proceeding. Although the first three terms do not recite “means,” they are means-plus-function terms because they do not “‘recite sufficiently definite structure’ or else recite[] ‘function without reciting sufficient structure for performing that function.’” *Williamson v. Citrix Online, LLC*, 792 F.3d 1339, 1349 (Fed. Cir. 2015) (*en banc*) (internal citations omitted). The term “unit,” like the “nonce” terms in *Williamson* (“element”, “mechanism”, “module”) does not, standing alone, connote any particular structure. *Id.* at 1350; *see also Diebold Nixdorf, Inc. v. Int’l Trade Comm’n*, 899 F.3d 1291, 1301 (Fed. Cir. 2018).

1. “first storage unit” (Claim 1)

Function: storing of said user’s data and documentation files

Structure: memory and equivalents

The ’875 patent consistently discloses the structure storing user’s data and document files is memory. (*See, e.g.*, EX-1001, 20:28-29 (“[H]ighly secured user’s

² All quoted language of the challenged claims is italicized.

personal data files [are] **stored in the secured mass memory sub-module 174.**”), 19:48-50 (“[T]he user’s name, his ID data and the user emergency medical data, **as stored in memory module 150**”), 20:25-29 (describing “highly secured user’s personal data files [are] stored in the secured **mass memory** sub-module 174”); EX-1003, ¶¶85-91.)

2. “second storage unit” (Claim 1)

Function: storing a pre-recorded set of personal biological biometric identification parameters uniquely associated with the specific user.”

Structure: memory and equivalents.

The function of “storing a pre-recorded set of personal biological biometric identification parameters uniquely associated with the specific user” is performed at sub-module 140 which is described as a “memory module” or “memory unit.” (EX-1001, 20:32-34 (“**Module 140** will store **the registered user’s original**, initial registration step, **bio sensors measured output** for reference....”), 24:47-48, 27:1-3; EX-1003, ¶¶92-94.)

3. “authentication unit” (Claim 1)

Function: comparing the plurality of personal biological biometric identification parameters of the user holding the apparatus with the pre-recorded set of personal biological biometric identification parameters stored in said second storage unit.

Structure: memory and processor programmed to perform the recited function

In addition to storing a pre-recorded set of parameters, sub-module 140 is also used to create “the authentication process and the related decision required to enable operation of the apparatus 100 only by the legitimate owner and user of said specific apparatus.” (EX-1001, 20:36-40.)

As noted above, the structure of sub-module 140 is described both as a “memory unit” (EX-1001, 27:3) and an “authentication sub-module” (EX-1001, 20:37).

“‘[M]odule’ is simply a generic description for software or hardware that performs a specified function.” *Williamson*, 792 F. 3d at 1349. Here, authentication is conducted “based on the measurement and processing” of “biometric parameters.” (EX-1001, 26:40-45.) Therefore, the corresponding structure is memory and processor programmed to perform the recited function. (EX-1003, ¶¶95-101.)

4. **“communication and data connection means for communicating with an external device, said communication and data connection means being controlled by and in communication with said processor” (Claim 4)**

Function: communicating with an external device

Structure: one or more of a “wireless Bluetooth communication interface, a RF medium to short range communication

interface, in-room IR communication interface, mini USB data connectors, RFID receiver and transmitter, cellular modem, magnetic card element, USB connector, mini USB data transfer connector, and equivalents thereof.”

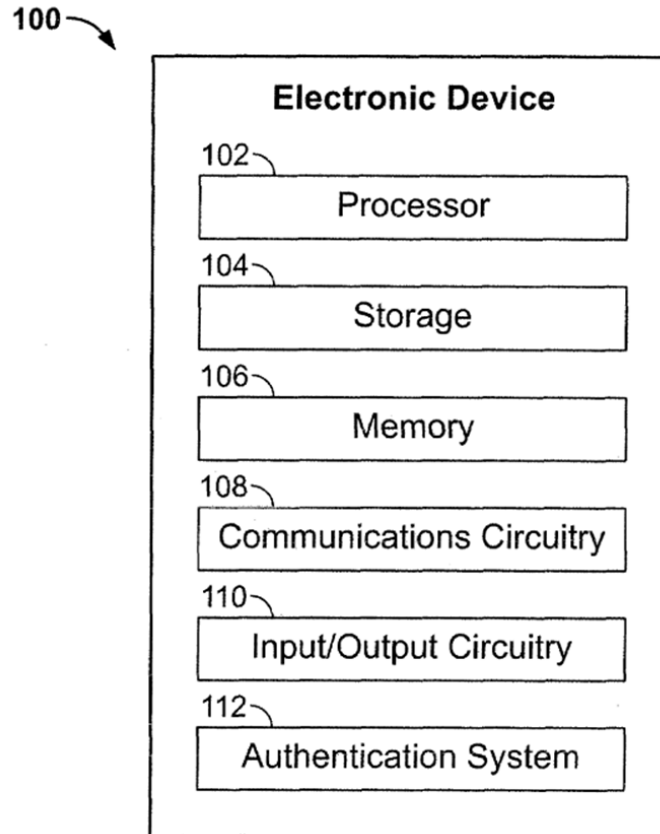
The ’875 patent describes a variety of structural components used to communicate with external devices. (*See, e.g.*, EX-1001, 17:23-34 (describing USB and non-standard data connectors, Bluetooth, and RF medium to short range interfaces, in-room IR, mini-USB), 22:34-37, 22:52-59 (RF transceiver and RFID units), 23:65-24:2 (cellular modems).) (EX-1003, ¶¶102-113.)

IV. GROUND 1: Fadell-Moran Combination Renders Obvious Claims 1, 4, 7, 10, 14, and 19

A. Combination Overview

1. Fadell

Fadell discloses “an electronic device with an embedded authentication system for restricting access to device resources.” (EX-1007, Abstract.) Fadell’s electronic device, illustrated in Figure 1 below, includes processor 102, storage 104, memory 106, communications circuitry 108, input/output circuitry 110, authentication system 112, and power supply 114. (EX-1007, ¶29.)



Fadell, Figure 1

Authentication system 112 “include[s] any suitable system or sensor operative to receive or detect an input identifying the user of device 100.” (EX-1007, ¶39.) For example, authentication system 112 includes “a skin-pattern sensing mechanism, an optical system for identifying users based on their facial patterns, eye features (e.g., retinas), or vein patterns, or any other sensor for detecting any other unique biometric feature or attribute of a user.” (*Id.*)

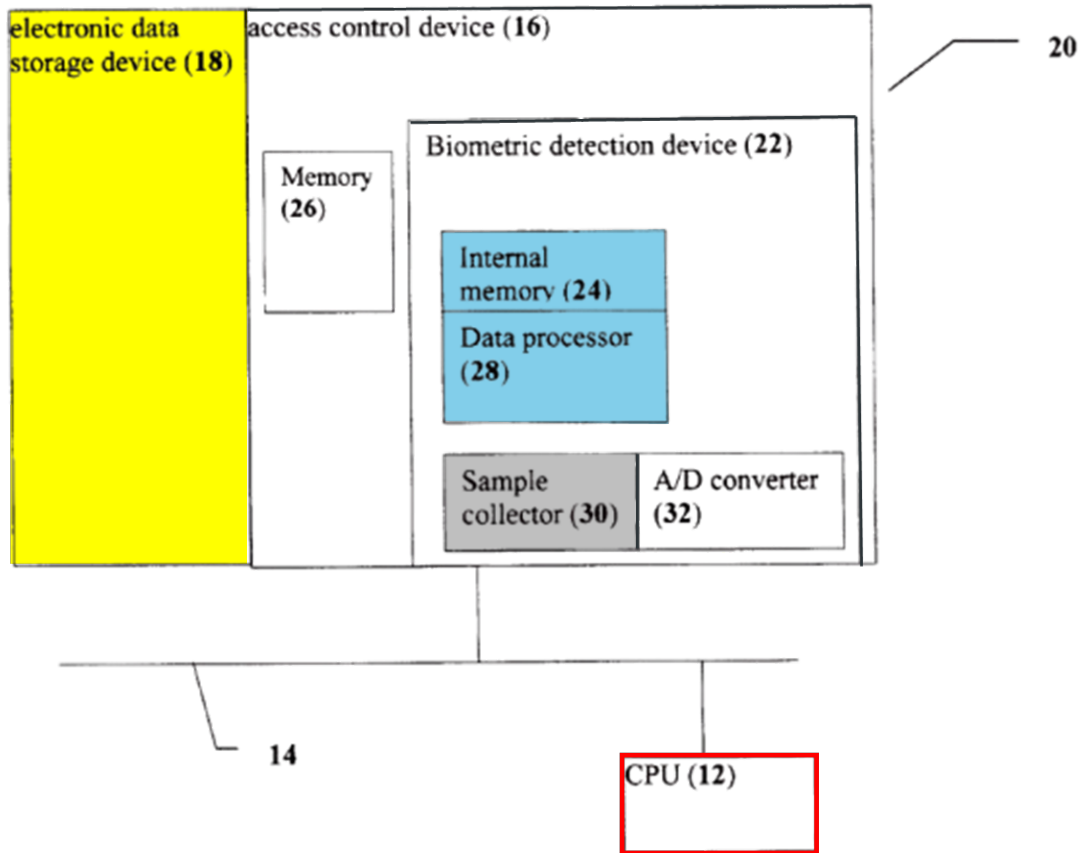
Furthermore, authentication system 112 also incorporates “suitable countermeasure[s] for preventing an unauthorized user from spoofing an

authorized user's skin patterns,” including “a combination of optical and capacitance sensors, a sonar or radio-frequency sensor, a sensor for detecting a user's pulse, a heat sensor for determining the temperature of the object placed against the sensor (e.g., to determine if the temperature is within a range of expected human skin temperatures), or any other suitable countermeasure.” (EX-1007, ¶57; EX-1003, ¶¶115-124.)

While Fadell broadly describes the “authentication system” as including “a system operative to detect and authenticate a user” based on biometric features (EX-1007, ¶25), it does not disclose implementation details, such the component that performs the authentication processing. Moran provides these details. (EX-1003, ¶125.)

2. Moran

Moran, like Fadell, is directed to “controlling access to data” using biometric authentication. (EX-1008, 1:11-14.) Moran's system includes an access control device 16 having memory 26 and a biometric detection device 22. Biometric detection device 22 “captur[es] data with regard to a biological parameter of a user, including, but not limited to, a fingerprint detection device and a device which performs a retinal scan, ... voice recognition, skin or other body chemical analysis.” (EX-1008, 4:62-67, Figure 3 (below).) (EX-1003, ¶¶125-130.)

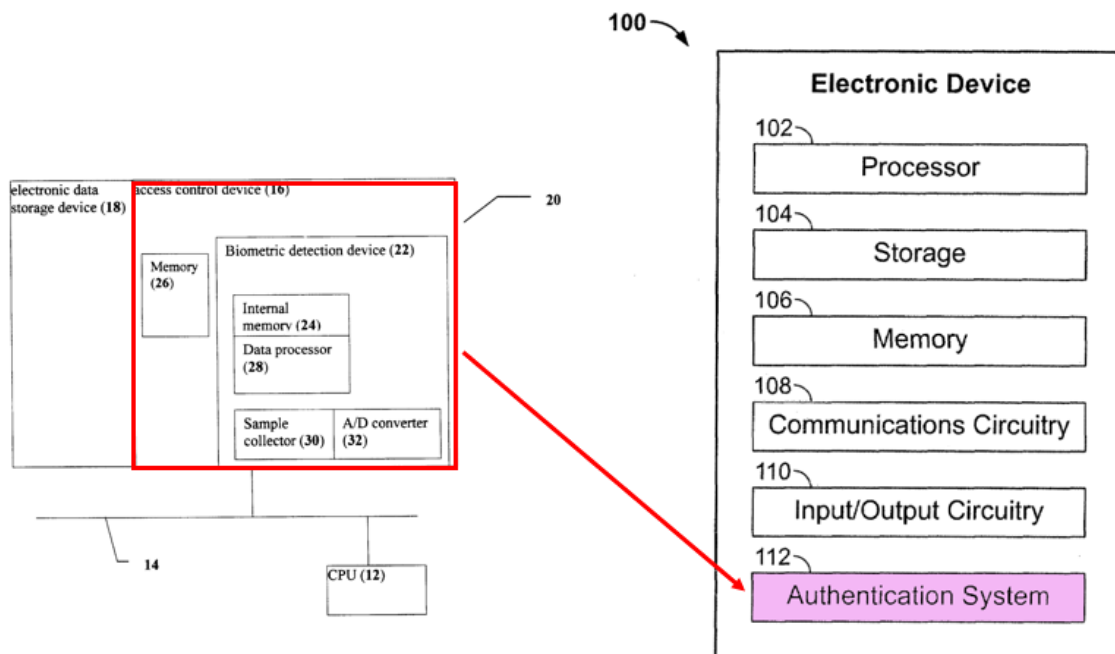


Moran, Figure 3

3. Motivation to Combine

A POSITA would have been motivated to combine Moran's teachings regarding an access control unit having an integrated biometric detection device with Fadell's device having multiple authentication systems. Fadell teaches that one or more of its device components "may be combined." (EX-1007, ¶29, *see also*, EX-1007, ¶39 ("Authentication system 112 may be combined or embedded in any other element of electronic device 112").) Based on this teaching, a POSITA would have been motivated to implement Fadell's multiple authentication systems as a biometric detection device with at least a shared processor and shared internal

memory within a hardware access control component (e.g., chip) as taught by Moran. In the resulting combination, Fadell's device includes an integrated access control (authentication) system supporting multiple types of biometric authentication that is coupled to the other components of Fadell's device (processor 102, storage 104, memory 106, communications circuitry 108, and input/output circuitry 110) via Fadell's bus which "provide[s] a data transfer path" among the components. (EX-1007, ¶40.)



Moran, Figure 3 (left); Fadell, Figure 1 (right)

A POSITA would have been motivated to make this combination for numerous reasons. First, Fadell is silent regarding implementation details of its authentication system, other than the types of sensors supported. A POSITA

would have therefore been motivated to search for references providing implementation details, and would have been led to Moran which is particularly related to “controlling access to data stored on a data storage device with a biometric detection device, such that access is determined through the operation of the biometric detection device.” (EX-1008, 1:10-14; EX-1003, ¶¶131-132.)

Second, a POSITA would have been motivated to modify Fadell to improve security, a motivation expressly stated in Moran. (EX-1003, ¶132.) Moran teaches that access control device 16 is “implemented as a chip, with a non-volatile memory.” (EX-1008, 7:9-11.) Moran stresses such an embodiment is preferred “since such an implementation also enables the security of access control device 16 to be more easily maintained, as electronic hardware devices are more difficult to ‘hack’ for unauthorized access.” (EX-1008, 7:52-55; *see also* EX-1008, 3:15-18.) Further, it was well-known long before the ’875 patent that implementing components such as a processor and memory within a physical boundary provided enhanced security. (*See, e.g.*, EX-1015, 1:33-36 (“A [trusted platform module] TPM is a hardware component that resides within a processing system and provides various facilities and services for enhancing the security.”), 8:6-7 (TPM provides “secure storage of keys and other data.”).) (EX-1003, ¶133.)

Third, a POSITA would have also been motivated to use Moran’s teachings of an access control (biometric authentication) device having a dedicated

processor/memory to improve the operation of Fadell's authentication process. For example, the combined authentication system does not have to compete with other applications for access to the device's main processor or storage unit. (*See, e.g.*, EX-1013, 4:66-5:1 ("By providing separate memory for each functional unit, the majority of issues with memory bottleneck are eliminated"); EX-1003, ¶¶134-135.)

Finally, the combination is nothing more than the application of a known technique (Moran's access control device architecture) to a known device (Fadell's device) ready for improvement and the simple substitution of one known element (Moran's access control device architecture) for another (Fadell's authentication system). The results of the combination would have been predictable. (EX-1003, ¶136.) A POSITA would have been motivated to make the combinations for the reasons discussed above. (*Id.*)

A POSITA would have had a reasonable expectation of success in the combination. (EX-1003, ¶137.) Moran expressly discloses its teachings apply to portable devices, like Fadell's device. (*See, e.g.*, EX-1008, 4:38-53 (describing the "computer" includes, e.g., a cellular phone or "any other handheld device").) Moran further discloses its access control device (and associated biometric device) can be "directly integrated" into the device for which it controls access (e.g., in Moran, the data storage device 18). (EX-1008, 7:32-33.) Therefore, integrating Moran's access control hardware component into Fadell's electronic device to act

as the embedded authentication system would have been well within the skill set of a POSITA before the '875 patent. (EX-1003, ¶137.)

