

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.

Case No. IPR2025-00613
U.S. Patent No. 8,401,875

PATENT OWNER'S PRELIMINARY RESPONSE

TABLE OF CONTENTS

I. INTRODUCTION	1
II. THE ‘875 PATENT	3
A. Overview of the ‘875 Patent.....	3
1. The ‘875 Patent’s Secured Personal Data Storage and Handling System.	6
2. The System Includes Separate, Independent Storage Units for User Data/Files and Pre-Recorded Personal Biological Biometric Identification Parameters.....	9
B. Prosecution History	10
1. Petitioners Mischaracterize the Prosecution History of the ‘875 Patent.....	10
2. Petitioners Overstate the Relevance of the European Counterpart’s Prosecution History.....	11
C. Priority Date.....	12
D. Person of Ordinary Skill in the Art (“POSA”)	13
III. CLAIM CONSTRUCTION.....	13
IV. SUMMARY OF REFERENCES RELIED ON BY PETITIONER	15
A. Fadell (Ex.1007)	15
B. Moran (Ex.1008).....	17
C. Kohinata (Ex.1009).....	20
D. Mizusawa (Exs.1011-1012).....	22
E. Rosenblatt (Ex.1010)	25
V. THE BOARD SHOULD DENY INSTITUTION OF THE PETITION.....	26
A. Petitioners Fail to Establish a Reasonable Likelihood That Any of the Challenged Claims Are Obvious Over Fadell and Moran (Grounds 1-2).....	26

1. The Fadell-Moran Combination Cannot Meet <i>Both</i> the “ <i>Authentication Unit</i> ” and “ <i>Processor</i> ” Limitations of Independent Claim 1.	27
2. A POSA Would Not Have Been Motivated to Combine Fadell and Moran.....	30
B. Petitioners Fail to Establish a Reasonable Likelihood That Any of the Challenged Claims Are Obvious Over Kohinata and Mizusawa (Grounds 3-4)	33
1. The Kohinata-Mizusawa Combination Fails to Disclose the “ <i>Access...Is Only Enabled After Said Authentication Unit Positively Matches Each of the Plurality of Personal Biological Biometric Identification Parameters of the User</i> ” Limitation of Independent Claim 1.	34
2. The Kohinata-Mizusawa Combination Fails to Disclose the “ <i>Authentication Unit Comprising a Second Storage Unit</i> ” Limitation of Independent Claim 1.	38
3. The Kohinata-Mizusawa Combination Fails to Disclose the “ <i>Life Signs Detector</i> ” and “ <i>Whenever Any of Said at Least One Life Signs Detector Detects a Critical Level of Said User Measured Life Sign Parameters</i> ” Limitations of Independent Claim 1.	41
4. A POSA Would Not Have Been Motivated to Combine Kohinata and Mizusawa.	45
VI. CONCLUSION	47

TABLE OF AUTHORITIES

Cases

<i>Axalta Coating Sys., LLC v. PPG Industries Ohio, Inc.</i> , IPR2022-00676, Paper 10 (PTAB Sept. 12, 2022).....	39
<i>Deere & Co. v. David's Dozer V-Loc System, Inc.</i> , IPR2024-01442, Paper 10 (PTAB March 18, 2025)	29, 32
<i>In re Gurley</i> , 27 F.3d 551 (Fed. Cir. 1994).....	32
<i>In re Wesslau</i> , 353 F.2d 238 (CCPA 1965)	39
<i>Intelligent Bio-Sys., Inc. v. Illumina Cambridge Ltd.</i> , 821 F.3d 1359 (Fed. Cir. 2016).....	31
<i>Medtronic, Inc. v. Teleflex Innovations S.A.R.L.</i> , IPR2020-00135, Paper 22 (PTAB June 8, 2020).....	12
<i>Pfizer, Inc. v. Ranbaxy Labs. Ltd.</i> , 457 F.3d 1284 (Fed. Cir. 2006).....	11
<i>Tec Air, Inc. v. Denso Manufacturing Mich. Inc.</i> , 192 F.3d 1353 (Fed. Cir. 1999).....	32
<i>Xerox Corp. et al. v. Bytemark, Inc.</i> , IPR2022-00624, Paper 12 (PTAB Feb. 10, 2023).....	41

Other Authorities

Patent Trial and Appeal Board Consolidated Trial Practice Guide (Nov. 2019)	31
--	----

EXHIBIT LIST

Exhibit No.	Description
2001	<i>OS-New Horizon Personal Computing Solutions Ltd. v. Samsung Electronics Co. Ltd. et al.</i> , No. 2:24-cv-00634-JRG-RSP (E.D. Tex.), Docket Control Order (Dkt. No. 23) (“Docket Control Order”)
2002	<i>OS-New Horizon Personal Computing Solutions Ltd. v. Samsung Electronics Co. Ltd. et al.</i> , No. 2:24-cv-00634-JRG-RSP (E.D. Tex.), Complaint (Dkt. No. 1) (“Complaint”)
2003	<i>OS-New Horizon Personal Computing Solutions Ltd. v. Samsung Electronics Co. Ltd. et al.</i> , No. 2:24-cv-00634-JRG-RSP (E.D. Tex.), Samsung Electronics America, Inc. and Samsung Electronics Co., Ltd.’s Invalidity Contentions dated January 16, 2025 (“Invalidity Contentions”)
2004	<i>OS-New Horizon Personal Computing Solutions Ltd. v. Samsung Electronics Co. Ltd. et al.</i> , No. 2:24-cv-00634-JRG-RSP (E.D. Tex.), Civil Docket (“Docket”)
2005	United States District Courts—National Judicial Caseload Profile for 12-month period ending December 31, 2024; available at https://www.uscourts.gov/data-news/reports/statistical-reports/federal-court-management-statistics (“Federal Court Management Statistics”)

I. INTRODUCTION

Patent Owner OS New Horizon Personal Computing Solutions Ltd.’s (“OSNH” or “PO”) founders developed and patented a highly secured system for storing, accessing, and managing a user’s data and files. The device, called “POMM,” was a data storage and management device that could also serve as a token to access services, including health, insurance, finance, or traditional web-based systems. While PO had several early successes—including discussions with Petitioners themselves regarding PO’s innovation—it was ultimately unable to successfully market its software in the wake of rampant infringement.

OSNH’s U.S. Patent 8,401,875 (“the ‘875 Patent”) is directed to systems and devices for securing a user’s personal data, solving security, authentication, and access deficiencies in prior art systems. The claimed systems and devices include a unique combination of features unknown in the art at the time, including providing a secure hardware and software environment isolated from the mobile device. A key feature that distinguishes PO’s invention from known systems is that the device includes multiple storage units to prevent hackers from accessing sensitive information. The device also includes multiple biometric sensors for authentication and a life signs detector for preventing access to a user’s data if a critical level of a user’s life signs parameters is detected. The Patent Office agreed, awarding OSNH the ‘875 Patent.

Petitioners Samsung Electronics Co. Ltd. and Samsung Electronics America, Inc. (“Samsung” or “Petitioners”) Grounds in the Petition (“Pet.”) rely primarily on two combinations of prior art references—Fadell (Ex.1007) in combination with Moran (Ex.1008) in Grounds 1-2 and Kohinata (Ex.1009) in combination with Mizusawa (Exs.1011-12) in Grounds 3-4. These references, however, fail to disclose, alone or in combination, numerous limitations of claim 1 of the ‘875 Patent, from which all the other claims challenged in the Petition (claims 4, 7, 10, 14-15, and 18-19) (collectively with claim 1, the “Challenged Claims”) depend. Moreover, the architecture of the systems disclosed in each of these references are such that a person of ordinary skill in the art would not have combined them in the manner proposed by Petitioners.

Petitioners’ proposed Fadell-Moran combination, for example, cannot simultaneously satisfy both the “authentication unit” and “processor” claim limitations. Petitioners’ attempt to fix one admitted deficiency in Fadell (*i.e.*, Fadell’s lack of a “second storage unit”) by incorporating Moran’s access control device creates another, equally fatal deficiency (*i.e.*, a combined system with a processor that is no longer “in communication with” the first storage unit, as claimed). Petitioners’ Kohinata-Mizusawa combination—which purportedly incorporates Mizusawa’s facial authentication and secondary authentication unit in Kohinata’s authentication module—fares no better. The combination fails to

disclose the required “authentication unit comprising a second storage unit,” “access” after “positively matching” each of the plurality of measured biometric parameters with stored reference parameters, and “life signs detector” limitations of the ‘875 Patent’s claims.

In sum, the Petition fails to provide a reasonable likelihood that any of the Challenged Claims of the ‘875 Patent are unpatentable over any of Petitioners’ Fadell-Moran (Grounds 1-2) or Kohinata-Mizusawa (Grounds 3-4) combinations. Accordingly, the Board should respectfully deny institution of this proceeding.