Fadell and Moran are both in the same field—managing access to user information (e.g., data or files). (See EX-1007, Abstract (“[A]n electronic device with an embedded authentication system for restricting access to device resources.”); EX-1008, Abstract (“A device, a method and a system for providing control of access to data which is stored in an electronic data storage device.”) Fadell and Moran are also reasonably pertinent to problems addressed by the '875 patent, namely the “need to improve and enhance the access control capabilities to first securely and efficiently authenticate the specific user before giving this user access to sensitive personal data files.” (EX-1001, 4:28-31; EX-1003, ¶138.)

B. Independent Claim 1

1. Preamble [1P]

The Fadell-Moran combination discloses an “*apparatus for storing and managing personal and secured data and documentation files associated with a specific user.*” (EX-1003, ¶¶139-144.)

Fadell’s device, illustrated in Figure 1 (below), includes “an embedded authentication system for restricting access to device resources.” (EX-1007, Abstract.) Fadell’s device, as modified by Moran, is an “*apparatus.*” (EX-1003, ¶139.)

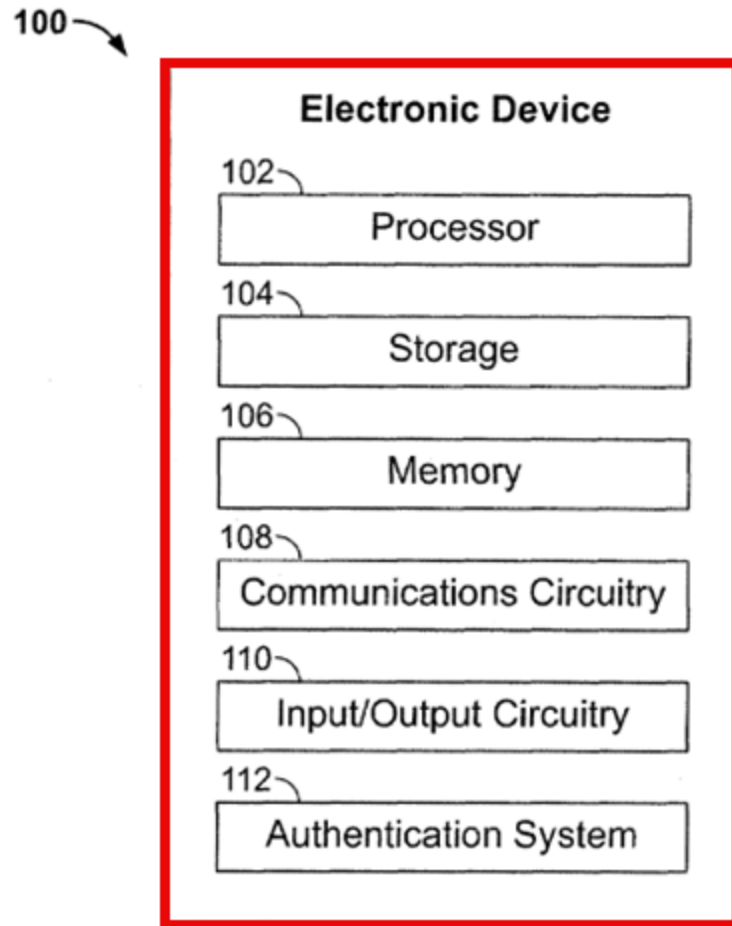


FIG. 1

Fadell, Figure 1

Fadell's device stores "*personal and secured data and documentation files associated with a specific user.*" (EX-1003, ¶140.) For example, Fadell's storage 104 stores, among other items, user preference information data, lifestyle information data, exercise information data, subscription information data, and contact information data. (EX-1007, ¶31.) Although Fadell does not use the term "file" when describing the user-specific data stored in storage 104, a POSITA would have understood data is stored using a file. (EX-1025, 211 (explaining that a file is

a “collection of information” and a “basic unit of storage”).) Indeed, Fadell uses the term “*file*” throughout its disclosure when referring to stored information. (EX-1007, Abstract, ¶¶24, 31, 42, 51, 52; EX-1003, ¶141.) The above listed items are therefore each examples of “*personal data*” and “*documentation files*” associated with the user. This data, as well as other data (e.g., authentication information), is “*secured*” because only authenticated individuals can obtain access. (EX-1003, ¶142.)

Fadell’s device “*manag[es]*” access to this “*personal and secured data and documentation files associated with a specific user*” through its authentication process. (See, e.g., EX-1007, ¶43 (requiring “user to authenticate” to access stored personal data), EX-1003, ¶143.) Specifically, “[a]ccess to any suitable electronic device resource may be restricted, including for example access to **files or data stored on or available to the device.**” (EX-1007, ¶24.)

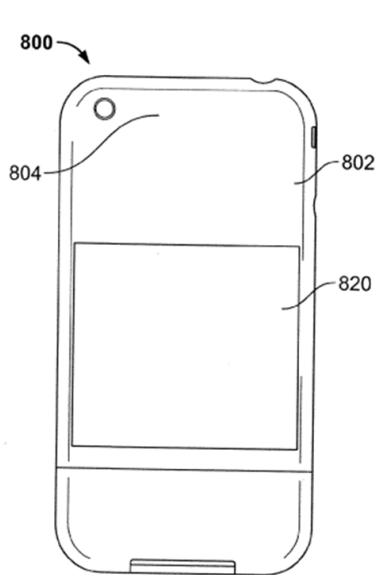
2. Integrated Biometric Sensors [1A]

The Fadell-Moran combination discloses “*a plurality of biometric sensors for reading a plurality of personal biological biometric identification parameters of the user holding the apparatus, said plurality of biometric sensors being integrated within the apparatus.*” (EX-1003, ¶¶145-154.)

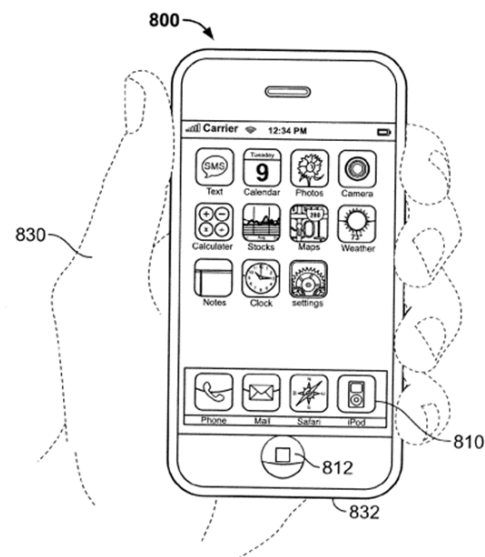
Fadell’s device is an “embedded authentication system” with “one or more sensors operative to detect biometric information of a user.” (EX-1007, Abstract.)

Fadell describes numerous sensors designed to be “*integrated within*” its device including, for example, the following:

- **Fingerprint:** Fadell describes sensors for detecting features of a user’s skin (i.e., fingerprints) that “may be placed at any suitable location within the device” such as embedded in the display (§62) or “adjacent to or behind any button or other physical input” (§65). (EX-1007, §§55-56, 59-60.) These sensor generates “an image or a representation of the skin placed over the sensor.” (EX-1007, §56.)
- **Handprint:** Fadell describes a sensor “embedded in back surface 804 and operative to detect features of a user’s palm or hand” when the user is holding the device. (EX-1007, §67.)



Fadell, Figure 8A



Fadell, Figure 8B

- **Under skin feature:** Fadell describes a sensor “located on the surface of the electronic device” that “detect[s] the pattern of a user’s veins,

arteries, follicle distribution, or any other suitable feature underneath the user's skin.” (EX-1007, ¶69.)

- **Facial feature:** Fadell describes “a light sensor (e.g., a camera), an infra-red sensor, an ultra-violet sensor, a scanning laser, an ultrasound sensor (e.g., sonar)” for detecting a user's facial features. (EX-1007, ¶71.) Each of these sensors is “located at any suitable position on the electronic device” or “a camera or other sensor provided with the electronic device for a different purpose.” (EX-1007, ¶73.)
- **Eye feature:** Fadell describes a sensor that “scan[s] a user's retina, iris or retinal blood vessels to detect unique patterns of the user.” (EX-1007, ¶74.)
- **Voice:** Fadell also discloses a sensor (e.g., a microphone used primarily for other purposes) for detecting attributes or qualities of a user's voice. (EX-1007, ¶77.)
- **Ear feature:** Fadell describes a sensor, located near a speaker, “operative to detect unique features of a user's ear canal (e.g., shape and length).” (EX-1007, ¶77.)

(*See also*, EX-1007, ¶¶39, 77-78.) To the extent it is not explicit, a POSITA would have understood the user holds the phone so that these integrated sensors can read a user's biometric data. (EX-1003, ¶¶145-152.)

The data collected by the fingerprint sensor, handprint sensor, under skin feature sensor, facial feature sensor, eye feature sensor, voice sensor, and ear

feature sensor are each “*personal biological identification parameter[s] of the user*” and, therefore, the corresponding sensors are each a “*biometric sensor[] for reading [] personal biological biometric identification parameters of the user holding the apparatus.*” (EX-1003, ¶¶145-152.)

Fadell’s device includes “*a plurality of*” the biometric sensors described above. Fadell’s device may include “several biometric authentication systems.” (EX-1007, ¶28.) Specifically, a user may “select one **or more** authentication systems to satisfy before providing access to the resource.” (EX-1007, ¶52.) Additionally, “the electronic device may require a user to satisfy **several authentication systems** prior to providing access to an application or data.” (EX-1007, ¶41.) That is, the device may require multi-biometric authentication before allowing access to requested resources. (EX-1003, ¶153.)

3. Life Signs Detector [1B]

The Fadell-Moran combination discloses “*at least one life signs detector integrated within the apparatus, said life signs detector being configured to measure and record at least one of said user’s life sign parameters.*” (EX-1003, ¶¶155-160.)

Fadell discloses “countermeasure[s] for preventing an unauthorized user from spoofing” such as detecting the user’s vital signs—pulse and temperature. (See, e.g., EX-1007, ¶57.) For example, Fadell’s device includes “a sensor for

detecting a user's pulse" or "heat sensor for determining the temperature of the object placed against the sensor (e.g., to determine if the temperature is within a range of expected human skin temperatures)." (EX-1007, ¶57.) The user's pulse/temperature are a "*user's life sign parameter[]*" and therefore the pulse sensor and temperature/heat sensor are each a "*life signs detector integrated within the apparatus.*" (EX-1003, ¶155.)

Fadell teaches its heat sensor "determin[es] if the temperature is within a range of expected human skin temperatures." (EX-1007, ¶57.) A POSITA would have understood that the pulse sensor would perform a similar determination to confirm the presence of a live individual. That is, the "*life signs detector*" measures and records the "*user's life signs parameter*" (vital sign), at least temporarily, so it can be compared against values indicative of a "live individual." (EX-1003, ¶156.)

PO contends in its infringement allegations that whether the user's eyes are opened or closed is a "*life sign parameter.*" (EX-1016, 8 ("Accused Instrumentalities ... use[] a camera to determine if a user's eyes are open (life sign parameter) to prevent spoofing and determine if the user is alive.")) A POSITA would have understood the simple metric of a user's eyes being opened, without more, is insufficient to determine whether a user is alive. (EX-1003, ¶158.) Regardless, even if PO's overly broad interpretation is adopted, the Fadell-Moran combination discloses additional "*life sign detectors.*" For example, Moran

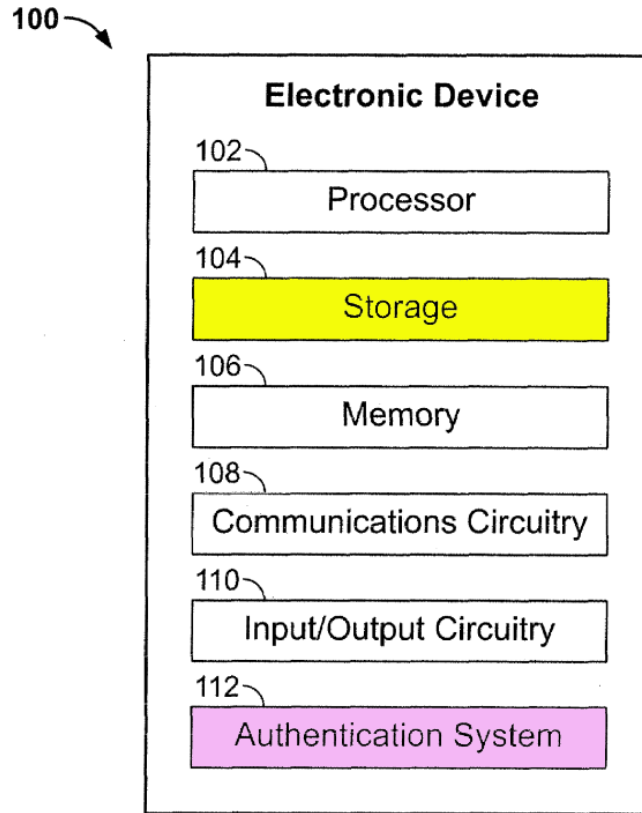
discloses “devices for measurement of ECG/EEG [and] pressure measurements on one or more body organs.” (EX-1008, 4:65-66.) Both measurements are indicative of whether an individual is alive. (EX-1003, ¶158.)

Fadell also discloses a sensor to “detect a predetermined eye movement set up by an authorized user” and when the user “moves his eyes in a manner that matches [this] predetermined eye movement,” the device “provide[s] access to restricted resources.” (EX-1007, ¶75.)

4. First Storage Unit [1C]

The Fadell-Moran combination discloses “*a first storage unit for the storage of said user’s data and documentation files.*” (EX-1003, ¶¶161-165.) “[F]irst storage unit” is a means-plus-function term with the function being “storing data and documentation files” and the structure being “memory.” (§III.E.1.)

Fadell’s device includes storage 104 (shaded yellow) which stores user preference information data, lifestyle information data, exercise information data, subscription information data and contact information data, which are each examples of both “*data*” and “*documentation files*” associated with the user. (See §IV.B.1.) Storage 104 includes “a hard-drive, solid state drive, flash memory, [and] permanent memory such as ROM.” (EX-1007, ¶31.) Thus, storage unit 104 performs the function—“storing a user’s data and documentation files” and meets the “*first storage unit*” structure (memory). (EX-1003, ¶¶162-163.)



Fadell, Figure 1

Should PO contend “*first storage unit*” is not a means-plus-function term, the Fadell-Moran combination discloses this limitation for the same reasons discussed above. (EX-1003, ¶165.)

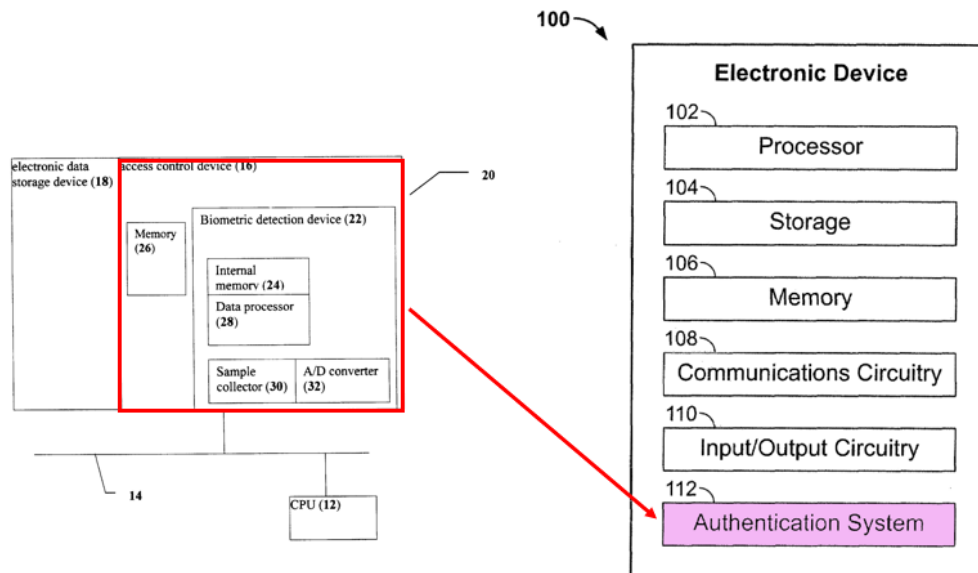
5. Authentication Unit [1D]

The Fadell-Moran combination discloses “*an authentication unit comprising a second storage unit, with said second storage unit configured to store a pre-recorded set of personal biological biometric identification parameters uniquely associated with the specific user, wherein said authentication unit is configured to compare the plurality of personal biological biometric identification parameters of*

the user holding the apparatus with the pre-recorded set of personal biological biometric identification parameters stored in said second storage unit.” (EX-1003, ¶¶166-186; §III.E.3 (means-plus-function construction of “authentication unit”; §III.E.2 (means-plus-function construction of “second storage unit”).)

a) Integrated Authentication System

As discussed in §IV.B.2, the device in the combination of Fadell and Moran integrates multiple types of biometric authentication (as taught by Fadell) into a single hardware component (e.g. a chip) as taught by Moran. (EX-1003, ¶168.) This integrated authentication system, embedded in the device, is coupled to other device components via Fadell’s internal bus. (*See* §IV.B.6.)