II. THE ‘875 PATENT

A. Overview of the ‘875 Patent

The ‘875 Patent is directed to systems and devices for accessing, storing, and managing highly secured personal data. Ex.1001, Abstract, 1:14-32. The invention integrates multiple components to ensure security, privacy, and portability, solving deficiencies in prior systems that lacked adequate security, user authentication, and reliable access to personal data and files. Unlike prior solutions, the ‘875 Patent discloses integrated systems and devices uniquely associated with a user, enabling secure data storage and communication with external service providers.

Prior to the ‘875 Patent, there was a need for computer systems that provided “higher data throughput and storage capacity, yet keeping the users and

clients personal information in full security and confidentiality.” *Id.*, 1:33-53. Moreover, users desired “new technological solutions and methods to be able to store and easily get access to their own personal data while storing it in small portable devices and through these devices also to be able to download, retrieve and manage most if not all their personal data and daily operational needs.” *Id.*, 1:54-59. Secured systems were thus used to allow users to securely transfer and exchange sensitive and private personal data and information. *Id.*, 1:60-2:4. In order to access such secured data files, users were “usually required to be first recognized and identified by the computerized system as legitimate registered users.” *Id.*, 2:5-9. This process, *i.e.*, “[t]he process of the user being recognized and approved by a computerized system,” is called ***authentication***. *Id.*, 2:14-15.

According to the patent, conventional authentication systems had various limitations. For example, two-factor authentication and/or token generators suffered drawbacks including that the hardware token generators were often lost/stolen and were susceptible to phishing attacks by malicious actors. *Id.*, 2:15-47. Similarly, “a simple password or even one biometric access permit . . . is not enough to ensure that a third party with negative intentions will not be able to get access” to the user data. *Id.*, 3:46-53. The ’875 Patent thus recognized a significant 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 and then after the user being authenticated in a very high level of security and reliability, to be able to safely and securely communicate and exchange the user's personal secured data with other specific authenticated and pre-approved users and especially with a wide spectrum of registered and approved service and dedicated data providers.” *Id.*, 4:28-37.

The inventors of the patent sought to address the needs in the art and the limitations of conventional authentication systems by disclosing and claiming systems and devices for storing and managing personal and secured data and documentation files associated with a user. As explained further below, the device includes, among other things, a first storage unit for storing the user's data and documentation files, biometric sensors for reading a user's personal biological identification parameters, a life signs detector to measure a user's life sign parameters, and an authentication unit including a second storage unit for separately storing a pre-recorded set of personal biological biometric identification parameters uniquely associated with the specific user. *E.g., id.*, 10:10-46, cl.1.

Storing the user's pre-recorded personal biological biometric identification parameters in a second storage unit separate and independent from the first storage unit containing the user's data and documentation files provides improved security and makes it more difficult for malicious actors to access the user's files. *Id.*,

21:58-22:2. These features, in combination with the other claimed features, were not known in the art prior to the invention of the '875 Patent.

1. The '875 Patent's Secured Personal Data Storage and Handling System.

Figure 2 (below) of the '875 Patent is a schematic illustration of an embodiment of the apparatus (100) for secured data communication and storage.

Id., 16:65-17:2.

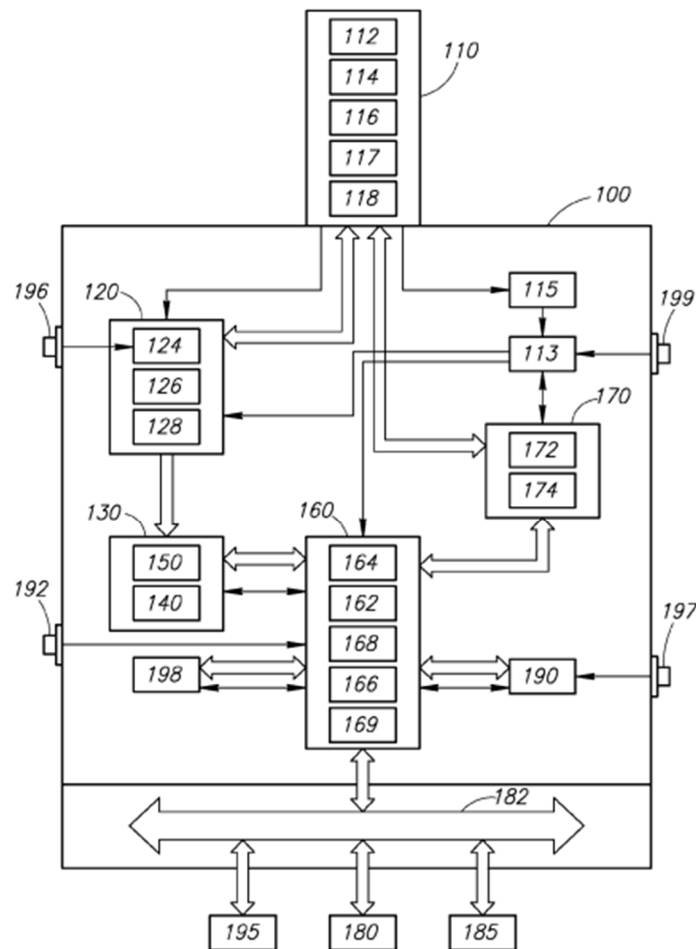


FIG. 2

Id., Fig.2. The apparatus (100) includes a variety of modules with specific functionality and capabilities, including among others:

- **module 110**, “the apparatus host terminals, cellular phones and other accessories connection support (*id.*, 17:23-24);
- **module 120** “containing the apparatus authentication dedicated set of biosensors,” such as sensor 124 for imaging a user’s specific face pattern or eye iris, sensor 126 for imaging and analyzing a user’s fingerprints, and biological life sign detection and measurement sensor 128 for measuring life signs parameters of a user such as heart pulse rate or oxygen content in the user’s blood (*id.*, 17:49-19:5);
- **module 130**, “a hardware and software combined module” that performs the user final authentication by processing the output of the biometric sensors in module 120 and “combining the measured results of the multi sensors tests output to a final ‘go/no-go’ user’s authentication result. *Id.*, 19:6:18. Module 130 includes sub-module 140 for storing the user’s pre-recorded personal biological biometric identification parameters, which are compared to the measured personal biological biometric identification parameters of the user holding the apparatus to authenticate the user. *See id.*, 19:6-18, 20:32-40, cl.1.

- **module 160**, “the central controller and data processing unit,” which is in communication with the biometric sensors, the first storage unit in module 170, and the authentication unit module 130 (*id.*, 20:15-16, cl.1); and
- **module 170**, the “mass memory secured data module,” including secured mass memory sub-module 174 for storing the user’s highly secured personal data and documentation files (*id.*, 20:25-29, 21:52-57, cl.1).

Preferably, the device also includes “a display and touch screen optional **module 185**” and **module 195** with “a cellular modem acting as the apparatus data communication module.” *Id.*, 23:54-24:14 (emphasis added). The device therefore supports a range of implementations, including acting as a standalone device or integration into portable computing or communication devices such as smartphones or similar multifunction hardware.

In operation, to authenticate a user and allow the user to access data and documentation files stored in mass memory sub-module 174 (*i.e.*, the “first storage unit”), the device executes a biometric sensing and testing sequence by measuring the user’s biometric parameters from biometric sensor data and comparing the measurements with the user’s “first registration stored set of bio parameters in unit 140,” *i.e.*, the “second storage unit.” *Id.*, 29:26-30:3. The device also checks the user’s measured life signs sensor output and detects whether the output is at a critical level. *Id.*, 30:8-13, cl.1. If either the biometric sensing and testing sequence

or the critical level life signs check is unsuccessful, the authentication process fails and the user is unable to access the personal data and documentation files stored on the device. *Id.*, 30:4-7, cl.1.

2. The System Includes Separate, Independent Storage Units for User Data/Files and Pre-Recorded Personal Biological Biometric Identification Parameters.

One key feature of the invention disclosed and claimed by the ‘875 Patent is that the device includes separate, independent storage units for the user’s personal data and the user’s stored, pre-recorded reference biometric parameters, underscoring the system’s layered security approach. The “first storage unit” is used to store the user’s personal data and documentation files. *Id.*, cl.1; *see also id.*, 20:24-29, 21:52-22:23. The “second storage unit” is “configured to store a pre-recorded set of personal biological biometric identification parameters uniquely associated with the specific user.” *Id.*, cl.1; *see also id.*, 20:32-36, 29:65-30:3. According to the patent, this architecture improves security and makes it more difficult for malicious actors to “hack” the device and gain access to the user’s secured, personal data and files:

In order to ensure that the encryption process will be highly immune to potential hackers trials to break the encryption code and read the personal highly secured data of the apparatus 100 user, ***the encryption keys required to encrypt and decipher the secured data in sub-module 174 will be stored in a separate special memory partition located in the other memory module 150 under a secured memory***

storage structure and in a way that it will be very hard for the hacker to allocate them and use them when he might try to break the encryption codes of the data stored in the secured data memory sub-module 174. Sub-module 150 is part of the memory and authentication larger module 130.

Id., 21:58-22:2 (emphasis added). This aspect distinguishes the invention from prior art devices and systems, including many of the references relied upon by Petitioner in this proceeding.

B. Prosecution History

1. Petitioners Mischaracterize the Prosecution History of the ‘875 Patent.

While the Petition concedes that the claims of the ‘875 Patent were allowed over a combination of references including Moran (Ex.1008)—one of Petitioners’ primary references in this IPR—Petitioners’ contention that the applicant somehow agreed that the prior art disclosed all but the “life signs detector” limitations of the claims mischaracterizes the prosecution history of the ‘875 Patent. *See* Pet. at 4-5. During prosecution of the ‘875 Patent, the examiner issued a rejection over U.S. Publication 2009/0062887 to Mass in view of Moran. *See* Ex.1002, 161-84. Following that rejection, applicant conducted an examiner interview in which the examiner indicated pending claim 1 (which issued as claim 1 of the ‘875 Patent) would be allowable if it included the “life signs detector” limitations of dependent claim 3. *Id.*, 207, 214. In response, and clearly to expedite prosecution, the

applicant amended claim 1 as suggested, and the examiner then allowed the claims. *Id.*, 192-93, 207. Petitioners' assertion that the applicant somehow conceded the other claim elements were known in the art is thus not supported by the record.

2. Petitioners Overstate the Relevance of the European Counterpart's Prosecution History.

Petitioners also point to the prosecution history of a European counterpart but overstate its relevance here. Fundamentally, subsequent events during the European prosecution, which involve foreign patentability requirements for a foreign application in a foreign jurisdiction, are not dispositive of patentability in the US. *See, e.g., Pfizer, Inc. v. Ranbaxy Labs. Ltd.*, 457 F.3d 1284, 1290 (Fed. Cir. 2006). Moreover, given the multitude of reasons a pending application (US or foreign) may be pursued or abandoned, the fact the European application was rejected over Fadell and at some later time abandoned does not mean Fadell was insurmountable to the European claims. And in any event, because the claims of the European counterpart differ from those of the '875 Patent, the rejection of the counterpart's claims over Fadell has limited, if any, relevance to the claims at issue here. *See, e.g., Ex.1005*, 147-48.

Setting those issues aside, any suggestion by Petitioners that the European examiner's reliance on Fadell somehow proves that Fadell discloses the limitations of the Challenged Claims here is squarely refuted by Petitioners' themselves in this proceeding. Petitioners do not contend that Fadell anticipates the claims. On the

contrary, Petitioners concede that Fadell fails to disclose key limitations, and therefore relies on a combination with Moran to attempt to meet the claim language. Accordingly, Petitioners' implicit suggestion that Fadell discloses the limitations of the '875 Patent's claims because the European counterpart was rejected over Fadell is belied by Petitioners' own arguments and provides no support for institution.

C. Priority Date

The '875 Patent claims priority to U.S. Prov. App. 61/313,145 filed on March 12, 2010. Ex.1001, [60]. Petitioners do not challenge this priority date in the Petition and thus concede the priority date is *at the latest* March 12, 2010 for purposes of this IPR. *See* Pet. at 1.¹ For the purposes of this Preliminary Response

¹ If IPR is instituted, PO intends to antedate the filing date of certain of Petitioners' references by demonstrating conception, diligence, and reduction to practice prior to March 12, 2010. PO recognizes, however, that antedation is fact intensive and that the Board may be reluctant to deny institution on that basis. *See, e.g., Medtronic, Inc. v. Teleflex Innovations S.A.R.L.*, IPR2020-00135, Paper 22 at 11 (PTAB June 8, 2020) (instituting trial because "Petitioner has not had an opportunity to fully consider and address [the antedation] evidence," and that "these factual issues are best resolved after the record is more fully developed").

(“POPR”) only, PO relies upon the priority date used by Petitioners, *i.e.*, March 12, 2010. *See id.*

D. Person of Ordinary Skill in the Art (“POSA”)

The level of ordinary skill in the art as of the priority date for the inventions claimed in the ‘875 Patent is a person with a bachelor’s degree in electrical engineering or computer science, and approximately 3 years of experience working with data storage and communication systems; or a more advanced degree such a master’s or doctorate with proportionally less work experience.

III. CLAIM CONSTRUCTION

For purposes of this POPR, the Board need not construe any terms of the ‘875 Patent. Petitioners, however, argue that several terms require explicit construction. *See* Pet. at 6-9. PO addresses those terms below.

Petitioners contend that the terms “*first storage unit*” (claim 1), “*second storage unit*” (claim 1), “*authentication unit*” (claim 1), and “*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) are means-plus-function terms. *See*

Thus, PO reserves the right to provide evidence and rely on an earlier priority date if trial is instituted in this IPR and/or in any other proceeding.

Pet. at 6-9. Notably, however, when addressing these limitations in the Petition, Petitioner consistently asserts that if these terms are *not* construed as means-plus-function terms, the asserted combinations disclose the limitation “for the same reasons discussed above.” *See, e.g., id.* at 24, 28, 31. Petitioners’ conclusory arguments effectively concede that the proposed means-plus-function constructions are immaterial to the merits of the Petition.

Regardless, PO disagrees that all these terms are means-plus-function terms because a POSA would understand that they recite sufficiently definite structure. As explained further below, however, the prior art references relied upon by Petitioners in this proceeding do not disclose a “first storage unit”, a “second storage unit”, and/or an “authentication unit” ***under any construction of these terms***. Moreover, because Petitioners’ references do not disclose all the required elements of independent claim 1, the Board need not even reach the construction of the “communication and data connection means” term in dependent claim 4. Thus, the Board need not construe any of the terms identified by Petitioners for purposes of institution. In any event, for purposes of this POPR only, PO will simply rely on Petitioners’ proposed constructions for these terms but reserves the right to provide its own constructions if IPR is instituted and/or in any other proceeding.

IV. SUMMARY OF REFERENCES RELIED ON BY PETITIONER

A. Fadell (Ex.1007)

Fadell is directed to implementing authentication systems in electronic devices, such as smartphones or portable computing devices. Ex.1007, Abstract, [0002]. Fadell's primary focus is improving the authentication process for users by embedding biometric and other authentication mechanisms into electronic devices "such that the device authenticates the user quickly and seamlessly." *Id.*, [0004]. The reference describes various mechanisms for restricting access to device resources based on biometric or behavioral authentication. In particular, Fadell discloses a system in which biometric sensors are integrated into the user interface or housing of the device to allow for the passive collection of biometric data during device operation. *Id.*, [0005].

As shown below, Fadell's system architecture includes, in pertinent part, a processor (102), storage (104), and authentication system (112).

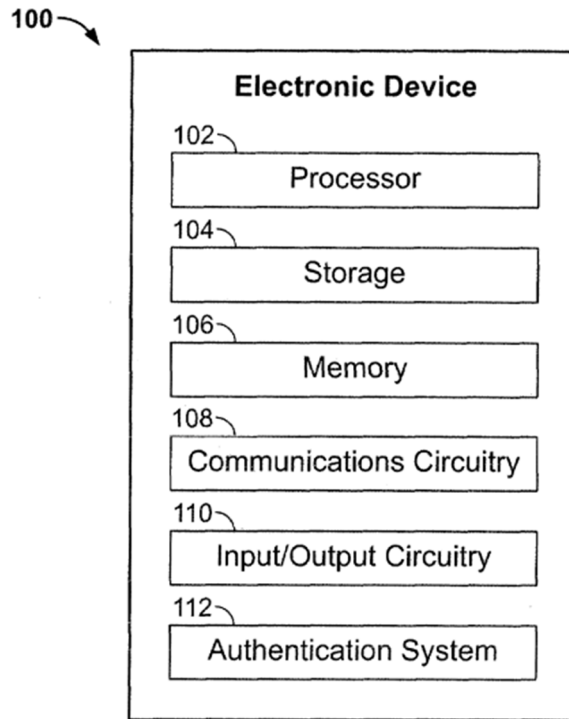


FIG. 1

Id., Fig.1. Fadell indicates that the device includes “a bus operative to provide a data transfer path for transferring data to, from, or between control processor 102, storage 104, . . . [and] authentication system 112.” *Id.*, [0040].

According to Fadell, “[a]uthentication system 112 may include any suitable system or sensor operative to receive or detect an input identifying the user of device 100.” *Id.*, [0039]; *see also id.*, [0025]. Although Fadell discloses a variety of systems and sensors that can be used, Petitioners concede that “*Fadell is silent regarding implementation details of its authentication system.*” *See* Pet. at 13 (emphasis added). This is unsurprising given that Fadell’s focus is not on the

details of the authentication system itself, but rather on incorporating authentication systems into portable devices to improve user convenience.

Moreover, as the Petition admits, Fadell does not disclose a “second storage unit” within the “authentication unit” as required by the claims of the ‘875 Patent. *See* Pet. at 27. In fact, Fadell does not disclose a “second storage unit” at all—rather, Fadell’s system includes a single storage unit (storage 104) that stores both the user’s data and files (such as media data, lifestyle data, exercise data, transaction data, subscription data, contact and calendar data, etc.) ***and*** “authentication information (*e.g.*, libraries of data associated with authorized users)” in a single storage location. Ex.1007, [0031] (emphasis added). Fadell thus fails to disclose the use of separate, dedicated storage units for authentication data and user data—a central requirement of the ‘875 Patent claims.