Moran, Figure 3 (left); Fadell, Figure 1 (right)

b) “pre-recorded set of personal biological biometric identification parameters”

Both Fadell and Moran disclose a “*pre-recorded set of personal biological biometric identification parameters.*” (EX-1003, ¶169.) With biometric authentication, a user must first enroll with the system by providing reference biometric data. (EX-1003, ¶170.) As discussed in §IV.B.2, the Fadell-Moran combination uses multiple types of biometric authentication and therefore the user must enroll data for each type of biometric authentication being used.

Fadell describes an enrollment process, according to which the user “provide[s] biometric information (e.g., a fingerprint, eye scan, or DNA sequence) **to be stored in a library.**” (EX-1007, ¶79.) During the authentication process, “detected biometric attributes” are compared with the stored “library of biometric attributes.” (EX-1007, ¶¶ 6, 79.) That is, the user’s reference biometric information is pre-recorded for later use during authentication. Moran similarly explains the “user is presumed to have provided a measurement of [] a biological parameter previously, in order for this information to be stored for later comparison.” (EX-1008, 12:22-25.)

c) Second Storage Unit

The Fadell-Moran combination discloses a “*second storage unit configured to store a pre-recorded set of personal biological biometric identification*

parameters uniquely associated with the specific user.” (EX-1003, ¶¶174-175;

§III.E.2 (means-plus-function claim construction).)

In Fadell, the user’s biometric reference parameters (“*pre-recorded set of personal biological biometric identification parameters uniquely associated with the specific user*”) are stored in a library. (See, e.g., EX-1007, ¶79 (user “provide[s] biometric information (e.g., a fingerprint, eye scan, or DNA sequence) to be stored in a library”), ¶6 (referring to “a library of biometric attributes”), ¶¶73-74.)

Although Fadell discloses “authentication information (e.g. libraries of data associated with authorized users)” is stored in storage 104 (EX-1007, ¶31), a POSITA would have been motivated to store this reference information in the dedicated internal memory of the integrated authentication system of the combined device, as taught by Moran. (EX-1003, ¶172.) Moran teaches biometric reference data (e.g., fingerprint data) is “stored on internal memory 24” of the access control device. (EX-1008, 10:64-67; *see also* EX-1008, 12:17-24.) For example, a POSITA would have recognized that internal memory in a separate hardware component (e.g., chip) provided improved security. Indeed Moran notes that this arrangement provides physical security and is “more difficult to ‘hack’.” (See EX-1008, 7:49-55.) A POSITA would have therefore been motivated to store sensitive reference data for authentication processing in this more secure location. (EX-1003, ¶173.) A POSITA would have also been motivated to store the reference

data internal and local to the authentication processor for improved operation and efficiency as explained in §IV.A.3.

Thus, internal memory 24 of the integrated authentication system performs the function of “storing a pre-recorded set of personal biological biometric identification parameters uniquely associated with the specific user” and meets the structure of a “memory.” (EX-1003, ¶174.)

Should PO contend that “*second storage unit*” is not a means-plus-function term, the combination of Fadell and Moran discloses this limitation for the same reasons discussed above. (EX-1003, ¶175.)

d) Authentication Unit

The Fadell-Moran combination discloses “*an authentication unit*” that “*is configured to compare the plurality of personal biological biometric identification parameters of the user holding the apparatus with the pre-recorded set of personal biological identification parameters stored in said second storage unit.*” (EX-1003, ¶¶182, 184.)

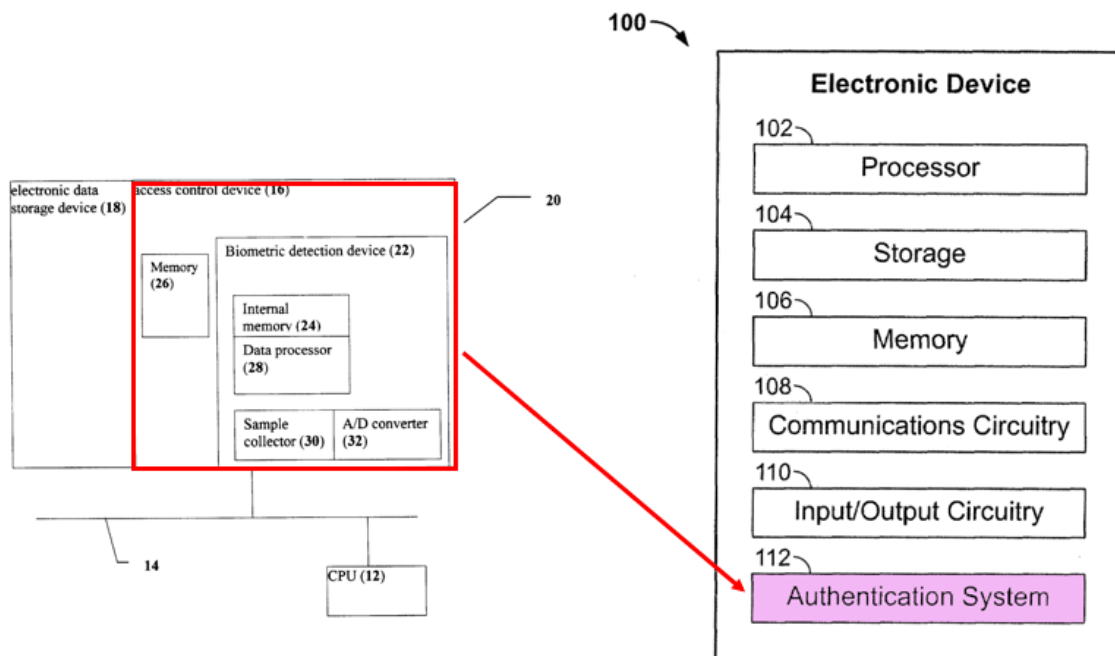
As discussed in §IV.B.2, the Fadell-Moran combination includes “*a plurality of biometric sensors for reading a plurality of personal biological biometric identification parameters of the user holding the apparatus.*” And as discussed above (§IV.B.5.b)), the Fadell-Moran combination discloses that a “*pre-recorded set of personal biological biometric identification parameters [is] stored*

in said second storage unit.” The collected biometric data is compared against the stored reference biometric data. As explained in Fadell, during authentication, the reference “biometric information stored in the library may be retrieved ... and **compared** to the biometric information provided by the user.” (EX-1007, ¶79.) For example, with fingerprint authentication, the collected fingerprint biometric is “compared to a library of images or representations available to the electronic device.” (EX-1007, ¶56.) As an additional example, for authentication based on eye attributes, the collected representation of the user’s eyes is “compared with a library of authorized user’s eyes.” (EX-1007, ¶74.) Similarly, Moran teaches collected biometric data is compared “to stored data which was previously captured from the user.” (EX-1008, 5:32-35.)

As discussed in §IV.B.2, “the electronic device may require a user to satisfy several authentication systems prior to providing access to an application or data.” (EX-1007, ¶41.) In this circumstance, the user will be required to perform biometric authentication for each of the designated authentication methods required for access and therefore must repeat the above process. (EX-1003, ¶178.) Thus, the Fadell-Moran combination discloses that the authentication system performs the function of “*compar[ing] the plurality of personal biological biometric identification parameters of the user holding the apparatus with the pre-*

recorded set of personal biological biometric identification parameters stored in said second storage unit.” (EX-1003, ¶¶179-180.)

In the Fadell-Moran combination, authentication processing is performed by the internal data processor within the integrated authentication system, discussed in §IV.B.5 and illustrated again below. Specifically, Moran teaches authentication processing is performed “by a software module which is stored in internal memory 24 and which is operated by data processor 28.” (EX-1008, 11:8-11, 11:31-34 (“digital signal is then optionally passed to data processor 28 for analysis”)); *see also, e.g.,* EX-1008, claims 3-4; EX-1003, ¶¶181-183.)



Moran, Figure 3 (left); Fadell, Figure 1 (right)

Thus, the Fadell-Moran combination discloses the structure of the authentication unit—memory (internal memory 24) and processor (data processor 28) that performs the recited function.

Should PO contend that “*authentication unit*” is not a means-plus-function term, the Fadell-Moran combination discloses this limitation for the same reasons discussed above. (EX-1003, ¶¶184-185.)

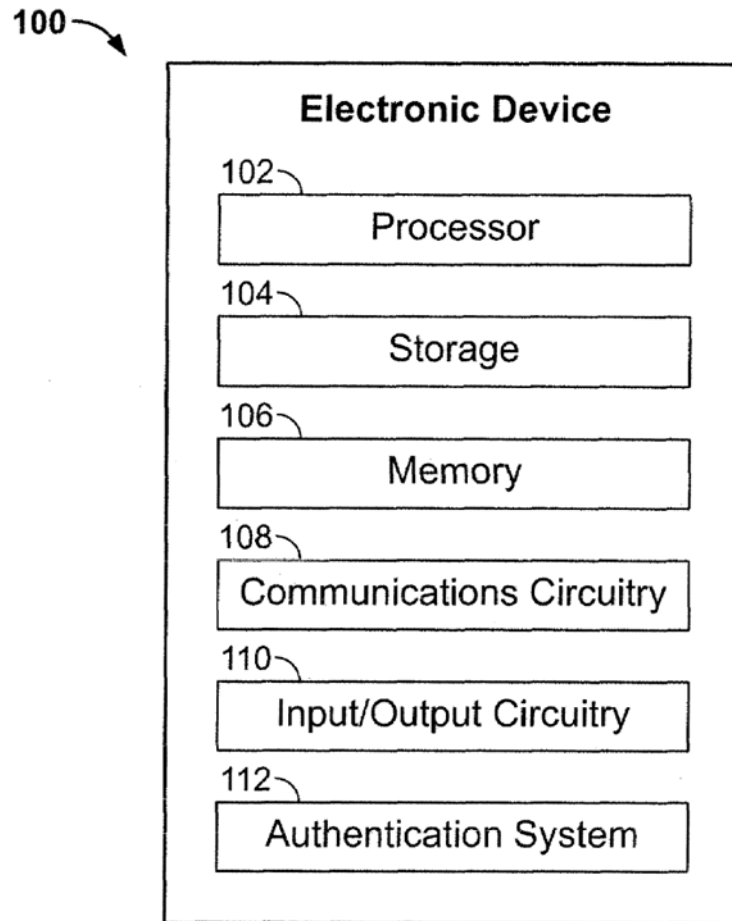
e) Authentication Unit Comprising the Second Storage Unit

As discussed in the prior section, the integrated authentication system of the Fadell-Moran combination includes an internal memory (e.g., internal memory 24) which is the “*second storage unit*” and a data processor. Thus, for the reasons discussed above, the combination discloses “*an authentication unit comprising a second storage unit.*” (EX-1003, ¶186.)

6. Processor [1E]

The Fadell-Moran combination discloses “*a processor in communication with said plurality of biometric sensors, said first storage unit and said authentication unit.*” (EX-1003, ¶¶187-189.)

Fadell’s device includes **processor 102** which “control[s] the operations and performance” of the device. (EX-1007, ¶30, Figure 1 (below).) The device also “include[s] a bus operative to provide a data transfer path for transferring data to, from, or between [any] component” in the device. (EX-1007, ¶40.)



Fadell, Figure 1

As explained by Moran, “any attempts to access data” must pass through the access control device (i.e., the authentication system). Therefore, if the processor “receives an instruction to read data”, it “cannot directly read such data” directly but “must send the command to access control device 16, which then determines if such access should be granted and the data read.” (EX-1008, 6:63-7:4.) A POSITA would understand the device in the Fadell-Moran combination operates in a similar manner. That is, to control device operations, the processor in the Fadell-Moran combination must communicate with the device components, including Fadell’s

biometric sensors, the storage unit (storing data sought to be accessed), and the integrated authentication system (controlling access to the stored data). (EX-1003, ¶¶187-188.)

7. Matching Personal Biological Biometric Identification Parameters [1F]

The Fadell-Moran combination discloses that “*access to the personal data and documentation files stored in said first storage unit is only enabled after said authentication unit positively matches each of the plurality of personal biological biometric identification parameters of the user holding the apparatus with the pre-recorded set of personal biological identification parameters stored in said second storage unit.*” (EX-1003, ¶¶190-193.)

The integrated authentication system in the combination controls (e.g., restricts) “[a]ccess to any suitable electronic device resource ... including for example access to files or data stored on or available to the device.” (EX-1007, ¶24.) Specifically, Fadell discloses that “[i]f the provided biometric authentication information matches information stored in the library”, the device “**provide[s] access to a restricted resource.**” (EX-1007, ¶79; *see also*, EX-1007, ¶41.) For example, for facial recognition, Fadell discloses that “[i]f an authorized user is detected,” the device “display[s] or **provide[s] access to restricted content 1112** on display 1110.” (EX-1007, ¶73.) Moran similarly discloses “access should be

granted and the data read from the data storage device” based on successful biometric authentication. (EX-1008, 7:2-5.)

As discussed in §IV.B.5, Fadell’s “electronic device may require a user to satisfy several authentication systems prior to providing access to an application or data.” (EX-1007, ¶41.) Therefore, each type of biometric authentication must be successful (positive match) to enable access to the requested resource (e.g., stored personal data and documentation files). (EX-1003, ¶¶190-192.)

8. Critical Level Detection [1G]

The Fadell-Moran combination disclose or suggests “*whenever any of said at least one life signs detector detects a critical level of said user measured life sign parameters, the apparatus is configured to prevent access to said user’s personal data and documentation files stored in said first storage unit.*” (EX-1003, ¶¶194-197.)

As discussed above (§IV.B.3), Fadell discloses use of pulse/temperature measurements to counter biometric spoofing. Although not explicit, Fadell suggests that access to requested data and/or files stored in its electronic device would be denied if the system detects spoofing. (EX-1003, ¶194.) With regards to body temperature, Fadell discloses that its sensor (“*life signs detector*”) determines if the user’s temperature (“*user measured life sign parameters*”) is within a range of expected human skin temperatures.” (EX-1007, ¶57.) That is, if the detected

value is below the lowest point of this range (i.e., is at a “*critical level*”), the “*detector*” determines the biometric was not obtained from a live person and restricts access. A POSITA would understand that the “user’s pulse” would be compared against a similar range of expected human pulse values and if the pulse falls below (or above) the range—i.e., is at a “*critical level*”, the “*detector*” determines the biometric was not obtained from a live person and restricts access. (EX-1003, ¶¶194-196.)

C. Claims 4 and 7

The Fadell-Moran combination discloses “*communication and data connection means for communicating with an external device, said communication and data connection means being controlled by and in communication with said processor*” [4] and “*said external device comprises any one of a group including a remote server, a local server, a host computer, voice or data communication means and a cellular phone.*” (EX-1003, ¶¶198-204.)

Fadell discloses the claimed “*communication and data connection means.*” Fadell’s device includes communications circuitry 108 permitting the device “to communicate with **one or more servers or other devices** using any suitable communications protocol.” (EX-1007, ¶33.) Specifically, Fadell’s communication circuitry may support, for example, “Wi-Fi (e.g., a 802.11 protocol)”, “Bluetooth™”, “radio frequency” systems, and cellular network protocols. (*Id.*) A

POSITA would have understood that a cellular network interface (and in fact any interface communicating using RF signals) includes a modulator/demodulation (e.g., a “cellular modem”). (*See, e.g.*, EX-1030, 6-8 (describing general RF transmitter/receiver architecture); EX-1029, 7:36-56 (describing use of a “modem”).) Thus, communication circuitry 108 performs the function of “communicating with an external device.” Because communication circuitry includes Bluetooth interface, an RF interface and/or a cellular modem, communication circuitry 108 further discloses the structure of the “*communication and data connection means*.” (EX-1003, ¶¶199-201.)

Fadell’s communication circuitry 108 is “*controlled by and in communication with said processor*.” In Fadell, processor 102 “control[s] the operations and performance” of the device. (EX-1007, ¶30.) And Fadell teaches that the device “include[s] a bus operative to provide a data transfer path for transferring data to, from, or between **control processor 102**, storage 104, memory 106, **communications circuitry 108**, input/output circuitry 110 authentication system 112, and any other component included in the electronic device.” (EX-1007, ¶40.)