B. Moran (Ex.1008)

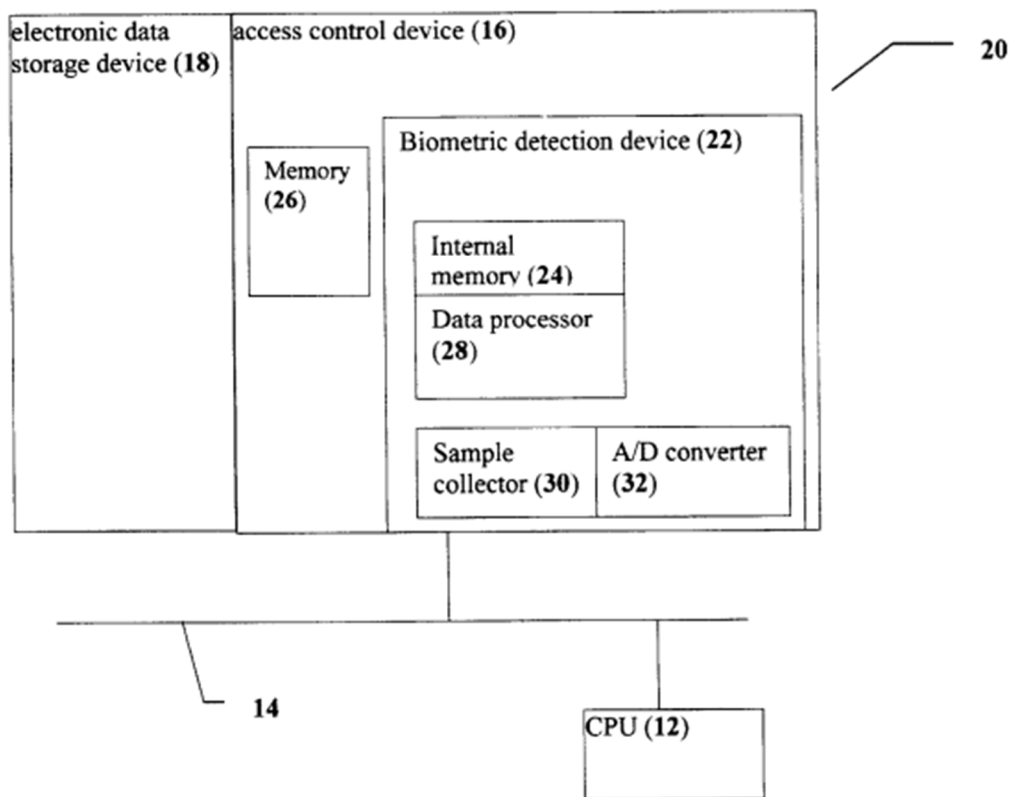
Moran, which as discussed above was heavily relied upon and overcome during prosecution of the ‘875 Patent, discloses a system for accessing data stored in an electronic data storage device. Ex.1008, Abstract. Moran’s system is directed to ***data access control*** and more particularly to determining the type of access a user has to stored data using a biometric detection device. *Id.*, 1:10-14.

Moran’s focus is on allowing different types/tiers of access to different users through authentication. For example, according to Moran:

[T]he important feature of the present invention is that it enables a plurality of different types of data access to be combined in a single storage device. Unlike background art storage devices which are generally restricted to a single type of data access in terms of the hardware implementation, ***the present invention is flexible and is able to store data according to several different access types within a single device.***

Id., 6:22-31 (emphasis added); *see also id.* 2:51-58 (“The present invention provides for access to be determined according to the identity of the user, as determined by the biometric detection device. The present invention also enables various types of permissions to be set for determining access to the stored data, such that if an attempt is made to access particular data which does not have a suitable permission type, access is denied.”), 7:61-9:12 (describing “different types of permissions for accessing data to be stored by access control device 16, such that a variety of different types of data access can be provided”). This differs significantly from the inventions covered by the claims of the ‘875 Patent challenged in this IPR, which are directed to an apparatus for securely storing a single user’s data and files and allowing the user to communicate with external service providers.

Moran’s system (20) for controlling data access, shown below, includes CPU (*i.e.*, central processing unit) (12), bus (14), access control device (16), and data storage device (18):



Id., Fig.3. The access control device (16), which regulates access to the electronic data storage device (18) based on whether the user is properly authenticated, includes a biometric detection device (22) that may be a fingerprint detection device or a retinal scanning device. *Id.*, 10:52-11:2.

Key to Moran's system is that *the CPU (12) is not in communication with data storage device (18)* and "any attempts to access data in data storage device 18 *must pass through* access control device 16." *Id.*, 6:59-62 (emphasis added). This architectural constraint is not merely illustrative but is a foundational principle of the Moran's system. For example, according to Moran:

[D]ata storage device 18 is not in direct communication with bus 14.

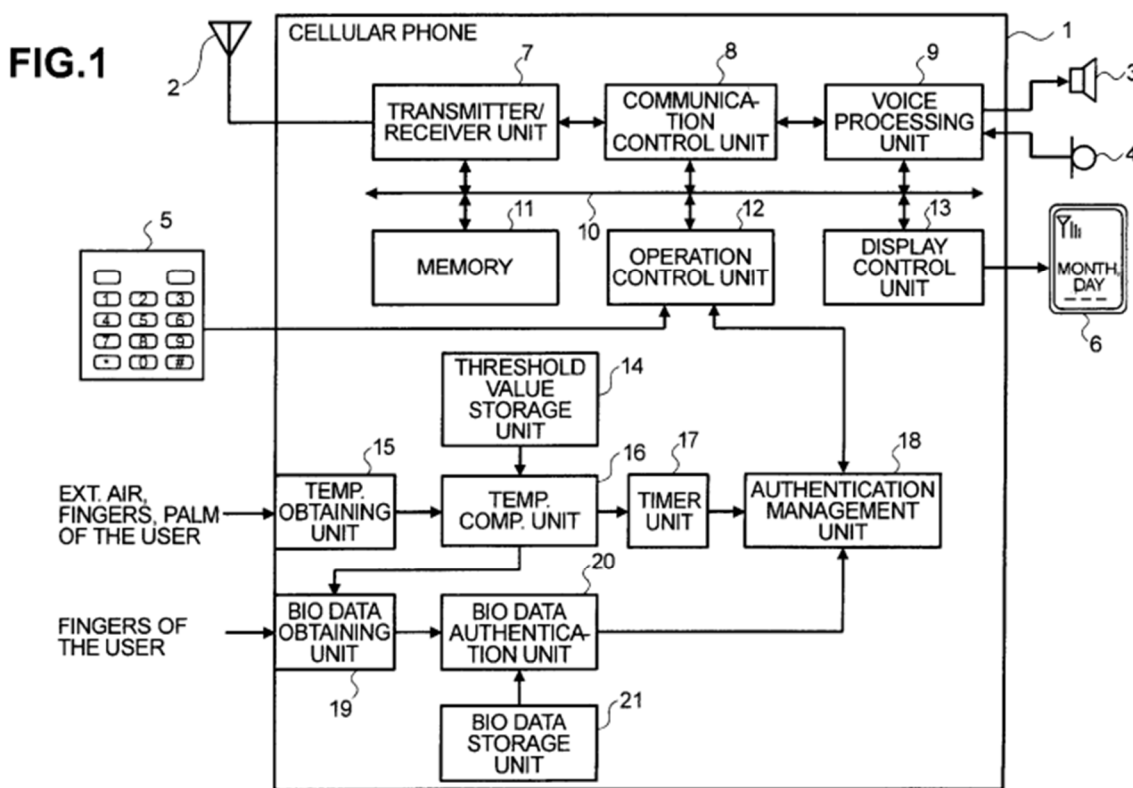
Therefore, if CPU 12 receives an instruction to read data from data storage device 18, CPU 12 preferably cannot directly read such data by sending a command through bus 14 directly to data storage device 18. Rather, preferably ***CPU 12 must send the command to access control device 16, which then determines if such access should be granted and the data read from data storage device 18.*** Thus, more preferably, data can only be read from, and written to, data storage device 18 through access control device 16.

Id., 6:59-7:5 (emphasis added); *see also id.*, 7:19-32, 10:36-46. Accordingly, Moran's system differs significantly from the claimed invention of the '875 Patent, which explicitly requires a processor ***in communication with*** the biometric sensors, the authentication unit, ***and the first storage unit.*** *See* Ex.1001, cl.1.

C. Kohinata (Ex.1009)

Kohinata describes a cellular phone with a security function for authenticating a user. Ex.1009, Abstract, 2:30-35. Kohinata's device "conduct[s] ***a minimum degree*** of required authentication operation which is ***not perceived by the user.***" *Id.*, Abstract (emphasis added). To accomplish this goal, the device relies on temperature measurement and fingerprint detection, both of which are taken from a user's fingers "[a]s the user holds the cellular phone [] by hand." *Id.*

Kohinata's cellular phone (1) is depicted in Figure 1 below.