Thus, the Fadell-Moran combination renders claim 4 obvious.

As noted above, Fadell’s communications circuitry 108 permits the device “to communicate with **one or more servers or other devices**.” (EX-1007, ¶33.)

Only two options exist for the server—it is either local or remote. (EX-1003, ¶204.) Fadell also notes that its device “allow[s] all users to place telephone calls” which a POSITA would understand encompasses communicating with another “*voice or data communication means*” and another “*cellular phone*.” (EX-1007, ¶43; EX-1003, ¶204.) And finally, Fadell notes that its embedded camera can be used as “an embedded webcam for chatting” which a POSITA would understand encompasses communicating with any or multiple of the following: a “*remote server, a local server, [or] a host computer*” [hosting the web chat], and/or “*voice or data communication means and a cellular phone* [of the other participants].” (EX-1007, ¶73; EX-1003, ¶204.)

Thus, the Fadell-Moran combination renders claim 7 obvious.

D. Claim 10

Claim 10 narrows claim 4 by specifying that the “*communication and data connection means comprises at least one of a group*” that includes “*a Bluetooth communication interface*.” As discussed above for claim 4, Fadell’s communication circuitry 108 supports “Bluetooth” (EX-1007, ¶33) and therefore Fadell discloses “*a Bluetooth communication interface*.” (EX-1003, ¶205.)

The Fadell-Moran combination discloses “communication and data connection means for communicating with an external device, said communication

and data connection means being controlled by and in communication with said processor” [4]. (EX-1003, ¶¶205-207.)

Thus, the Fadell-Moran combination renders claim 10 obvious.

E. Claim 14

The Fadell-Moran combination discloses “*the processor is configured to securely update the user’s data and documentation files.*” (EX-1003, ¶¶208-212.)

Fadell explains that its embedded authentication system “restrict[s] access to device resources” (e.g., “access to files or data stored on or available to the device.” (EX-1007, Abstract, ¶24.) “In response to authenticating, a user may access restricted files, applications (e.g., applications purchased by the user), or settings (e.g., application settings such as contacts or saved game profile).” (EX-1007, Abstract.) Fadell further teaches that a user can store “media data (e.g., music and video files)” in its storage. (EX-1007, ¶24.) Fadell does not detail the type of access but a POSITA would have understood Fadell applies to standard types of data access such as read access and write (update) access. (EX-1003, ¶209.)

This level of access control is explained by Moran. Specifically, in a device secured through authentication, the storage “is in communication with access control device 16, such that any attempts to access data” stored in the storage “must pass through access control device 16” which performs authentication. (EX-

1008, 6:59-63). Preferably, the CPU “must send the command” (e.g., read/write command) “to access control device 16, which then determines if such access should be granted and the data read” from storage. (EX-1008, 6:67-7:3) As stressed by Moran “more preferably, data can only be read from, **and written to**” the data storage through the access control device performing authentication. (EX-1008, 7:3-5) A POSITA would have understood Fadell’s data access restriction processing operates in the same manner. (EX-1003, ¶210.) Accordingly, as taught by Moran, in a system protected by biometric authentication like that of Fadell-Moran, any request by the processor to read from or write to protected data must go through the integrated authentication unit performing user authentication. (EX-1003, ¶211.)

Thus, because all access (read and write) is secured by the biometric authentication process in the combined device of Fadell and Moran, including, e.g., requests by the user to store new data (music/video files) or alter previously stored data (e.g., application settings), “*the processor is configured to securely update the user’s data and documentation files.*” (EX-1003, ¶212.)

F. Claim 19

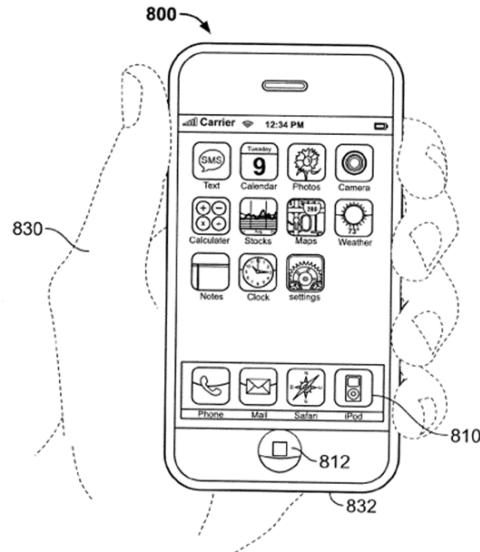
The Fadell-Moran combination discloses that the apparatus further comprises “*at least one of a group of units including a cellular modem and a flat*

display, and a touch screen for communication with the processor.” (EX-1003.

¶¶213-215.)

As discussed above for claims 4 and 10, Fadell’s communications circuitry 108 supports cellular network protocols including, e.g., “GSM, AMPS, GPRS, CDMA, ... or any other suitable cellular network or protocol.” (EX-1007, ¶33.) A POSITA would have understood a device supporting a cellular protocol includes a cellular modem, since modulation and demodulation is a necessary step when communication data through any RF network, including a cellular network. (*See, e.g., EX-1030, 6-8 (describing general RF transmitter/receiver architecture); EX-1029, 7:36-56; EX-1003, ¶214.)*

Fadell’s “electronic device 100 may include any suitable input mechanism, such as for example, a button, keypad, dial, a click wheel, or **a touch screen**” and Fadell’s touch screen can be a **flat display** as shown in Figure 8B, reproduced below. Thus, the Fadell-Moran combination discloses each of the recited “*units*” and renders claim 19 obvious. (EX-1003, ¶215.)



Fadell, Figure 8B

V. GROUND 2: Fadell-Moran-Rosenblatt Combination Renders Obvious Claims 15 and 18

Fadell's communication circuitry includes a “*wireless transceiver module*” supporting numerous protocols including Wi-Fi (e.g., a 802.11 protocol), Bluetooth™, radio frequency, and cellular. (EX-1007, ¶33.) Fadell does not disclose that its device is “*configured to communicate with any of a group of external devices including RF operated credit card readers, ATM machines, and remotely operated electronic locks gates and doors opener using RFID based techniques*” [15]. Rosenblatt discloses this missing feature.

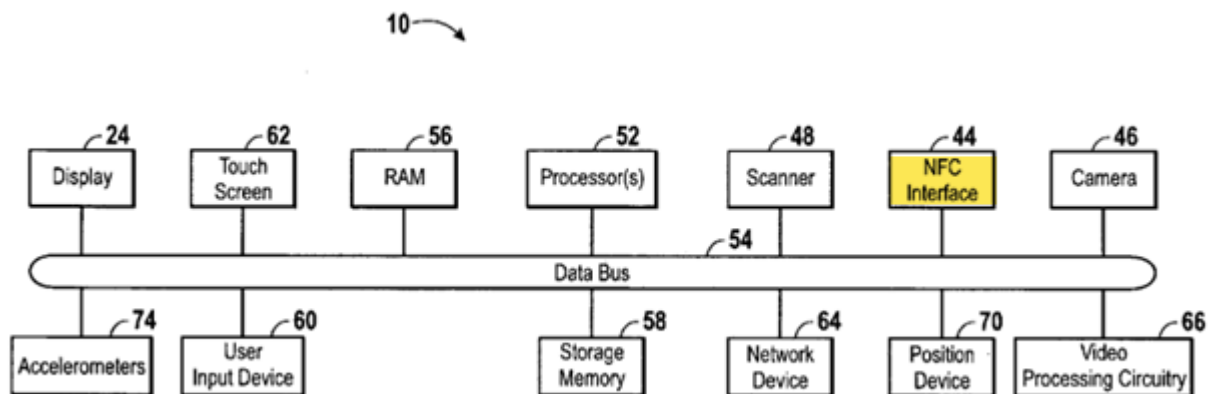
Additionally, neither Fadell nor Moran discloses a device comprising “*an integrated GPS module in communication with the processor to precisely locate the geographical position of the apparatus*” [18]. As acknowledged by the '875 patent, integration of GPS modules within wireless devices was well-known. (EX-

1001, 16:58-60 (noting GPS was “becoming a very common module in most smart phones”).) This feature is likewise disclosed by Rosenblatt. (EX-1003, ¶¶216-217.)

A. Overview of the Combination

1. Rosenblatt

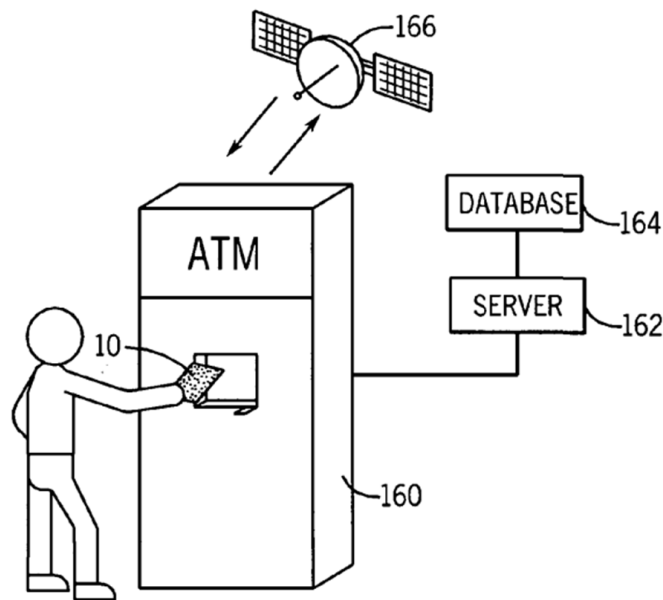
Rosenblatt describes a device 10 having near field communication (NFC) device 44 that “retrieve[s] information from tags having radio frequency identification (RFID) circuitry.” (EX-1010, ¶41, Figure 3.) That is, NFC is a “*RFID-based technique*” for communication between devices. Rosenblatt’s device further includes “a positioning device 70 used to determine a user’s geographical position” through “the global positioning system (GPS) implemented using satellite communications” (EX-1010, ¶55.)



Rosenblatt, Figure 3

Rosenblatt describes transactions between a device and transaction terminal, such as an ATM, using NFC. (See, e.g., EX-1010, ¶¶63, 71.) Specifically, “once the device 10 has initiated communications for transactions with the transaction

terminal 130”, e.g., an ATM as illustrated in Figure 9B, the device is authenticated “based on the location of the device 10” determined by the integrated positioning device 70. (EX-1010, ¶¶71.) After successful authentication, the device “automatically select[s] a card” and after an additional authentication measure (e.g., PIN entry), “the user may gain access to the account and may conduct a transaction with the terminal 130” (e.g., a withdrawal). (EX-1010, ¶¶76, 79.)

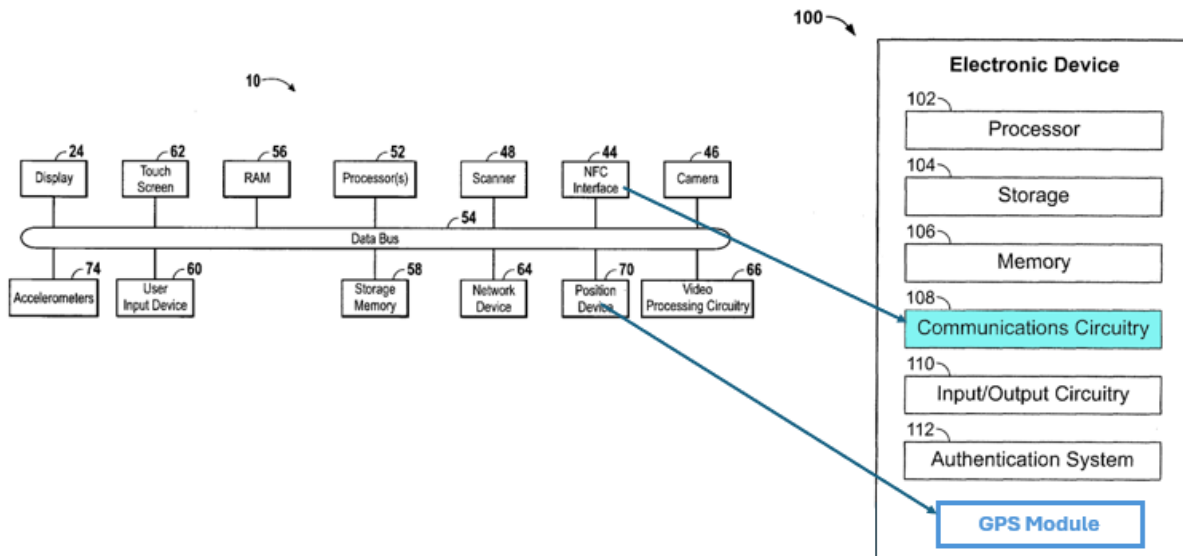


Rosenblatt, Figure 9B

2. Motivation to Combine

A POSITA would have been motivated to combine: (1) Rosenblatt’s teachings regarding use of NFC (RFID) protocol for communicating with an ATM machine to perform financial transactions and (2) Rosenblatt’s teachings regarding an integrated GPS module with the Fadell-Moran device. (EX-1003, ¶223.) For

example, a POSITA would have been motivated to include support for NFC protocol in the device's "*wireless transceiver*" and include a GPS module, as illustrated below. (EX-1003, ¶223.)



Rosenblatt, Figure 3; Fadell, Modified Figure 1

Fadell, Moran, and Rosenblatt are both in the same field of the '875 patent—
“authentication systems and methods to allow access to data and transactions.”
(See EX-1001, 7:47-49; Moran, Abstract; EX-1010, ¶75 (“After the device 10 has
been authenticated, [it] may list a number of accounts []that may be used for the
transaction.”); Fadell, Moran, and Rosenblatt are also reasonably pertinent to
problems addressed by the '875 patent, namely the “need to improve and enhance
the access control capabilities to first securely and efficiently authenticate the
specific user before giving this user access to sensitive personal data files...” (EX-
1001, 4:28-31; EX-1003, ¶¶223-224.)

A POSITA would have been motivated to include a GPS module in the Fadell-Moran device to enable enhanced features and applications which provide added convenience and safety for users and provide revenue opportunities for service providers. (EX-1003, ¶225.) Rosenblatt discloses the GPS module can precisely locate the geographical position of the device. (EX-1010, ¶55 (“The positioning device 70 may provide **information such as longitude and latitude of the device** as well as the devices position relative to landmarks including streets and buildings”).) By enabling the device to determine its precise geographical location-enabled services and be provided, including the location-based authentication process described above and a variety of location-based infotainment services (e.g., maps/directions, tracking, location-based information dissemination such as advertisements, and location-based games). (*See, e.g.*, EX-1034, 85-88.) Additionally, inclusion of GPS in phones was motivated by the FCC’s mandate to provide enhanced emergency services. (*See, e.g.*, EX-1034, 28.)

A POSITA would have also been motivated to include support for NFC in the Fadell-Moran device to enable the device to act as NFC financial card (e.g., debit/credit card), further enhancing the functionality available to a user. (EX-1003, ¶226.) Fadell also discloses communication circuitry which supports “radio frequency systems” and generally “any other communications protocol” (other than those listed). (EX-1007, ¶33.) NFC is a form of RF communication.

Rosenblatt confirms the motivation to use the device as an ATM card, stressing that the “portability of the device 10 makes it particularly well suited to **performing transactions such ...[ATM] transactions**, and purchase transactions.” (EX-1010, ¶57.) A POSITA would understand the ability to use a portable device as a debit or payment card provides added convenience to users. (EX-1003, ¶226.)

Moreover, the combination would merely be a use of known techniques (e.g., using a GPS module and allowing the execution of financial transactions) to improve similar methods (e.g., using a portable electronic device) in the same way (e.g., by allowing Rosenblatt’s GPS module to determine the position of the device). (EX-1003, ¶227)

A POSITA would have had a reasonable expectation of success in the combination and the results of the combination would have been predictable because NFC transceivers and integrated GPS modules were both well-known prior to the ’875 patent. (EX-1003, ¶228; *see, e.g.*, EX-1001, 16:58-60, EX-1034, 28, 184-188; EX-1035, 1:16-20 (describing a cellular phone with NFC capabilities).) Moreover, both references are assigned to the same assignee (“Apple”) and are directed to the same portable electronic device. (*Compare* EX-1007, 1 (“Assignee: Apple Inc.”), *with* EX-1010, 1 (same).) Therefore, a POSITA

would have had an expectation of success combining features designed for Apple wireless devices. (EX-1003, ¶228.)

B. Claim 15

The Fadell-Moran-Rosenblat combination discloses “*an integrated digital data encoder/decoder and a wireless transceiver module in communication with the processor, said integrated digital data encoder/decoder and a wireless transceiver being configured to communicate with any of a group of external devices including RF operated credit card readers, ATM machines, and remotely operated electronic locks gates and doors opener using RFID based techniques.*” (EX-1003, ¶¶229-233.)

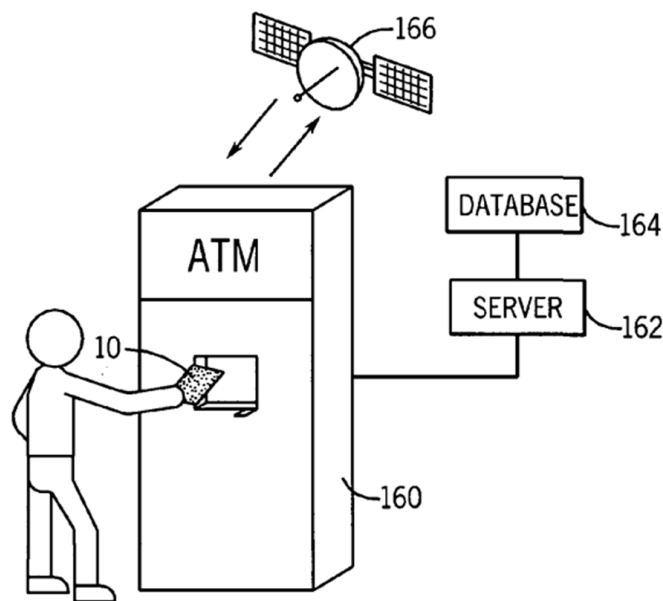
As discussed in §V.A.2, the Fadell-Moran-Rosenblat combination includes support for an NFC interface 44 (“*wireless transceiver module*”) in the communication circuitry of device, as taught by Rosenblatt. (See, e.g., EX-1010, ¶41.) The Fadell-Moran-Rosenblatt combination teaches or suggests that the communications circuitry includes an “*integrated digital data encoder/decoder*” in at least 2 ways. First, a POSITA would have understood the NFC transceiver requires an encoder/ decoder to communicate with another NFC device. (See, e.g., EX-1032, ¶¶23-24; EX-1027; EX-1028.) The inclusion of an encoder/decoder in a wireless device, to the extent not inherent, would have been well-known and commonplace to a POSITA. (EX-1003, ¶230.) Second, Rosenblatt teaches the

device uses “one or more cryptographic protocols” (EX-1010, ¶58) and uses an encryption key to “encrypt communications from the device 10 to the transaction terminal.” (EX-1010, ¶69.) That is, the device in the combination includes an encoder/decoder to encrypt/decrypt communication. (EX-1003, ¶¶229-230.) Thus, the Fadell-Moran-Rosenblatt combination teaches or suggests “*an integrated digital data encoder/decoder and a wireless transceiver module*” that communicate “*using RFID base techniques.*” (EX-1003, ¶230.)

The encoder/decoder and wireless transceiver which are part of the device’s communication circuitry communicate with processor 102. (EX-1007, ¶40 (“[E]lectronic device 100 may include a bus operative to provide a data transfer path for transferring data to, from, or between control processor 102” and communications circuitry 108.) Thus, the combination discloses “*an integrated digital data encoder/decoder and a wireless transceiver module in communication with the processor.*” (EX-1003, ¶231.)

Fadell contemplates use of its device in financial transactions, explaining that storage 104 stores a user’s credit card information, which Fadell characterizes as “transaction information data.” (EX-1007, ¶31 (Storage 104 stores “transaction information data (e.g., information such as credit card information)”)).) Fadell does not provide any details regarding how a financial transaction using its stored cards are performed. Rosenblatt discloses use of a device to “wirelessly transfer and

receive ... sensitive or personal information, such as **the information to conduct a financial transaction.**” (EX-1010, ¶5, *see also* EX-1010, ¶31 (“The present disclosure is directed to techniques for providing security **for wireless communications, including conducting a financial transaction, using a portable electronic device.**”).) Rosenblatt describes an exemplary transaction between a device and transaction terminal, such as an ATM, using NFC. (*See, e.g.*, EX-1010, ¶¶63-79, Figure 9B; §V.A.1.)



Rosenblatt, Figure 9B

Accordingly, the Fadell-Moran-Rosenblatt combination discloses “*an integrated digital data encoder/decoder and a wireless transceiver module in communication with the processor*” that are “*configured to communicate*” with at least an “*ATM machine*” “*using RFID-based techniques.*” (EX-1003, ¶¶232-233.)

C. Claim 18

As discussed in §V.A.2, the device in the Fadell-Moran-Rosenblatt combination includes an integrated GPS module, as taught by Rosenblatt. (EX-1010, ¶55 (“The device 10 may also include a positioning device 70 used to determine a user's geographical position.”).) Rosenblatt’s GPS module can precisely locate the geographical position of the device, e.g., by “provid[ing] **information such as longitude and latitude of the device** as well as the devices position” on a map.” (*Id.*)

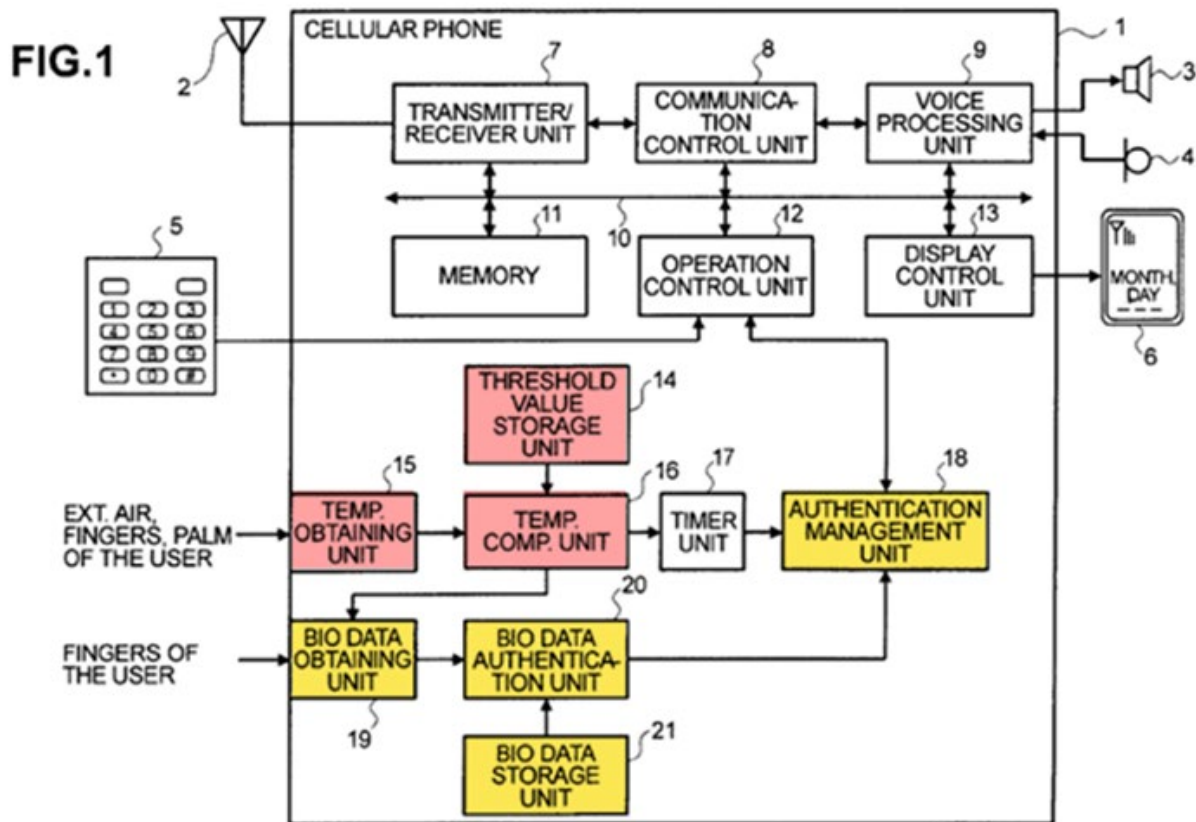
Thus, the Fadell-Moran-Rosenblatt combination discloses “*an integrated GPS module in communication with the processor to precisely locate the geographical position of the apparatus.*” (EX-1003, ¶¶234-236.)

VI. GROUND 3: Kohinata-Mizusawa Combination Render Obvious Claims 1 and 4

A. Overview of the Combination

1. Kohinata

Kohinata describes a cellular phone “capable of managing a variety of personal data related to the owner of the phone.” (EX-1009, 1:16-17; *see also*, EX-1009, 2:30-59.) Kohinata’s phone includes an authentication module having the following set of “functional units” (each shaded yellow): biodata obtaining unit 19, biodata authentication unit 20, biodata storage unit 21, and authentication management unit 18. (EX-1009, 5:41-6:29.)



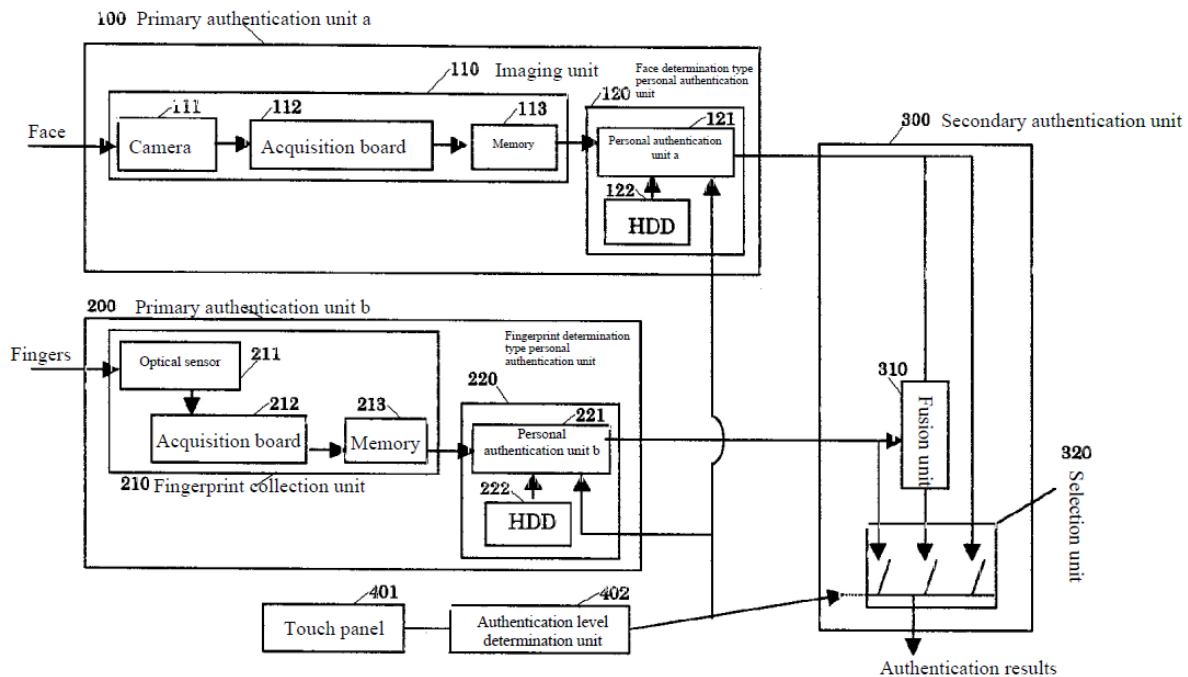
Kohinata, Figure 1

Kohinata's cellular phone also includes a "use detection module" having the following set of functional units (each shaded red): threshold value storage unit 14, temperature obtaining unit 15, and temperature comparator unit 16. (EX-1009, 4:29-5:40.)

2. Mizusawa

Mizusawa provides a personal authentication device (Figure 1, below) having two "primary authentication means", facial authentication and fingerprint authentication, and a "secondary authentication means that finally authenticates an individual." (EX-1012, ¶7.) The secondary authentication unit 300 includes fusion

unit 310 that “merges the authentication results” from both primary authentication units, “thereby authenticating the individual with a higher accuracy than if each authentication was performed separately.” (EX-1012, ¶20.)



Mizusawa, Figure 1

3. Motivation to Combine

A POSITA would have been motivated to combine Mizusawa’s teachings regarding flexible, multi-biometric authentication techniques with Kohinata’s cellular phone. (EX-1003, ¶349.) For example, Kohinata discloses an authentication module supporting fingerprint authentication. (EX-1003, ¶349.) A POSITA would have been motivated to add Mizusawa’s facial authentication to

the authentication module and to combine Mizusawa's secondary authentication teachings with Kohinata's authentication management unit within the authentication module. (EX-1003, ¶249.)

Mizusawa expressly motivates the combination, noting when “authentication method is fixed to one,” balancing authentication, accuracy, and burden the person authenticated is not always possible. (EX-1012, ¶5.) A POSITA would have therefore been motivated to use Mizusawa's flexible multi-modal biometric authentication which allows the device to set an authentication level based on requested user action. That is, actions requiring less security require only as single biometric authentication whereas more secure actions (e.g., financial transactions) use multi-modal authentication. (EX-1003, ¶250.) Moreover, Mizusawa's goal of “minimize[ing] the burden” on the authenticated person while maintaining the requisite authentication accuracy (EX-1012, ¶6) is consistent Kohinata's goal to provide an “easy to use” cellular phone with “a sufficient degree of safety preventing unauthorized use” with “a minimum degree of required authentication” that is “not perceived by the user” (EX-1009, Abstract; EX-1003, ¶251.)

A POSITA would have been further motivated to use Mizusawa's multi-modal biometric authentication to improve reliability. The limitations of single biometric systems such as noisy input data, poor fingerprint ridge quality, improperly maintained sensors, unfavorable ambient conditions, and non-

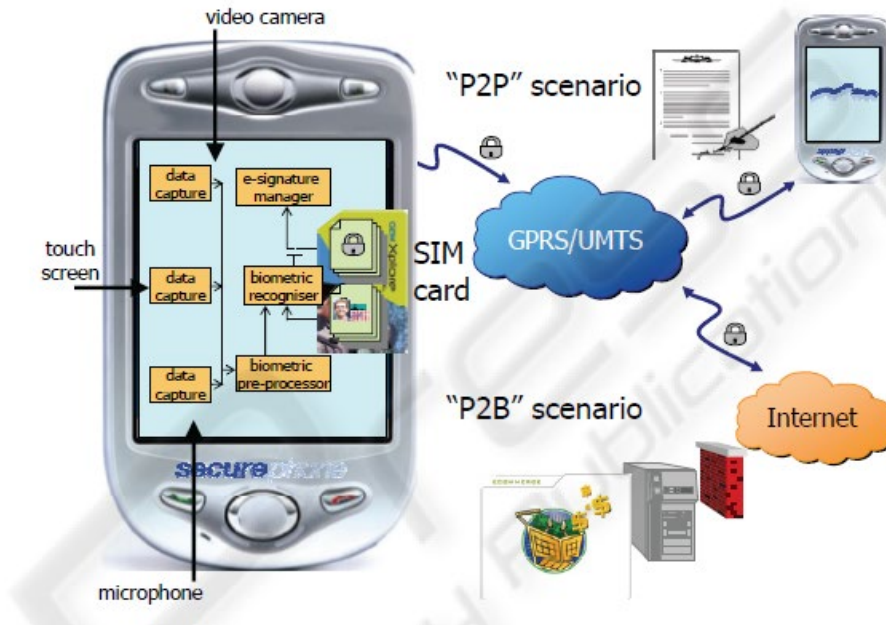
distinctiveness were well known. (EX-1006, 14.) A POSITA would have understood the use of multiple biometric modalities (e.g., face and fingerprint) provides more reliable security due to the user of independent pieces of evidence. (EX-1003, ¶252.)

A POSITA would also have been motivated to include Mizusawa's multi-modal authentication to enhance security for specific operations. (EX-1003, ¶253.) Kohinata discloses a cellular phone "capable of managing a variety of personal data related to the owner" and offering "functions equivalent to the cash and credit cards." (EX-1009, 1:16-20.) The financial risks from unauthorized access to a user's credit or debit card would have motivated a POSITA to provide strong security and would have been led to Mizusawa's multi-modal biometric authentication which provides heightened security with minimal user burden. (EX-1003, ¶253.)

Finally, the combination applies a known technique (Mizusawa's facial authentication unit and authentication level determination) to a known device (Kohinata's cellular phone) ready for improvement to yield predictable results (Kohinata's cellular phone selectively performing authentication based on two biometric parameters). (EX-1003, ¶254.)