Id., Fig.1. The device includes, in pertinent part, an authentication management unit (18), a memory (11), and an operation control unit (12) (*i.e.*, “chiefly a CPU”), as well as a variety of functional units that make up a “use detection module” and an “authentication module.” *Id.*, 3:21-62, 4:29-30, 5:41-42. The authentication management unit (18) “is a state machine for managing the present authenticated state of the cellular phone 1, and controls the operation of the cellular phone.” *Id.*, 6:17-29. According to Kohinata, “[t]he shifts among the states constituting the state machine is generated by various instructions from the timer unit 17, biodata authentication unit 20 and operation control unit 12.” *Id.*

Kohinata’s “use detection module” includes a temperature obtaining unit (15) (*i.e.*, “a use detection module for detecting the state of contact to the user” that includes temperature sensors), a threshold value storage unit (14) that stores threshold body temperatures, a temperature comparator unit (16) “for judging whether the cellular phone 1 is touched by the user,” and a timer unit (17) “for judging that the cellular phone 1 has not been touched by the user.” *Id.*, 3:42-45, 4:29-5:40. The “authentication module” includes a biodata obtaining unit (19) (*i.e.*, “a dedicated device for imaging the fingerprint”), a biodata authentication unit (20) that “compares the fingerprint data obtained by the biodata obtaining unit 19 with the fingerprint data stored in the biodata storage unit 21,” and a biodata storage unit (21) that “stores in advance the fingerprint data.” *Id.*, 3:45-48, 5:41-6:16.

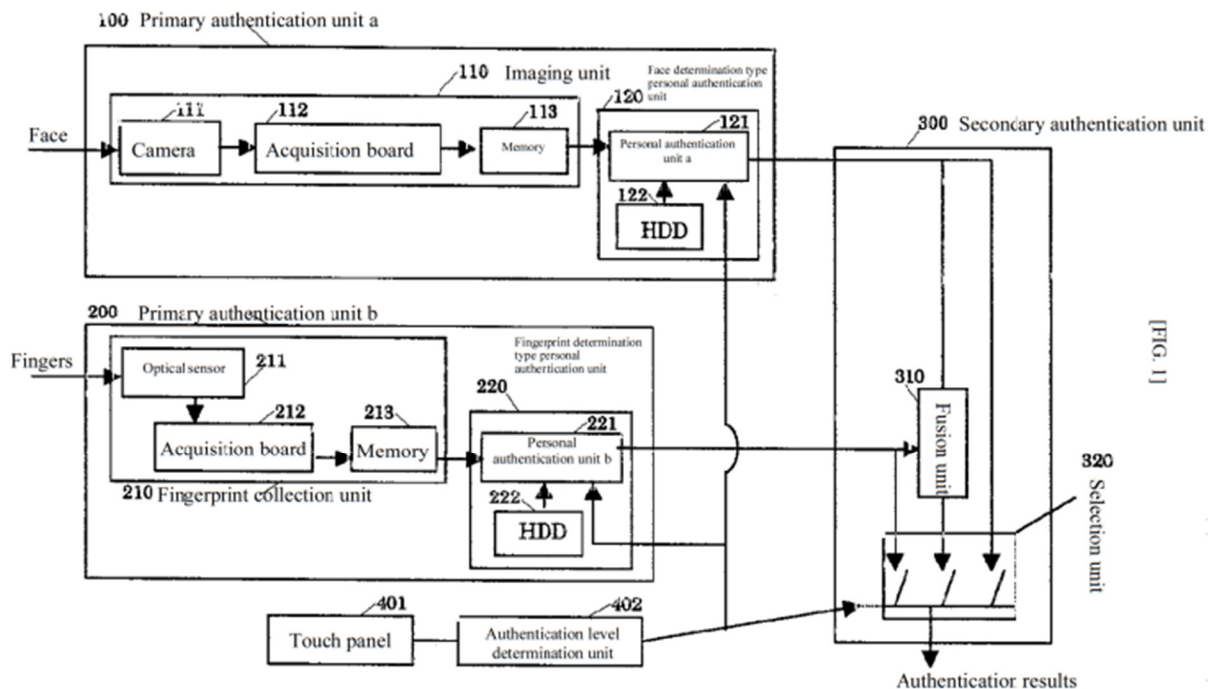
Notably, Petitioners concede that Kohinata does not disclose or suggest a plurality of biometric sensors, as required by the challenged claims of the ‘875 Patent. *See* Pet. at 57-59. Rather, Kohinata’s device merely uses temperature sensors to determine whether a user is touching the device and a single biometric sensor for obtaining a user’s fingerprint.

D. Mizusawa (Exs.1011-1012)

Mizusawa is directed to a personal authentication device that uses a layered authentication architecture. *See* Ex.1012, Abstract. According to Mizusawa, the device uses “multiple primary authentication means that use different personal

authentication methods, and a secondary authentication means that finally authenticates an individual using the output result of the primary authentication unit.” *Id.*, [0007]. The reference explicitly requires that “one of the primary authentication means *always includes a means of authenticating an individual by face.*” *Id.* (emphasis added).

As shown below, Mizusawa’s personal authentication device includes primary authentication unit a (100), primary authentication unit b (200), and secondary authentication unit (300). *Id.*, [0013-14].



Id., Fig.1. Primary authentication unit a (100) includes imaging unit (110) for capturing a facial image and a face determination type personal authentication unit (120) that includes HDD (122) for storing reference facial image data. *Id.*, [0014-

16]. Primary authentication unit b (200) includes fingerprint collection unit (210) for capturing a fingerprint and a fingerprint determination type personal authentication unit (220) that includes HDD (222) for storing reference fingerprint data. *Id.*, [0017-19]. Primary authentication units a and b (100, 200) therefore ***each include separate dedicated processors and storage for storing reference biometric data and operate independently to generate intermediate authentication results***.

Secondary authentication unit (300) receives the outputs from the primary authentication units a and b (100, 200) and “finally authenticates an individual using the output result[s]” based on “required authentication accuracy.” *Id.*, [0007-08]. Secondary authentication unit (300) includes fusion unit (310) for merging authentication results for primary authentication units a and b (100, 200) and selection unit (320). *Id.*, [0020]. An authentication level determination unit (402) determines which primary authentication unit(s) to rely on based on required security level. *Id.* Selection unit (320) can then output the results of primary authentication unit a (100) individually, output the results of primary authentication unit b (200) individually, or output the results of fusion unit (310), “depending on the authentication level input from the authentication level determination unit 402.” *Id.*

Crucially, Mizusawa’s system therefore ***need not*** use multiple biometric parameters to authenticate a user. Moreover, even when both primary

authentication units a and b (100, 200) are used, secondary authentication unit (300) “fuses” the outputs (although the reference fails to provide any details whatsoever describing how it does so) and makes a final authentication determination. Thus, it is at best unclear whether Mizusawa’s system authenticates a user only after “positively match[ing] 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,” as required by the ‘875 Patent.

E. Rosenblatt (Ex.1010)

Petitioners do not rely on Rosenblatt with regard to independent claim 1 in either Grounds 1 or 3 set forth in the Petition. *See* Pet. at 2. Rather, Petitioners rely on Rosenblatt only in Grounds 2 and 4 for their arguments regarding dependent claims 15 and 18, both of which depend from independent claim 1. *See id.*; Ex.1001, cl.15, cl.18. Petitioners do not contend that Rosenblatt discloses any of the elements of independent claim 1 that are missing from Fadell, Moran, Kohinata, and/or Mizusawa, discussed below.

Simply put, Rosenblatt is inconsequential for purposes of determining whether to institute the Petition. Given that the references relied upon in Petitioners’ Grounds 1 and 3 fail to disclose key elements claimed in independent claim 1 and further that Petitioners do not even attempt to argue that Rosenblatt

supplies those missing claim elements, the Board can dispense with the Petition on all grounds.

V. THE BOARD SHOULD DENY INSTITUTION OF THE PETITION²

A. Petitioners Fail to Establish a Reasonable Likelihood That Any of the Challenged Claims Are Obvious Over Fadell and Moran (Grounds 1-2)

Petitioners' Grounds 1-2 fail because, as explained below, Fadell (Ex.1007) and Moran (Ex.1008) do not teach or suggest crucial elements of independent claim 1 (from which all the other claims challenged in Grounds 1-2 depend) and a POSA would not have combined the teachings of these references. Specifically, Petitioners' Ground 1 challenges independent claim 1 and dependent claims 4, 7, 10, 14, and 19 as obvious over Fadell and Moran. Pet. at 2. Petitioners' Ground 2 challenges dependent claims 15 and 18 as obvious over Fadell, Moran, and Rosenblatt (Ex.1010). *Id.* Because all the claims challenged in Grounds 1-2 depend from independent claim 1 and thus contain all claim 1's limitations, Petitioners' challenges to these claims likewise fall short for the exact same reasons.

² For purposes of this POPR, PO will address only the most glaring omissions in Petitioners' purported invalidity grounds. The missing claim elements cannot be remedied by Petitioners' expert's conclusory statements that in many cases merely copy the Petition. Petitioners' Petition for IPR should be denied.

1. The Fadell-Moran Combination Cannot Meet *Both* the “Authentication Unit” and “Processor” Limitations of Independent Claim 1.

Petitioners’ Fadell-Moran combination fails because the references do not teach or suggest both the “authentication unit” and “processor” limitations of claim 1 of the ‘875 Patent. Claim 1 requires a specific combination of elements, including “*an authentication unit comprising a second storage unit . . . configured to store a pre-recorded set of personal biological biometric identification parameters uniquely associated with the specific user*” and “*a processor in communication with said plurality of biometric sensors, said first storage unit and said authentication unit.*” Petitioners attempt to remedy the acknowledged deficiencies in Fadell by incorporating Moran’s access control device, but doing so introduces architectural incompatibilities that prevent the resulting combined system from simultaneously satisfying both claim limitations.

It is undisputed that Fadell does not disclose an authentication unit with a second storage unit. Fadell is explicit that its system includes a single storage unit (storage 104) that stores both a user’s data and files and “authentication information (e.g., libraries of data associated with authorized users).” Ex.1007, [0031]. Petitioners do not contend otherwise—the Petition admits that Fadell’s authentication unit does not include a second storage unit. *See* Pet. at 27.

Conceding that Fadell alone cannot meet this element, Petitioners instead incorrectly argue that it would have been obvious to modify Fadell’s system to incorporate Moran’s access control device, which purportedly includes an authentication unit and a second storage unit for storing pre-recorded biometric parameters. *See id.* Moran, however, relies on a fundamentally different architecture than the one disclosed in Fadell or claimed in the ‘875 Patent. Specifically, *Moran’s system explicitly requires that the CPU (12) is not in communication with data storage device (18).* *See, e.g.,* Ex.1008, 6:59-7:5, 7:19-32, 10:36-46. Indeed, Moran expressly states that “any attempts to access data in data storage device 18 *must pass through* access control device 16” and “CPU 12 *must send the command* to access control device 16, which then determines if such access should be granted and the data read from data storage device 18.” *Id.*, 6:59-7:5 (emphasis added). The separation between the processor (CPU) and data storage device (18) is key to Moran’s system—according to Moran, implementing the system as an access control device that “*controls all access* to the data storage device” makes the system “more difficult to ‘hack’ for access by an unauthorized user.” *Id.*, 2:58-64 (emphasis added); *see also id.*, Abstract, 5:54-59.

Contrary to Petitioners’ contentions, however, *Moran’s architectural separation of the processor (CPU (12)) from the data storage device (18) is incompatible with both Fadell’s system and the requirements of claim 1.* In

Fadell, processor (102) is in direct communication with storage (104) through a bus “operative to provide a data transfer path for transferring data to, from, or between” components. Ex.1007, [0040]. Claim 1 of the ‘875 Patent similarly requires that the processor be “in communication with” the first storage unit. Thus, incorporating Moran’s access control device into Fadell’s system creates a fundamental “catch-22” for Petitioners. If Moran’s architecture is preserved in the combination—*i.e.*, if Fadell’s processor (102) is not allowed to directly communicate with storage (104)—then the resulting Fadell-Moran combined system cannot satisfy the “processor” limitation of claim 1. On the other hand, if the processor in the combined Fadell-Moran system is allowed to communicate directly with the storage unit (as required by claim 1), then the resulting system would be inconsistent with Moran’s explicit teachings and core architecture. More problematically for Petitioners, such a system would render Moran’s access control device inoperable for its intended purpose because it would no longer “control all access” to the data storage device. *See, e.g., Deere & Co. v. David’s Dozer V-Loc System, Inc.*, IPR2024-01442, Paper 10 at 28-30 (PTAB March 18, 2025) (denying institution where proposed combination rendered reference’s system “inoperable for its intended purpose”).

Accordingly, Petitioner’s proposed Fadell-Moran combination cannot simultaneously satisfy both the “authentication unit” and “processor” limitations of

claim 1 of the '875 Patent. Petitioners' attempt to fix one deficiency in Fadell (*i.e.*, Fadell's lack of a "second storage unit") by incorporating Moran's access control device creates another, equally fatal deficiency (*i.e.*, a modified system with a processor that is no longer "in communication with" the first storage unit, as claimed). Petitioners cannot pick and choose individual components of Moran while ignoring Moran's limiting architecture that makes those components function as intended. This is a fatal flaw in the Petition that, even if IPR is instituted, cannot be remedied by Petitioners. Petitioners' Fadell-Moran combination (Grounds 1-2) therefore fails.

2. A POSA Would Not Have Been Motivated to Combine Fadell and Moran.

In addition to the Fadell-Moran combination's failure to satisfy all elements of claim 1, the proposed combination fails for a related reason—a POSA would not have been motivated to combine Fadell and Moran because they are directed to fundamentally different systems and, in fact, Moran explicitly teaches away from such a combination. The Petition fails to account for the substantial architectural incompatibilities between the two references and provides no explanation for how or why a POSA would have been motivated to override the fundamental structure of Fadell's system in favor of Moran's incompatible architecture. Petitioners could have, but did not, address this in the Petition. Nor can Petitioners salvage their deficient argument at some later point in the proceeding. *See Intelligent Bio-Sys.*,

Inc. v. Illumina Cambridge Ltd., 821 F.3d 1359, 1369 (Fed. Cir. 2016) (“Unlike district court litigation—where parties have greater freedom to revise and develop their arguments over time and in response to newly discovered material—the expedited nature of IPRs bring with it an obligation for petitioners to make their case in their petition to institute. While the Board’s requirements are strict ones, they are requirements of which petitioners are aware when they seek to institute an IPR.”); Patent Trial and Appeal Board Consolidated Trial Practice Guide (Nov. 2019) at 73 (“Petitioner may not submit new evidence or argument in reply that it could have presented earlier, *e.g.* to make out a prima facie case of unpatentability.”). The time for addressing the incompatibility of Fadell and Moran was in the Petition, and Petitioners’ failure to do so dooms their Fadell-Moran grounds.

Fadell discloses a system where the processor (102) directly communicates with storage (104) through a bus. Ex.1007, [0040]. Moran’s system, by contrast, is premised on an entirely different architecture: one in which the CPU is not permitted to communicate directly with the main storage unit. Ex.1008, 6:59-7:5, 7:19-32, 10:36-46. A POSA would have recognized that Moran’s approach is incompatible with Fadell’s and thus would not have been motivated to combine the teachings of these references.

Moreover, Moran explicitly teaches away from Petitioners’ proposed combination. “A sufficient reason to combine reference teachings is absent if a reference teaches away from its combination.” *Deere*, IPR2024-01442, Paper 10 at 10 (citing *Tec Air, Inc. v. Denso Manufacturing Mich. Inc.*, 192 F.3d 1353, 1360 (Fed. Cir. 1999)). Courts and the Board have consistently found that “[a] reference teaches away from a combination, if ‘a person of ordinary skill, upon reading the reference, would be discouraged from following the path set out in the reference, or would be led in a direction divergent from the path that was taken by the applicant.’” *Id.* (quoting *In re Gurley*, 27 F.3d 551, 553 (Fed. Cir. 1994)). That is precisely the case here. Moran discourages the very design—direct processor-to-storage communication—that is required by the claims and used in Fadell’s system. Moran’s separation is not a peripheral feature—it is the core principle on which Moran’s system is built. Indeed, Moran repeatedly emphasizes that its invention improves security precisely because CPU (12) must communicate with the data storage device (18) only through the access control device (16), thereby making the system “more difficult to ‘hack’ for access by an unauthorized user.” Ex.1008, Abstract, 2:58-64, 5:54-59.

At a minimum, however, Moran would have led a POSA in a direction divergent from claimed invention. Based on Moran’s teachings regarding the importance of disallowing communication between the processor and data storage

device, a POSA incorporating Moran's access control device into Fadell's system would have modified Fadell's architecture such that storage (104) is accessible to processor (102) *only through* the access control device. As explained above, however, such an architecture does not meet the "processor" element of claim 1.

As such, Petitioners' proposed Fadell-Moran combination is not merely unsupported by the prior art; it is directly contrary to it. At bottom, a POSA would have either not been motivated to combine the references because Moran teaches away from Fadell's design or would have combined the references in a way that does not meet all the limitations of claim 1. In either case, Petitioners' Fadell-Moran combination would not have rendered claim 1 obvious. Petitioners' Grounds 1-2 should therefore be rejected.