A POSITA would have had a reasonable expectation of success and the resulting combination would have been predictable because integrating multi-

biometric authentication measures into cellular phones was well-known long before the '875 patent. (EX-1003, ¶255.) For example, a 2006 SecurePhone prototype, illustrated below, used both facial authentication and voice authentication for user authentication. (EX-1026, 11.)



SecurePhone, Figure 1

Kohinata and Mizusawa are both in the same field of the '875 patent—“authentication systems and methods to allow access to data and transactions.” (See EX-1001, 7:47-49; EX-1009, 2:30-35; EX-1012, ¶7.) Kohinata and Mizusawa are also reasonably pertinent to the problem addressed by the '875 patent, i.e., enhancing security through biometric authentication. (Compare EX-1001, Abstract, with EX-1009, 7:20-25, and EX-1012, ¶17; EX-1003, ¶256.)

B. Independent Claim 1

1. Preamble [1P]: “Apparatus”

The Kohinata-Mizusawa combination discloses an “*apparatus for storing and managing personal and secured data and documentation files associated with a specific user.*” (EX-1003, ¶¶257-261.)

Kohinata is directed to “technology for maintaining security of cellular phones.” (EX-1009, 1:4-5.) Kohinata’s cellular phone, as modified by the teachings of Mizusawa, is an “*apparatus.*” (EX-1003, ¶258.)

Kohinata’s cellular phone stores “*personal and secured data and documentation files associated with a specific user.*” Kohinata’s memory 11 stores the user’s “classified telephone directory, personal schedule data, transmitted and received mails, and data such as of automatic answering machine.” (EX-1009, 3:49-54.) Personal schedule data is an example of both “*personal data*” and “*documentation files*” associated with the user. (EX-1003, ¶259; EX-1025 (Microsoft), 211.) The user’s transmitted and received mail are also examples of “*personal data.*” (EX-1003, ¶259.) This data is “*secured*” because access requires authentication, as discussed further below.

Kohinata’s cellular phone “*manag[es]*” access to this “*personal and secured data and documentation files associated with a specific user*”: “cellular phone is capable of **managing** a variety of personal data related to the owner of the phone”

(EX-1009, 1:16-18) and “prevent[s] unauthorized use by conducting a minimum degree of required authentication operation” (EX-1009, Abstract). If personal authentication fails, Kohinata’s “cellular phone is limited to receiving a call only, preventing the unauthorized use by the third person.” (EX-1009, 10:12-16; *see also* EX-1009, 2:30-59; EX-1003, ¶260.)

2. Integrated Biometric Sensors [1A]

The Kohinata-Mizusawa combination discloses “*a plurality of biometric sensors for reading a plurality of personal biological biometric identification parameters of the user holding the apparatus, said plurality of biometric sensors being integrated within the apparatus.*” (EX-1003, ¶¶262-270.)

As discussed in §VI.A.3, the Kohinata-Mizusawa combination combines Mizusawa’s multi-biometric authentication with Kohinata’s authentication module. That is, as taught by Mizusawa, the cellular phone includes at least two authentication units, each supporting different type biometric authentication that use biometric data collected from the biometric sensors discussed below.

Fingerprint sensor: Kohinata’s cellular phone includes a biodata obtaining unit 19 (e.g., a small imaging device such as a CCD camera) that obtains “data such as feature quantity inherent in the fingerprint from a particular finger of the user.” (EX-1009, 5:43-51.) Like Kohinata, Mizusawa’s fingerprint collection unit 210 “captures the fingerprint of the person to be authenticated” (EX-1012, ¶17)

and includes optical sensor 211, acquisition board 212, and memory 213 (EX-1012, ¶18).

The user's fingerprint is a "*personal biological identification parameter of the user*" and therefore the biodata obtaining unit/collection unit is a "*biometric sensor[] for reading [] personal biological biometric identification parameters of the user holding the apparatus*" which is "*integrated within*" the cellular phone. (EX-1003, ¶¶263-266.)

Facial feature sensor: In Mizusawa's facial feature authentication, imaging unit 110 "captures a facial image" of the person to be authenticated (EX-1012, ¶14) and includes camera 111, acquisition board 112, and memory 113 (EX-1012, ¶15). A POSITA would have understood the user holds the device in a "selfie-style" position when this photo is captured. (EX-1003, ¶267.) The user's facial feature is a "*personal biological identification parameter of the user*" and therefore the imagining unit/camera is a "*biometric sensor[] for reading [] personal biological biometric identification parameters of the user holding the apparatus*" which is "*integrated within*" the cellular phone. (EX-1003, ¶267.)

Mizusawa further teaches that one authentication unit may be an "authentication unit that uses a voice print or an iris to authenticate an individual." (EX-1012, ¶21)

Kohinata's cellular phone, as modified by Mizusawa, discloses "*a plurality of biometric sensors*" because the combination uses "multiple primary authentication means that use different authentication methods," as taught by Mizusawa. (EX-1003, ¶¶268-269.) That is, the cellular phone requires authentication of both fingerprint and facial recognition before granting access to specific resources. (EX-1003, ¶269.)

3. Life Signs Detector [1B]

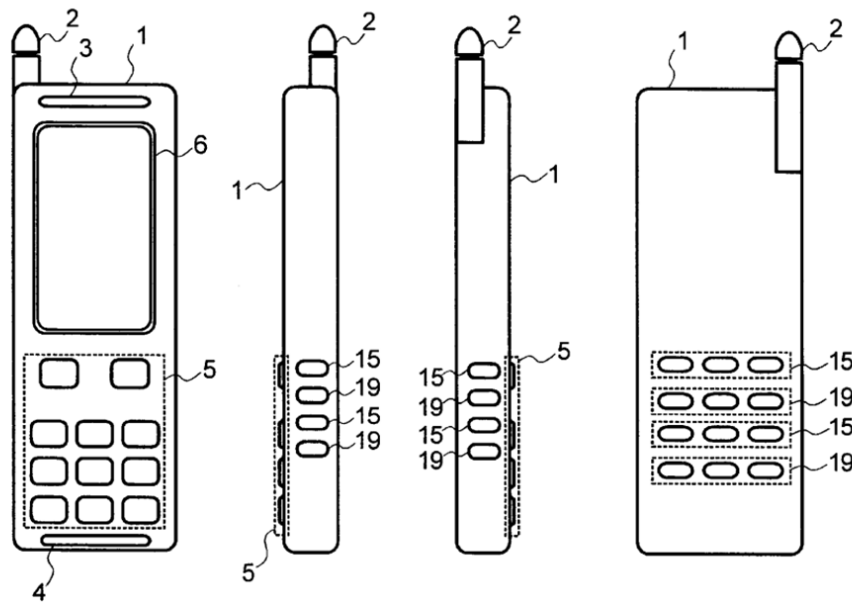
The Kohinata-Mizusawa combination discloses "*at least one life signs detector integrated within the apparatus, said life signs detector being configured to measure and record at least one of said user's life sign parameters.*" (EX-1003, ¶¶271-275.)

Kohinata's cellular phone includes a "use detection module" judging "the state of contact to the user by measuring temperature" (EX-1009, 2:56-57) and includes temperature obtaining unit 15 and temperature comparator unit 16. (EX-1009, Figure 1.) Temperature obtaining unit 15 alone or in combination with comparator unit 16 is a "*life signs detector.*" (EX-1003, ¶272.)

Temperature obtaining unit 15 "measur[es] the body temperature of the user" when touched by the user's palm or fingers. (EX-1009, 4:35-38.) The user's temperature is a "*life sign parameter*" of the user. In operation, stored threshold temperatures "are compared with the temperature detected." (EX-1009, 7:14-17.)

A POSITA would have understood that to perform the comparison, the measured temperatures are recorded. (EX-1003, ¶273.) That is, the “*life signs detector*” of the Kohinata-Mizusawa combination measures and records the “*user’s life signs parameter*” (vital sign), at least temporarily, so it can be compared against values indicative of a “live individual.” (EX-1003. ¶273.)

The sensors of temperature obtaining unit 15 are “on the surface of the cellular phone.” (EX-1009, 4:31-33.) For example, the temperature obtaining units 15 are “the right side portion of the housing” (Figure 4B), “the left side portion thereof” (Figure 4C), and “on the back surface portion” (Figure 4D). (EX-1009, 9:40-54.) Thus, temperature obtaining unit 15 (“*life signs detector*”) is “*integrated within the apparatus.*” (EX-1003, ¶274.)

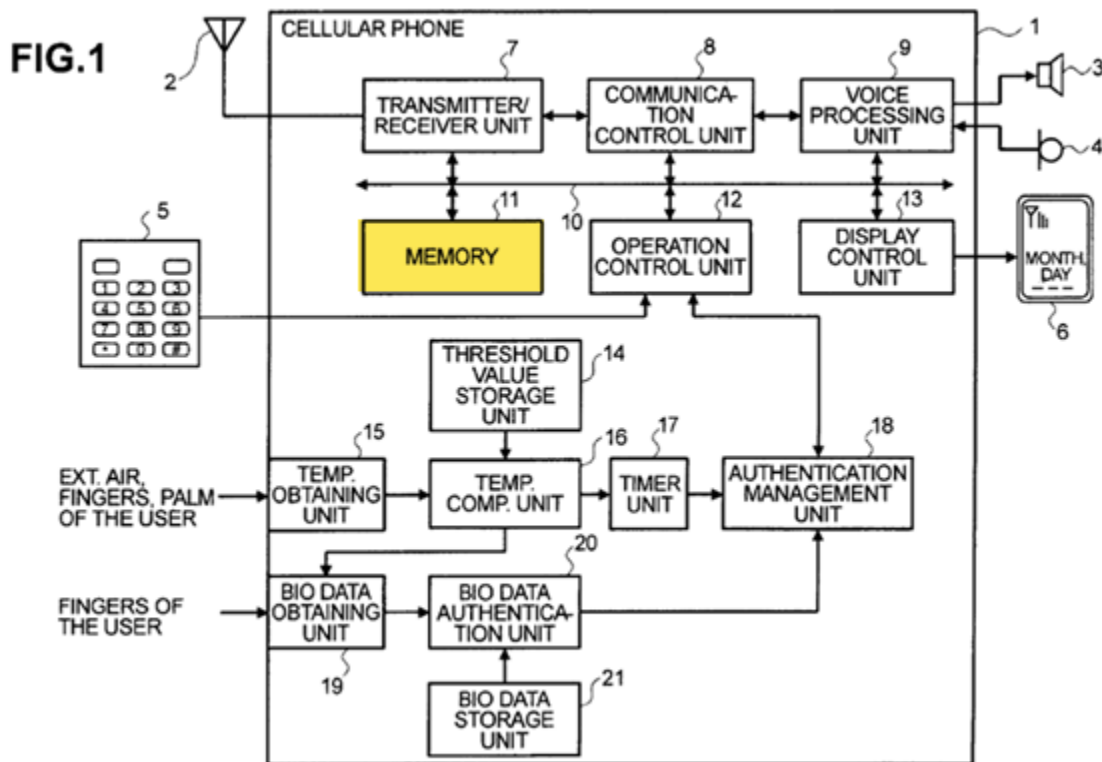


Kohinata, Figures 4A-4D (left to right)

4. First Storage Unit [1C]

The Kohinata-Mizusawa combination discloses “a first storage unit for the storage of said user’s data and documentation files.” (EX-1003, ¶¶276-280.)

Kohinata’s **memory 11** stores a user’s “classified telephone directory, personal schedule data, transmitted and received mails, and data such as of [sic] automatic answering machine,” which are each examples of both “data” and “documentation files” associated with the user. (See §VI.B.1.) Thus, memory 11 performs the function of “storing a user’s data and documentation files” and meets the structure of the “first storage unit” term (memory). (EX-1003, ¶¶277-279.)



Kohinata, Figure 1

Should PO contend “*first storage unit*” is not a means-plus-function term, the Kohinata-Mizusawa combination discloses this limitation for the same reasons. (EX-1003, ¶280.)

5. Authentication Unit [1D]

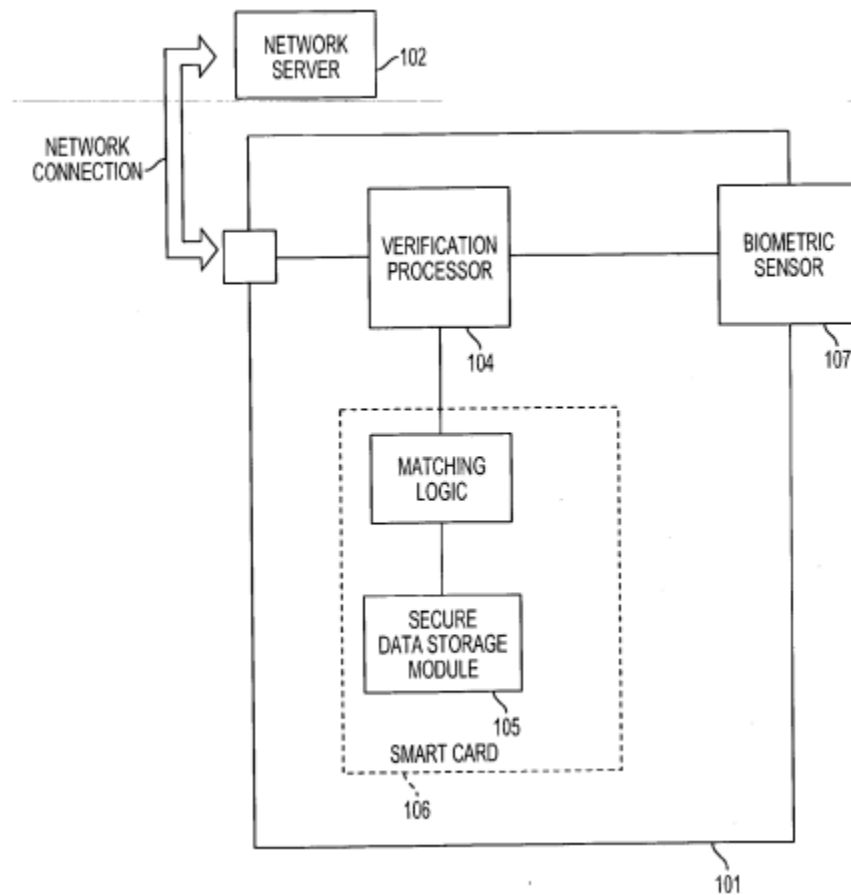
The Kohinata-Mizusawa combination discloses “*an authentication unit comprising a second storage unit, with said second storage unit configured to store a pre-recorded set of personal biological biometric identification parameters uniquely associated with the specific user, wherein said authentication unit is configured to compare the plurality of personal biological biometric identification parameters of the user holding the apparatus with the pre-recorded set of personal biological biometric identification parameters stored in said second storage unit.*” (EX-1003, ¶¶281-307; §III.E.3 (means-plus-function construction of “authentication unit”; §III.E.2 (means-plus-function construction of “second storage unit”).)

a) Authentication Module

As discussed above (§VI.A.3), the “authentication module” of the combined device of Kohinata and Mizusawa includes multiple biometric authentication (e.g., a facial and fingerprint) as taught by both Kohinata and Mizusawa) and integrates Mizusawa’s secondary authentication unit teachings (fusion and selection) with Kohinata’s authentication management unit. (EX-1003, ¶283.)

Kohinata does not disclose (or limit) the implementation of its “authentication module.” Should PO contend that the “authentication module” must be a standalone physical component, a POSITA would have been motivated to implement the processing units performing the comparisons and the biometric reference data storage within a separate, physical component, such as a chip (as taught by Moran) or SIM card. (EX-1003, ¶284.) For example, U.S. Publication 2003/0115490 to Russo, et al. (“Russo”), published June 19, 2003, describes and motivates such an arrangement. (EX-1033.)

Russo describes a GSM phone having an integrated SIM card that “provides stored biometric data and processing capabilities for the matching function within a cellular phone.” (EX-1033, Abstract, ¶40, Figure 1 (below).) Russo stresses that “[b]y storing biometric data on the SIM (a type of smart card) and performing the biometric matching process on the SIM, the need to transmit or store biometric data in a way that leaves it available for retrieval or tampering is minimized.” (EX-1033, Abstract, ¶40.)



Russo, Figure 1

The SecurePhone implementation also used multi-biometric authentication and stored its templates in a standalone physical component (SIM card) within the mobile phone. (EX-1026, 11-12; EX-1003, ¶285.)