B. Petitioners Fail to Establish a Reasonable Likelihood That Any of the Challenged Claims Are Obvious Over Kohinata and Mizusawa (Grounds 3-4)

Like Petitioners' Ground 1-2 challenges, Petitioners' Grounds 3-4 also fail because Kohinata (Ex.1009) and Mizusawa (Exs.1011-12) do not teach or suggest all elements of independent claim 1 (from which all the other claims challenged in Grounds 3-4 depend) and a POSA would not have combined the teachings of these references. Specifically, Petitioners' Ground 3 challenges independent claim 1 and dependent claim 4 as obvious over Kohinata and Mizusawa. Pet. at 2. Petitioners' Ground 4 challenges dependent claims 15 and 18 as obvious over Kohinata,

Mizusawa, and Rosenblatt (Ex.1010). *Id.* Because all the claims challenged in Grounds 3-4 depend from independent claim 1 and therefore contain all claim 1's limitations, Petitioners' challenges to these claims likewise fall short.

1. The Kohinata-Mizusawa Combination Fails to Disclose the “Access...Is Only Enabled After Said Authentication Unit Positively Matches Each of the Plurality of Personal Biological Biometric Identification Parameters of the User” Limitation of Independent Claim 1.

Claim 1 requires “*a plurality of biometric sensors for reading a plurality of personal biological biometric identification parameters of the user holding the apparatus*” and further 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.*” Petitioners Kohinata-Mizusawa combination, which purportedly “combines Mizusawa’s multi-biometric authentication with Kohinata’s authentication module” (*see* Pet. at 57), fails to disclose or render obvious these limitations.

As an initial matter, Petitioners admit that Kohinata lacks a plurality of biometric sensors. While Petitioners identify Kohinata’s biodata obtaining unit 19 for obtaining a user’s fingerprint, Petitioners do not identify any other purported biometric sensors in Kohinata’s device. *See id.*, 57-59. Conceding Kohinata alone

cannot meet the “plurality of biometric sensors” limitation, Petitioners attempt to remedy this deficiency by relying on Mizusawa. *See id.* In particular, Petitioners contend that it would have been obvious “to add Mizusawa’s facial authentication to [Kohinata’s] authentication module and to combine Mizusawa’s secondary authentication teachings with Kohinata’s authentication management unit within the authentication module.” *Id.* at 52-53. Petitioners assert that the combined device therefore meets the “plurality of biometric sensors” limitation.

Combining the teachings of Kohinata and Mizusawa as proposed in the Petition, however, creates another problem for Petitioners—the modified device cannot satisfy the “access” control condition recited in the claims. In Mizusawa’s system, two primary authentication units a and b are used that are each capable of authenticating a user independently using a different biometric modality. Ex.1012, [0014-19]. Mizusawa’s system further includes a secondary authentication unit—which Petitioners contend would be incorporated into Kohinata’s authentication management unit—that receives the outputs from the primary authentication units a and b and “finally authenticates an individual using the output result[s]” based on “required authentication accuracy.” *Id.*, [0007-08]. While Mizusawa teaches that the secondary authentication unit receives the outputs from primary authentication units, nothing in Mizusawa explicitly indicates that the secondary authentication unit enables access only after *positively matching each of the plurality of personal*

biological biometric identification parameters with the pre-recorded set of reference parameters, as required by the claim.

Instead, according to Mizusawa, an authentication level determination unit determines which primary authentication unit(s) to rely on based on required security level. *Id.*, [0020]. A selection unit within the secondary authentication unit can then output the results of primary authentication unit a individually, output the results of primary authentication unit b individually, or output the results of a fusion unit “depending on the authentication level input from the authentication level determination unit.” *Id.* Plainly, in instances where Mizusawa’s secondary authentication unit authenticates a user based on the output of a single primary authentication unit (*e.g.*, facial recognition from unit a alone or fingerprint detection from unit b alone), Mizusawa’s secondary authentication unit does not enable access only after positively matching *each of the plurality of personal biological biometric identification parameters* with the pre-recorded set of reference parameters, as required by the claim.

Moreover, although Mizusawa’s secondary authentication unit can combine the outputs of primary authentication units a and b using a “fusion unit” to authenticate a user, Mizusawa does not disclose the logic or algorithm used by the fusion unit or specify that the fusion unit requires positive matching of *both* biometric modalities to grant access. On the contrary, Mizusawa’s architecture

permits the secondary authentication unit to authenticate a user even if only one (or neither) of the two primary units returns a “positive match” if the combined output of the fusion unit satisfies the required security level. Thus, even when Mizusawa’s secondary authentication unit combines the outputs of both primary authentication units via the fusion unit, the secondary authentication unit does not require positively matching *each* biometric parameter with a set of reference parameters, as claimed.

Accordingly, the final authentication decision in Mizusawa is not tied to a positive match of a plurality of biometric parameters. There is no disclosure in Mizusawa that would lead a POSA to understand that access is only granted following a successful match of each biometric parameter against corresponding stored reference data, as the claim expressly requires. Petitioners fail to address this, nor do they even attempt to explain how Mizusawa’s secondary authentication unit would function any differently in a combined Kohinata-Mizusawa device. Petitioners’ proposed combination is therefore deficient. *Neither Kohinata nor Mizusawa, individually or in combination, teaches or suggests conditioning access to user data on the authentication unit positively matching each of a plurality of biometric identification parameters with pre-recorded reference data.* Petitioners’ Kohinata-Mizusawa combination thus fails.

**2. The Kohinata-Mizusawa Combination Fails to Disclose the
“Authentication Unit Comprising a Second Storage Unit”
Limitation of Independent Claim 1.**

Claim 1 recites “*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*” and where “*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.*” Petitioners’ Kohinata-Mizusawa combination fails to meet these limitations of claim 1.

According to Petitioners, the combined Kohinata-Mizusawa 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 prerecorded biological biometric identification parameters stored in memory (biodata authentication unit 20 and processor 110)” and “[a] POSITA would have understood that the comparison is performed by a processor for each type of biometric authentication.” Pet. at 69. Thus, Petitioners’ combined device explicitly includes two separate storage units, each storing an individual pre-recorded reference parameter, and two separate processors, each for comparing an individual measured biometric parameter with

an individual pre-recorded reference parameter. But because the “authentication unit” of Petitioners’ Kohinata-Mizusawa combination includes multiple storage units and multiple processors, the modified device does not have the required second storage unit for storing a *set* of biometric reference parameters and does not compare a *plurality* of measured biometric parameters with the *set* of reference parameters, as claimed.

This architecture is not merely optional—by incorporating the “secondary authentication unit” of Mizusawa, this architecture is required by Petitioners’ combination. *See, e.g., In re Wesslau*, 353 F.2d 238, 241 (CCPA 1965) (“It is impermissible within the framework of section 103 to pick and choose from any one reference only so much of it as will support a given position, to the exclusion of other parts necessary to the full appreciation of what such reference fairly suggests to one of ordinary skill in the art.”); *Axalta Coating Sys., LLC v. PPG Industries Ohio, Inc.*, IPR2022-00676, Paper 10 at 18-19 (PTAB Sept. 12, 2022) (denying institution in part because Petitioner failed to explain why a POSA would rely on certain teachings of a reference “in isolation” from reference’s other requirements). Mizusawa’s device divides processing and storage across two independent primary authentication units a and b. Ex.1012, [0014-19]. Each unit includes its own processor and local hard disk drive (HDD), and each processes a different biometric input modality. *Id.* There is no disclosure in Mizusawa of a

single authentication unit that stores and compares a *plurality* of biometric parameters against a stored reference dataset as claimed. Instead, Mizusawa’s system separates the processing and storage of biometric data across multiple primary reference units. Reference parameters are not stored in a unified “second storage unit” within a single authentication unit, and there is no indication that any one unit performs a comparison of all measured biometric parameters. To the contrary, each primary authentication unit independently processes its own biometric input and produces a partial result, which is then passed to a secondary authentication unit.

This fragmented architecture cannot reasonably be considered a single “authentication unit comprising a second storage unit” configured to compare “a plurality” of biometric parameters with stored reference data. At most, each primary unit stores its own biometric reference parameters locally on separate HDDs and performs a comparison of a single parameter. The secondary authentication unit then makes a separate decision based on the outputs—but does not itself store reference parameters or perform the claimed comparison.

Apparently recognizing these deficiencies, Petitioners contend that a POSA would have been motivated to use a single memory and single processor in the authentication unit of the combined device. *See* Pet. at 67, 69-70. Petitioners’ conclusory arguments fail for multiple reasons. First, they are unsupported because

they cite expert testimony that merely repeats the Petition nearly verbatim. Compare *id.* with Ex.1003, ¶¶296, 305; see also *Xerox Corp. et al. v. Bytemark, Inc.*, IPR2022-00624, Paper 12 at 5 (PTAB Feb. 10, 2023) (Director Review affirming Board’s denial of institution and finding “the Board was correct in giving little weight to Petitioner’s expert because the expert declaration merely offered conclusory assertions without underlying factual support and repeated, *verbatim*, Petitioner’s conclusory arguments”). Second, using a single memory and single processor is wholly inconsistent with the architecture of Mizusawa and contradicts the reference’s explicit purpose of providing a configuration that “maintains the required authentication accuracy at all times, while making it possible to select the optimal authentication method depending on the security level, improving the user interface during operation.” Ex.1012, [0009]. Thus, contrary to Petitioners’ assertions, a POSA would not have used a single memory and single processor in the authentication unit of the combined device.

3. The Kohinata-Mizusawa Combination Fails to Disclose the “Life Signs Detector” and “Whenever Any of Said at Least One Life Signs Detector Detects a Critical Level of Said User Measured Life Sign Parameters” Limitations of Independent Claim 1.

Claim 1 requires “*at least one life signs detector...configured to measure and record at least one of said user’s life sign parameters*” and further that “*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." Petitioners argue Kohinata's temperature obtaining unit (alone or with comparator unit) is the claimed "life signs detector." Pet. at 59. Not so.

Although Kohinata's device includes temperature sensors for measuring the body temperature of a user and the ambient temperature, Kohinata merely uses the measurement to determine if a user is touching the device, not as a measure of the user's life signs parameters. For example, Kohinata's device includes "use detection module *for judging the state of contact to the user* by measuring the temperature." Ex.1009, 2:56-57 (emphasis added). Further, according to Kohinata, the temperature measurement is used to "judge[] that the cellular phone 1 is *touched by the user and is used or is going to be used.*" Ex.1009, 4:54-60 (emphasis added); *see also id.*, 3:42-44 ("use detection module for *judging the state of contact to the user* by measuring the temperature") (emphasis added), 4:54-55 ("The temperature comparator unit 16 is a module for *judging whether the cellular phone 1 is touched by the user.*") (emphasis added), 10:66-67. This assessment—whether the phone is touched by a user—is utilized by Kohinata not to determine the physiological state of the user, but instead merely to initiate biometric fingerprint detection to authenticate the user. *See id.*, 6:49-59 ("the cellular phone 1 is held by hand causing an increase in the temperature data from

the temperature obtaining unit 15 which is touched by the finger or palm of hand of the user. When the temperature data from the temperature obtaining units 15 is not smaller than a predetermined number exceed the threshold temperature set to the threshold value storage unit 14, the temperature comparator unit 16 so judges that the use of the cellular phone 1 is started as it is touched by the user and issues an instruction to the biometric data obtaining unit 19 to obtain the fingerprint data of the user.”). Thus, while Kohinata’s device includes temperature sensors, they are not used “to measure and record at least one of said user’s life sign parameters” and “detect[] a critical level of said user measured life sign parameters” to “prevent access to said user’s personal data and documentation files stored in said first storage unit,” as claimed.

Moreover, the ability of the user to set the temperature threshold undermines any characterization of these sensors as a life signs detector. Kohinata’s use detection module includes threshold value storage unit 14 that stores threshold body temperatures. *Id.*, 4:40-48. According to Kohinata, “[t]he threshold temperatures ***can be freely set by the user*** of the cellular phone 1.” *Id.*, 47-48 (emphasis added). This further underscores that the purpose of the temperature sensor is not to assess any physiological risk or condition of the user, but rather to trigger biometric fingerprint detection under user-defined conditions. A temperature sensor whose threshold is arbitrarily set by the user to control device

functionality cannot reasonably be said to detect “a critical level” of a life sign parameter as required by the claim.

Finally, Kohinata does not disclose “preventing access” in response to a “critical” temperature measurement. Even setting aside the functional purpose of the temperature sensor, Kohinata does not disclose that the system blocks access to user data based on any detected temperature measurement. There is no logic or mechanism in Kohinata by which a measured temperature would result in any limitation on access to stored data. Instead, as explained above, the temperature check simply determines whether a user is touching the phone and initiates the fingerprint sensor to obtain a fingerprint. *See id.*, 6:49-59. Crucially, the fingerprint sensor and associated units authenticate the user and ultimately determines whether access to the phone is permitted or denied. *See id.*, 6:59-7:10 (when fingerprint data is not in agreement with stored fingerprint data of user, “the biodata authentication unit 20 notifies ‘authentication has failed’ to the authentication management unit 18 to indicate that the authentication was not successful”).

In sum, although Kohinata’s device measures user and ambient temperature, it does not do so for purposes of measuring a user’s life sign parameters, does not detect a critical level of any measured temperature, and does not prevent access to the user’s data and files when a critical level of the user’s temperature is detected.

Accordingly, Kohinata does not disclose or render obvious the “life signs detector” limitations as required by claim 1.

4. A POSA Would Not Have Been Motivated to Combine Kohinata and Mizusawa.

Even setting aside the individual and collective deficiencies in Kohinata and Mizusawa, Petitioners’ proposed combination should be rejected for a more fundamental reason: a POSA would not have been motivated to combine the references in the manner proposed by Petitioners. The systems disclosed in Kohinata and Mizusawa are based on divergent design goals—particularly with respect to user interaction and visibility of the authentication process—and Petitioners offer no persuasive rationale that reconciles those differences.

On one hand, Kohinata prioritizes an authentication experience that is not perceptible to the user. Kohinata repeatedly emphasizes that a core goal of the invention is to authenticate users without their awareness. For example, Kohinata describes the invention as “[a] cellular phone which is easy to use featuring a sufficient degree of safety preventing unauthorized use by conducting a minimum degree of required authentication operation *which is not perceived by the user.*” Ex.1009, Abstract (emphasis added). To achieve this goal, Kohinata uses biometric input modalities that are inherently non-intrusive—specifically, measuring temperature when a user is holding the device and fingerprint detection, both of which rely on a user’s incidental contact with the device. These choices are

deliberate, allowing the authentication process to occur passively and without significant user action.

By contrast, Mizusawa requires active user participation and includes biometric modalities that are inherently perceptible to the user. According to Mizusawa, the system *must include facial imaging and/or recognition*. Ex.1012, [0007] (“the system is characterized in that *one of the primary authentication means always includes a means of authenticating an individual by face*”) (emphasis added). Although Mizusawa intends for this type of authentication to minimize the burden on the user, it cannot reasonably be disputed that facial recognition is perceptible to a user. Indeed, a user must align his/her face and engage with the device in a very specific, perceptible manner. This type of interaction is plainly incompatible with Kohinata’s goal of authentication without user perception.

Petitioners do not explain how or why a POSA would combine the teachings of a reference (Mizusawa) that explicitly requires facial imaging/recognition necessitating overt user action with a reference (Kohinata) whose system is explicitly designed to be imperceptible to the user. Doing so would fundamentally alter the user experience and defeat the core objectives of the references.

Accordingly, the Petition should be denied for the additional reason that a POSA would not have combined Mizusawa's facial-recognition-based system with Kohinata's device with passive, contact-based, imperceptible authentication.

VI. CONCLUSION

PO respectfully submits that the evidence presented in the Petition fails to establish a reasonable likelihood Petitioners will prevail in establishing that any of the Challenged Claims of the '875 Patent are unpatentable. PO therefore respectfully requests that the Board deny the Petition in its entirety.

Dated: June 20, 2025

Respectfully submitted,

/s/ Roger Thompson

Roger Thompson (Reg. No. 29,594)

rthompson@villegascefo.com

Damir Cefo (Reg. No. 51,538)

dcefo@villegascefo.com

VILLEGAS & CEFO, LLP

1350 Avenue of the Americas, Floor 2

New York, New York 10019

P: 646-844-0679

Kyle Deighan (Reg. No. 75,525) (*updated
Mandatory notices forthcoming*)

kdeighan@calfee.com

Mark McDougall (Reg. No. 62,670)

(*updated Mandatory notices forthcoming*)

mmcdougall@calfee.com

CALFEE, HALTER & GRISWOLD LLP

The Calfee Building

1405 East Sixth Street

Cleveland, Ohio 44114

P: 216-622-8200

F: 216-241-0816

*Attorneys for Patent Owner OS New
Horizon Personal Computing Solutions
Ltd.*

CERTIFICATE OF COMPLIANCE

The undersigned certifies that Patent Owner's Preliminary Response complies with the type-volume limitations of 37 C.F.R. §42.24 because it contains 9,583 words (as determined by the Microsoft Word word-processing system used to prepare the Petition), excluding the parts of the Petition exempted by 37 C.F.R. §42.24.

Dated: June 20, 2025

/s/ Roger Thompson

Roger Thompson (Reg. No. 29,594)

*Attorney for Patent Owner OS New
Horizon Personal Computing Solutions
Ltd.*

CERTIFICATE OF SERVICE

The undersigned certifies that the foregoing **PATENT OWNER'S PRELIMINARY RESPONSE** was served on the date below via email at the following email addresses:

Lori Gordon (Gordon-ptab@goodwinlaw.com)

Doug Kline (dkline@goodwinlaw.com)

Srikanth Reddy (sreddy@goodwinlaw.com)

Naomi Birbach (NBirbach@goodwinlaw.com)

Theodoros Konstantakopoulos (tkonstantakopoulos@goodwinlaw.com)

Dated: June 20, 2025

/s/ Roger Thompson

Roger Thompson (Reg. No. 29,594)

*Attorney for Patent Owner OS New
Horizon Personal Computing Solutions
Ltd.*