Thus, in the Kohinata-Mizusawa combination the comparison processor and template storage of the “authentication module” is implemented in a separate hardware unit. (EX-1003, ¶286.)

b) “**pre-recorded set of personal biological biometric identification parameters**”

Both Kohinata and Mizusawa disclose a “*pre-recorded set of personal biological biometric identification parameters.*” (EX-1003, ¶287.) As discussed in §VI.B.2, the Kohinata-Mizusawa combination discloses use of at least two types of biometric authentication and therefore the user must enroll data for each type of biometric being used. That is, the user has a “*set of personal biological biometric identification parameters.*”

Both Kohinata and Mizusawa reference the enrollment process. For example, Kohinata discloses that biodata storage unit 21 “**stores in advance the fingerprint data** obtained from at least one or more fingers of the owner of the cellular phone.” (EX-1009, 5:55-57.) Kohinata teaches enrollment (registering) is “done from a particular application program for effecting various initial settings at the time of purchase or, after the purchase, for only a period of time in which it is authenticated that the user of the cellular phone 1 is its owner.” (EX-1009, 5:65-6:3.) Mizusawa similarly references enrolling biometric data. For example, the facial feature authentication unit includes “facial image data in [an] authentication list **previously recorded** in the HDD 122” (EX-1012, ¶16) and the fingerprint authentication unit includes “fingerprint data in an authentication list **recorded in advance** in the HDD 222.” (EX-1012, ¶19; EX-1003, ¶288-291.)

c) Second Storage Unit

The Kohinata-Mizusawa combination discloses a “*second storage unit configured to store a pre-recorded set of personal biological biometric identification parameters uniquely associated with the specific user.*” (EX-1003, ¶292; §III.E.2 (means-plus-function claim construction).)

As discussed above (§VI.B.5.b)), the authentication module of the Kohinata-Mizusawa combination includes internal storage for the enrolled biometric data of a user. Kohinata discloses that authentication module includes the **biodata storage unit 21** which “stores in advance the fingerprint data obtained from at least one or more fingers of the owner of the cellular phone.” (EX-1009, 5:55-57.) Thus, the user’s enrolled/registered biometric data (“*set of personal biological biometric identification parameters uniquely associated with the specific user*”) are stored in storage unit 21 in advance of authentication processing (i.e., “*pre-recorded*”). (EX-1003, ¶293.)

Mizusawa similarly discloses internal memory (HDD) within an authentication unit storing pre-recorded enrolled biometric data for a user. As discussed above, Mizusawa teaches the authentication units include “facial image data in [an] authentication list previously recorded in the HDD 122” (EX-1012, ¶16) and “fingerprint data in an authentication list recorded in advance in the HDD 222.” (EX-1012, ¶19; EX-1003, ¶294)

Thus, internal memory of the authentication module of the Kohinata-Mizusawa device performs the function of “storing a pre-recorded set of personal biological biometric identification parameters uniquely associated with the specific user” and meets the structure of a “memory.” (EX-1003, ¶295.)

Should PO contend the “*second storage unit*” must be a single physical memory, a POSITA would have been motivated to use the same memory to store the enrolled biometric data for each biometric authentication type included in the authentication module for implementation efficiency. (EX-1003, ¶296.) Such a design would have been well within the skill of a POSITA prior to the earliest possible priority date of the ’875 patent. (EX-1003, ¶296.)

And should PO contend the “*second storage unit*” is not a means-plus-function term, the Kohinata-Mizusawa combination discloses this limitation for the same reasons discussed above. (EX-1003, ¶297.)

d) Authentication Unit

The Kohinata-Mizusawa combination discloses “*an authentication unit*” that “*is configured to compare the plurality of personal biological biometric identification parameters of the user holding the apparatus with the pre-recorded set of personal biological identification parameters stored in said second storage unit.*” (EX-1003, ¶298.)

As discussed in §VI.B.2, the Kohinata-Mizusawa combination includes “*a plurality of biometric sensors for reading a plurality of personal biological biometric identification parameters of the user holding the apparatus.*” As further discussed above, the Kohinata-Mizusawa combination discloses that a “*pre-recorded set of personal biological biometric identification parameters [is] stored in said second storage unit.*”

The collected biometric data is compared against the stored reference biometric data. As explained by Kohinata, “biodata authentication unit 20 **compares** the fingerprint data obtained by the biodata obtaining unit 19 with the fingerprint data stored in the **biodata storage unit 21**, and notifies **the result of comparison** such as in agreement or not in agreement to the authentication management unit 18.” (EX-1009, 6:6-11.) Similarly, Mizusawa discloses “personal authentication unit a 121 **compares** the facial image data of the person to be authenticated acquired by the imaging unit 110 with the facial image data in the authentication list previously recorded in the HDD 122, and authenticates the person to be authenticated.” (EX-1012, ¶16.)

As discussed in §VI.B.2, the authentication module of the combined device requires both facial and fingerprint authentication. Thus, the Kohinata-Mizusawa combination discloses that the authentication module performs the function of “*compar[ing] the plurality of personal biological biometric identification*

parameters of the user holding the apparatus with the pre-recorded set of personal biological biometric identification parameters stored in said second storage unit.”

(EX-1003, ¶¶299-302.)

The Kohinata-Mizusawa combination also discloses the corresponding structure. As discussed above in §§VI.A.3 and VI.B.5, the “authentication module” of Kohinata-Mizusawa’s cellular device includes memories (biodata storage unit 21 and HDD 122) for storing biometric reference templates and functional “units” to compare at least two biological biometric identification parameters with pre-recorded biological biometric identification parameters stored in memory (biodata authentication unit 20 and processor 110). A POSITA would have understood that the comparison is performed by a processor for each type of biometric authentication. (EX-1003, ¶303.)

Thus, the Kohinata-Mizusawa combination discloses the structure of the authentication unit—memory (internal memory 24) and processor (data processor 28) that performs the recited function. And discussed above, should PO argue the “*authentication unit*” must be a standalone hardware/software component, a POSITA would have been motivated to implement the “authentication module” in a SIM card or separate chip. (EX-1003, ¶304; §VI.B.5.a.)

Should PO contend the authentication unit requires as single physical processor, a POSITA would have understood the comparison performed by both

the facial authentication unit and fingerprint authentication unit could be performed by a single processor and would have been motivated to use a shared processor for efficiency in design (and to have a smaller footprint in the assembled device). (EX-1003, ¶305.)

Should PO contend the “*authentication unit*” is not a means-plus-function term, the Kohinata-Mizusawa combination discloses this limitation for the same reasons discussed above. (EX-1003, ¶¶306.)

e) Authentication Unit Comprising the Second Storage Unit

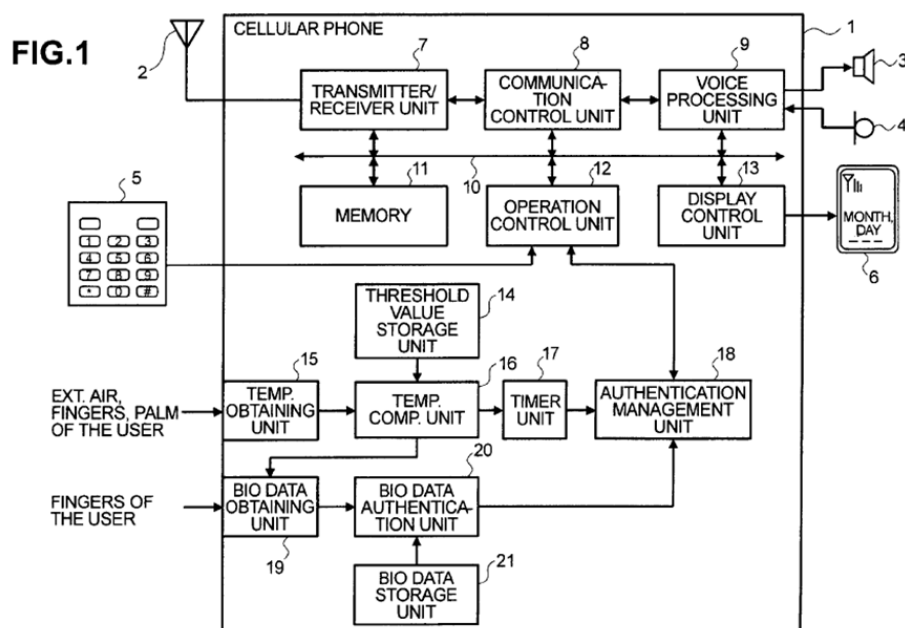
As discussed in the prior section, the authentication module of the Kohinata-Mizusawa combination includes internal memory which is the “*second storage unit*” and a data processor. Thus, for the reasons discussed above, the combination discloses “*an authentication unit comprising a second storage unit.*” (EX-1003, ¶¶307.)

6. Processor [1E]

The Kohinata-Mizusawa combination discloses “*a processor in communication with said plurality of biometric sensors, said first storage unit and said authentication unit.*” (EX-1003, ¶¶308-310.)

Kohinata’s cellular phone includes operation control unit 12 “comprising chiefly a **CPU**.” (EX-1009, 3:57-58, Figure 1 (below).) Control unit 12 “control[s] the communication module and [] execut[es] the application programs depending

upon a direct instruction from the user” (EX-1009, 3:58-60) , the temperature obtaining unit 15 (EX-1009, 4:1-3), and “biodata obtaining units 19, biodata authentication unit 20, biodata storage unit 21 and authentication management unit 18 that constitute the personal authentication module” (EX-1009, 10:44-47). To control these units, the CPU must communicate with them. (EX-1003, ¶¶308-309.)



Kohinata, Figure 1

As shown above, memory 11 and operation control unit 12 “are coupled together through a bus 10, so that the necessary data can be exchanged among them.” (EX-1009, 3:65-67.) And as shown above, control unit 12 is coupled to authentication management unit 18 in the authentication module (“*authentication unit*”).

7. Matching of Personal Biological Biometric Identification Parameters [1F]

The Kohinata-Mizusawa combination discloses “*access to the personal data and documentation files stored in said first storage unit is only enabled after said authentication unit positively matches each of the plurality of personal biological biometric identification parameters of the user holding the apparatus with the pre-recorded set of personal biological identification parameters stored in said second storage unit.*” (EX-1003, ¶¶311-315.)

As discussed in §VI.B.5.d), each authentication unit (e.g., facial authentication unit and fingerprint authentication unit) in the Kohinata-Mizusawa device “*compar[es] the plurality of personal biological biometric identification parameters of the user holding the apparatus with the pre-recorded set of personal biological biometric identification parameters stored in said second storage unit.*”

As discussed in §VI.A.3, the Kohinata-Mizusawa combination combines Mizusawa’s teachings regarding a secondary authentication unit with Kohinata’s authentication management unit 18. In Mizusawa, the authentication results from each unit are “output to the secondary authentication unit”, as taught by Mizusawa. (See EX-1012, ¶¶16, 19.) The secondary authentication unit includes fusion unit which “merges the authentication results” of each authentication unit, “thereby authenticating the individual with a higher accuracy than if each authentication was

performed separately.” (EX-1012, ¶20.) A selection unit then “outputs the results of the fusion unit 310.” (EX-1012, ¶20.)

In Kohinata, the authentication management unit 18 “controls the access to various kinds of data stored in the memory 11.” (EX-1009, 6:17-23.) The results of the authentication (e.g., the results of fusion 310) determine whether the access is granted. (EX-1003, ¶314.) For example, in Kohinata, like in Mizusawa, the authentication results are sent to the authentication management unit 18. When the comparison is successful (data is “in agreement”), the user of the cellular phone is recognized as its owner and when the comparison is not successful (data is “not in agreement”), **“limitation is imposed on the use of the functions with which the cellular phone 1 is provided.”** (EX-1009, 6:6-16; *see also* EX-1009, 6:63-7:11; 11:64-12:12.) That is, in the Kohinata-Mizusawa combination, access to personal data and documentation files stored on the phone is only enabled after a positive result from each authentication unit. (EX-1003, ¶¶312-315.)

8. Critical Level Detection [1G]

In Kohinata, temperature data (“*life sign parameters*”) measured by the temperature obtaining unit 15 (“*life signs detector*”) “are added to the conditions for obtaining the fingerprint data” and in this manner “it is made possible to prevent unauthorized authentication by using a fingerprint that is artificially

reproduced.” (EX-1009, 10:16-20.) That is, Kohinata provides a countermeasure that detects the vital signs of a user—temperature.

Kohinata teaches a comparator unit 16 “compares the temperature data measured by the temperature obtaining unit 15 with the threshold temperatures stored in the threshold value storage unit 14 at regular intervals” to determine whether the phone is being “touched by the user.” (EX-1009, 4:54-63.) When the measured temperature is not within the range of the threshold temperature, authentication is not initiated. (*See, e.g.*, EX-1009, 4:54-63, 7:53-61.) That is, if the detected value is below the lowest point of this range (i.e., is at a “critical level”), the “detector” determines a live person is not present and restricts access to the phone (i.e., “to said user’s personal data and documentation files”) by not starting authentication.

Accordingly, the Kohinata-Mizusawa combination discloses or suggests “*whenever any of said at least one life signs detector detects a critical level of said user measured life sign parameters, the apparatus is configured to prevent access to said user’s personal data and documentation files stored in said first storage unit.*” (EX-1003, ¶¶316-318.)

C. Claim 4

Kohinata describes that “cellular phones are finding diversifying applications, such as a data (packet) communication terminal for carrying out

electronic mails, chatting and internet browsing.” (EX-1009, 1:6-9.) Kohinata also explains the cellular phone receives a call. (EX-1009, 3:24-27 (explaining that “the cellular phone includes ... a speaker ... for letting the user know a call”), 8:29-30 (explaining that “the cellular phone [] is placed in the waiting state to receive a call”).) Thus, Kohinata discloses the cellular phone communicates “*with an external device*” and therefore the communication module performs the function of “communicating with an external device.” (EX-1003, ¶¶319-320.)

To communicate with an external device, Kohinata’s cellular phone includes a communication module having transmitter/receiver unit 7, control unit 8, and voice processing unit 9. (EX-1009, 4:9-28.) Control unit 8 “is constituted by a modulator, a demodulator or a communication protocol processor, and executes the communication protocol processing for modulating the signals from the transmitter/receiver unit.” (EX-1009, 4:15-22.) Thus, Kohinata’s communication module includes a cellular modem, meeting the structure of the “*communication and data connection means*.”

Kohinata’s communication module is “*controlled by and in communication with said processor*.” Kohinata’s operation control unit 12 (“*processor*”) “control[s] the communication module.” (EX-1009, 3:57-58.) Accordingly, in Kohinata, transmitter/receiver unit 7, communication control unit 8, voice processing unit 9, memory 11, operation control unit 12 and display control unit 13

“are coupled together through a bus 10, so that the necessary data can be exchanged among them.” (EX-1009, 3:62-67.)

Thus, the Kohinata-Mizusawa combination discloses “*communication and data connection means for communicating with an external device, said communication and data connection means being controlled by and in communication with said processor.*” (EX-1003, ¶¶319-323.)

VII. GROUND 4: Kohinata-Mizusawa-Rosenblatt Combination Render Obvious Claims 15 and 18

Kohinata’s cellular phone includes a communication module having a transmitter/receiver unit (“*wireless transceiver*”). Kohinata however does not explicitly disclose its device is “*configured to communicate with any of a group of external devices including RF operated credit card readers, ATM machines, and remotely operated electronic locks gates and doors opener using RFID based techniques*” [15]. Rosenblatt, described in §V.A.1, discloses this missing feature. (EX-1003, ¶324.)

Additionally, neither Kohinata nor Mizusawa disclose a device comprising “*an integrated GPS module in communication with the processor to precisely locate the geographical position of the apparatus*” [18]. However, integration of GPS modules within wireless devices was well-known as acknowledged by the ’875 patent. (EX-1001, 16-58-60.) This feature is also disclosed by Rosenblatt. (EX-1003, ¶325.)

A. Motivation to Combine

A POSITA would have been motivated to combine: (1) Rosenblatt’s teachings regarding use of NFC (RFID) protocol for communicating with an ATM machine to perform a financial transaction and (2) Rosenblatt’s teachings regarding an integrated GPS module with the Kohinata-Mizusawa cellular phone. (EX-1003, ¶326.) For example, a POSITA would have been motivated to include support for NFC protocol in the device’s “*wireless transceiver*” and include a GPS module. (EX-1003, ¶326.)

Kohinata, Mizusawa, and Rosenblatt are in the same field as the ’875 patent—“authentication systems and methods to allow access to data and transactions.” (See EX-1001, 7:47-49; EX-1009, 1:12-19; EX-1012, Abstract, ¶7; EX-1010, ¶75 (“After the device 10 has been authenticated, the device 10 may list a number of accounts stored on the device 10 that may be used for the transaction”).) Kohinata, Mizusawa and Rosenblatt are also reasonably pertinent to the problem addressed by the ’875 patent, i.e., enhancing security through biometric authentication. (Compare EX-1001, Abstract, with EX-1009, 7:20-25; EX-1012, ¶7; EX-1010, ¶75; EX-1003, ¶327.)

A POSITA would have been motivated to include a GPS module in the Kohinata-Mizusawa device for the same reasons discussed in §V.A.2, including to enable enhanced features and applications which provide added convenience and

safety for users and provide revenue opportunities for service providers. (EX-1003, ¶328.).

A POSITA would have also been motivated to include support for NFC in the Kohinata-Mizusawa wireless device to enable the device to act as NFC financial card (e.g., a debit and credit card), further enhancing the functionality available to a user. (EX-1003, ¶329.) Kohinata motivates the combination, describing a cellular phone capable of “conducting the settlement” which thereby “offers functions equivalent to the cash and credit cards.” (EX-1009, 1:16-19.) Kohinata however fails to provide details permitting use of its cellular phone for card “settlement” and therefore a POSITA would have been motivated to search for techniques to provide this capability and would have been led to Rosenblatt. (EX-1003, ¶329.) Rosenblatt confirms the motivation for using a phone as a payment card, explaining the “portability of the device 10 makes it particularly well suited to **performing transactions such as automatic teller machine (ATM) transactions**, and purchase transactions.” (EX-1010, ¶57.) A POSITA would understand the ability to use a cellular phone as a debit or payment card provides added convenience to users. (EX-1003, ¶¶329-331.)

Moreover, the combination is further merely the use of known techniques (e.g., using a GPS module and allowing the execution of financial transactions) to improve similar methods (e.g., using a portable electronic device) in the same way

(e.g., by allowing Rosenblatt’s GPS module to determine the longitude and latitude of the device). (EX-1003, ¶332.)

A POSITA would have had a reasonable expectation of success in the combination and the results of the combination would have been predictable because NFC transceivers and integrated GPS modules were both well-known prior to the ’875 patent. (EX-1003, ¶333; *See, e.g.*, EX-1001, 16:58-60, EX-1034, 28, 184-188; EX-1035, 1:16-20 (describing a cellular phone with NFC capabilities).).

B. Claim 15

The Kohinata-Mizusawa-Rosenblatt combination discloses “*an integrated digital data encoder/decoder and a wireless transceiver module in communication with the processor, said integrated digital data encoder/decoder and a wireless transceiver being configured to communicate with any of a group of external devices including RF operated credit card readers, ATM machines, and remotely operated electronic locks gates and doors opener using RFID based techniques.*” (EX-1003, ¶¶334-338.)

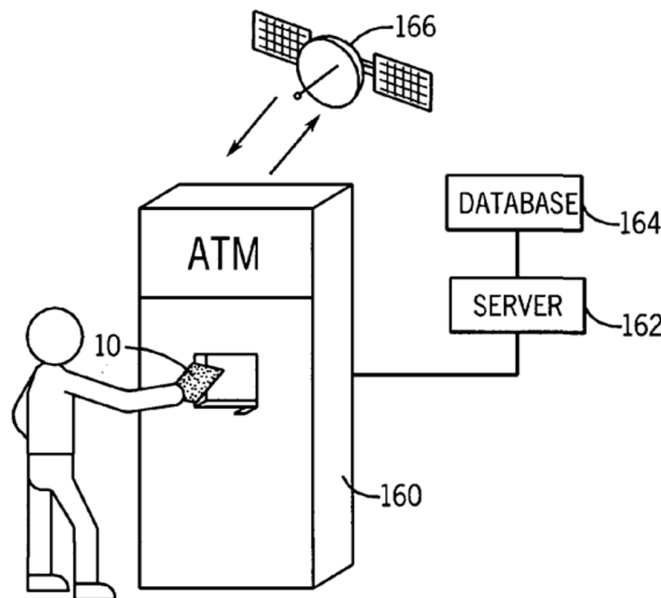
As discussed in §V.A.2, the Kohinata-Mizusawa-Rosenblatt combination includes support for an NFC interface 44 (“*wireless transceiver module*”) in the communication module of Kohinata’s cellular phone, as taught by Rosenblatt. (*See, e.g.*, EX-1010, ¶41.)

The Kohinata-Mizusawa-Rosenblatt combination teaches that the communication module further includes an “*integrated digital data encoder/decoder*.” (EX-1003, ¶335.) Kohinata’s communication module includes transmitter/receiver unit 7 (“*wireless transceiver module*”), control unit 8, and voice processing unit 9. (EX-1009, 4:9-28.) Voice processing unit 9 includes a digital data encoder/decoder: voice processing unit 9 “**decodes** the encoded voice data from the communication control unit 8, converts the digital data into analog signals ... [and] convert[s] ... analog signals into digital data” and “**encode[s]**” the digital data and “input[s the digital data] to the communication control unit 8.” (EX-1009, 4:22-28.) Thus, the Kohinata-Mizusawa-Rosenblatt combination teaches “*an integrated digital data encoder/decoder and a wireless transceiver module*” that communicate “*using RFID base techniques*.” (EX-1003, ¶335.)

As discussed in §VI.A.1, the communication module communicates with “*the processor*” and therefore the “*integrated digital data encoder/decoder and a wireless transceiver module*” in the communication module are also “*in communication with the processor*.” (EX-1003, ¶337.)

Kohinata contemplates use of its device in financial transactions, explaining its cellular phone is “capable of ... **conducting the settlement**” (e.g., debit or credit card payment). (EX-1009, 1:12-19.) Kohinata does not provide any details regarding how a financial (settlement) transaction using its phone is performed.

Rosenblatt discloses use of a device to “wirelessly transfer and receive ... sensitive or personal information, such as **the information to conduct a financial transaction.**” (EX-1010, ¶5, *see also* EX-1010, ¶31 (“The present disclosure is directed to techniques for providing security **for wireless communications, including conducting a financial transaction, using a portable electronic device.**”).) Rosenblatt describes an exemplary transaction between a device and transaction terminal, such as an ATM, using NFC. (*See, e.g.*, EX-1010, ¶¶63-79, Figure 9B; §V.A.1; EX-1003, ¶336.)



Rosenblatt, Figure 9B

Accordingly, the Kohinata-Mizusawa-Rosenblatt combination discloses “*an integrated digital data encoder/decoder and a wireless transceiver module in*

communication with the processor” that are “configured to communicate” with at least an “ATM machine” “using RFID-based techniques.” (EX-1003, ¶338.)

C. Claim 18

As discussed in §VII.A, the Kohinata-Mizusawa-Rosenblatt device includes an integrated GPS module, as taught by Rosenblatt. (EX-1010, ¶55.) Rosenblatt’s GPS module can precisely locate the geographical position of the device, e.g., by “provid[ing] **information such as longitude and latitude of the device** as well as the devices position” on a map.” (EX-1010, ¶55.)

Thus, the Kohinata-Mizusawa-Rosenblatt combination discloses “*an integrated GPS module in communication with the processor to precisely locate the geographical position of the apparatus.*” (EX-1003, ¶¶339-341.)

VIII. Discretionary Denial is Not Appropriate

A. 35 U.S.C. §314(a)

The Board should reach the merits because the Petition presents a compelling unpatentability challenge. (*See* Interim Procedure for Discretionary Denials, 4-5.) The evidence presented in this Petition, “if unrebutted in trial, would plainly lead to a conclusion that one or more claims are unpatentable by a preponderance of the evidence.” (Interim Procedure, 4.)

The median time to trial in the Eastern District of Texas is 21.9 months and the case is scheduled for trial on June 1, 2026. Nonetheless, the district court case is in its early stages and little fact discovery has taken place. In addition, because a

claim construction hearing is not scheduled until December 11, 2025, no claim construction order will issue prior to a decision on institution.

Regardless, to simplify the issues in the pre-institution stage, and in accordance with the Board's precedential decision in *Sotera Wireless, Inc. v. Masimo Corp.*, IPR2020-01019, Paper 12 at 18-19 (PTAB Dec. 1, 2020), Petitioners agree that if IPR is instituted, they will not pursue in the related district court proceeding "any ground that [Petitioners] raised or reasonably could have raised" during the instituted IPR. 35 U.S.C. §315(e).

B. 35 U.S.C. §325(d)

Advanced Bionics Part 1 is not satisfied. This Petition presents new art and new arguments not previously presented to the Office. Moran is the only art of record. However, Moran was not considered in combination with Fadell. Applicant also did not dispute examiner's finding that Moran discloses the "*second storage unit*" limitation. (EX-1002, 192-93.) Besides, this Petition demonstrates how each of Fadell and Kohinata discloses the "*life signs detector*" limitation that applicant argued (and examiner agreed) was missing from the evaluated prior art. (EX-1002, 192-203, 222-23.) Thus, the same or substantially the same art or arguments have not been presented to the Office. *See Caterpillar Inc. v. Wirtgen Am. Inc.*, IPR2022-01278, Paper 12, 43 (PTAB Feb. 7, 2023). Because the first part of the

Advanced Bionics framework is not satisfied, the Board need not consider the second part.

IX. Mandatory Notices

A. Real Party In Interest

The real parties-in-interest are Samsung Electronics Co. Ltd. and Samsung Electronics America, Inc.

B. Related Matters

To the best of Samsung's knowledge, the following is a list of judicial or administrative matter that would affect, or be affected by, a decision in the proceeding:

- *OS-New Horizon Person Computing Solutions, Ltd. v. Samsung Electronics Co. Ltd. et al.*, 2:24-cv-00634-JRG-RSP (E.D. Tex.)

C. Notice of Counsel and Service Information

Pursuant to 37 C.F.R. §§ 42.8(b)(3), 42.8, Petitioners designate the following lead and backup counsel:

Lead Counsel	Back Up Counsel
Lori Gordon (Reg. No. 50,633) GOODWIN PROCTER LLP 1900 N St. N.W. Washington, D.C. 20036 Phone: (202) 346-4000 Fax: (202) 346-4444 Gordon-ptab@goodwinlaw.com	Doug Kline (Reg No. 35,574) GOODWIN PROCTER LLP 100 Northern Avenue Boston, MA 02210 Tel: (617) 570 1000 Fax: (617) 523-1231 dkline@goodwinlaw.com
	Srikanth Reddy (<i>pro hac vice</i> application to be filed) GOODWIN PROCTER LLP 100 Northern Avenue Boston, MA 02210 Tel: (617) 570 1000 Fax: (617) 523-1231 sreddy@goodwinlaw.com
	Naomi Birbach (Reg. No. 67,113) GOODWIN PROCTER LLP 620 Eighth Avenue New York, NY 10018 Phone: (212) 813-8800 Fax: (212) 355-3333 NBirbach@goodwinlaw.com
	Theodoros Konstantakopoulos (Reg. No. 74,155) GOODWIN PROCTER LLP 620 Eighth Avenue New York, NY 10018 Phone: (212) 813-8800 Fax: (212) 355-3333 tkonstantakopoulos@goodwinlaw.com

Petitioners consent to electronic service at the email addresses listed in the table above.

X. Conclusion

IPR is respectfully requested.

Date: February 20, 2025

Respectfully submitted,

/Lori A. Gordon/

Lori A. Gordon (Reg. No. 50,633)
Goodwin Procter LLP
1900 N Street, N.W.
Washington, D.C. 20036
Phone: (202) 346 4435
Gordon-ptab@goodwinlaw.com

Lead Counsel for Petitioner

APPENDIX A – LIST OF CLAIMS

[1P] Apparatus for storing and managing personal and secured data and documentation files associated with a specific user, comprising:

[1A] a plurality of biometric sensors for reading a plurality of personal biological biometric identification parameters of the user holding the apparatus, said plurality of biometric sensors being integrated within the apparatus;

[1B] at least one life signs detector integrated within the apparatus, said life signs detector being configured to measure and record at least one of said user's life sign parameters;

[1C] a first storage unit for the storage of said user's data and documentation files;

[1D] an authentication unit comprising a second storage unit, with said second storage unit configured to store a pre-recorded set of personal biological biometric identification parameters uniquely associated with the specific user, wherein said authentication unit is configured to compare the plurality of personal biological biometric identification parameters of the user holding the apparatus with the pre-recorded set of personal biological biometric identification parameters stored in said second storage unit;

[1E] a processor in communication with said plurality of biometric sensors, said first storage unit and said authentication unit;

[1F] wherein access to the personal data and documentation files stored in said first storage unit is only enabled after said authentication unit positively matches each of the plurality of personal biological biometric identification parameters of the user holding the apparatus with the pre-recorded set of personal biological identification parameters stored in said second storage unit; and

[1G] wherein, whenever any of said at least one life signs detector detects a critical level of said user measured life sign parameters, the apparatus is configured to prevent access to said user's personal data and documentation files stored in said first storage unit.

[4] The apparatus according to claim 1, further comprising:

communication and data connection means for communicating with an external device, said communication and data connection means being controlled by and in communication with said processor.

[7] The apparatus according to claim 4, wherein said external device comprises any one of a group including a remote server, a local server, a host computer, voice or data communication means and a cellular phone.

[10] The apparatus according to claim 4, wherein said communication and data connection means comprises at least one of a group of connection and communication devices including a data interface connector attached to a host computer, a Mini USB, a compatible industrial data interface connector attached to a cellular phone, a near field wireless communication interface, a Bluetooth communication interface, a magnetic reader interface, and a smart card reader based on a contact-less communication interface using induction or RF communication.

[14] The apparatus according to claim 1, wherein the processor is configured to securely update the user's data and documentation files.

[15] The apparatus according to claim 1, further comprising an integrated digital data encoder/decoder and a wireless transceiver module in communication with the processor, said integrated digital data encoder/decoder and a wireless transceiver being configured to communicate with any of a group of external devices including RF operated credit card readers, ATM machines, and remotely operated electronic locks gates and doors opener using RFID based techniques.

[18] The apparatus according to claim 1, further comprising an integrated GPS module in communication with the processor to precisely locate the geographical position of the apparatus.

[19] The apparatus according to claim 1, further comprising at least one of a group of units including a cellular modem and a flat display, and a touch screen for communication with the processor.

CERTIFICATE OF WORD COUNT UNDER 37 CFR §42.24(d)

Pursuant to 37 C.F.R. §42.24(a), Samsung hereby certifies that portions of the above-captioned Petition for *Inter Partes* Review of U.S. Patent No. 8,401,875 in accordance with and reliance on the word count provided by the word-processing system used to prepare this Petition, that the number of words in this paper is 13,995. Pursuant to 37 C.F.R. §42.24(a), this word count is in compliance and excludes the table of contents, table of authorities, mandatory notices under §42.8, certificate of service, certificate of word count, appendix of exhibits, and any claim listing. This word count was prepared using Microsoft Word.

Date: February 20, 2025

Respectfully submitted,

/Lori A. Gordon/

Lori A. Gordon (Reg. No. 50,633)
Goodwin Procter LLP
1900 N Street, N.W.
Washington, D.C. 20036
Phone: (202) 346 4435
Gordon-ptab@goodwinlaw.com

Lead Counsel for Petitioner

CERTIFICATE OF SERVICE

The undersigned certifies that a true copy of the Petition for *Inter Partes* Review of U.S. Patent No. 8,401,875 together with all exhibits identified in the above Table of Exhibits and Petitioners' Power of Attorney, have been served on the Patent Owner via United States Postal Service Priority Mail Express on the below date, at the correspondence address of record as listed on the Patent Center:

Henry M. Sinai
IP-Partnership
P.O Box 669
Raanana, Israel

*Attorneys for OS-New Horizon Person
Computing Solutions, Ltd.*

Courtesy copies of the foregoing document were served by e-mail on the following counsel of record for Patent Owner in the concurrent litigation:

Francisco A. Villegas
Mark W. Halderman
Damir Cefo
Evan Rosenbaum
VILLEGAS & CEFO LLP
1350 Avenue of the Americas, Floor 2
New York, NY 10019
T: (646) 844-0679
fvillegas@villegascefo.com
mhalderman@villegascefo.com
dcefo@villegascefo.com
erosenbaum@villegascefo.com

Mark McDougall
CALFEE HALTER & GRISWOLD LLP

The Calfee Building
1405 East Sixth Street
Cleveland, Ohio 44114-1607
T: (216) 622-8200
mmcdougall@calfee.com

Deron R. Dacus
THE DACUS FIRM, P.C.
821 ESE Loop 323, Suite 430
Tyler, TX 75701
T: (903) 705-1117
ddacus@dacusfirm.com

*Attorneys for OS-New Horizon Person
Computing Solutions, Ltd.*

Date: February 20, 2025

/Lori A. Gordon/

Lori A. Gordon

Lead Counsel for Petitioner