

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 HORIZONS PERSONAL COMPUTING SOLUTIONS LTD.,
Patent Owner

IPR2025-00613

U.S. Patent No. 8,401,875

**DECLARATION OF ANDREW WOLFE, PH.D. IN SUPPORT OF
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

	Page
I. INTRODUCTION	1
II. QUALIFICATIONS	2
III. UNDERSTANDING OF RELEVANT LEGAL PRINCIPLES	8
IV. '875 PATENT	10
A. Technical Background	10
B. Overview of the '875 Patent	20
C. Level of Ordinary Skill in the Art	30
D. Prosecution Histories	31
1. U.S. Patent & Trademark Office (USPTO)	31
2. European Patent Office (EPO)	37
E. Claim Construction	40
1. “first storage unit” (Claim 1)	41
2. “second storage unit” (Claim 1)	45
3. “authentication unit” (Claim 1)	46
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)	50
V. GROUND 1: THE COMBINATION OF FADELL AND MORAN RENDERS OBVIOUS CLAIMS 1, 4, 7, 10, 14, AND 19	57
A. Overview of the Combination	57
1. Fadell	57
2. Moran	63
3. Motivation to Combine Fadell and Moran	66

TABLE OF CONTENTS

(continued)

Page ii

B.	Independent Claim 1	71
1.	Preamble [1P]: “Apparatus”	71
2.	Integrated Biometric Sensors [1A]	75
3.	Life Signs Detector [1B].....	81
4.	First Storage Unit [1C].....	84
5.	Authentication Unit [1D]	86
a)	Integrated Authentication System	87
b)	“pre-recorded set of personal biological biometric identification parameters”.....	88
c)	Second Storage Unit	90
d)	Authentication Unit	92
e)	Authentication Unit Comprising the Second Storage Unit.....	97
6.	Processor [1E].....	97
7.	Matching of Personal Biological Biometric Identification Parameters [1F].....	99
8.	Critical Level Detection [1G]	101
C.	Claims 4 and 7 – Communicating With An External Device/Server	103
D.	Claim 10 – Communicating With An External Device	106
E.	Claim 14 – Secure Update Of User’s Data	107
F.	Claim 19 – Cellular Modem, Flat Display, And Touch Screen.....	109
VI.	GROUND 2: FADELL, MORAN, AND ROSENBLATT RENDER OBVIOUS CLAIMS 15 AND 18.....	111
A.	Overview of the Combination.....	112
1.	Rosenblatt.....	112
2.	Motivation to Combine	115

TABLE OF CONTENTS

(continued)

Page iii

B.	Claim 15 – Encoder/Decoder And Wireless Transceiver Module.....	119
C.	Claim 18 – GPS Module	122
VII.	GROUND 3: KOHINATA AND MIZUSAWA RENDER OBVIOUS CLAIMS 1 AND 4.....	123
A.	Overview of the Combination	124
1.	Kohinata	124
2.	Mizusawa	129
3.	Motivation to Combine Kohinata and Mizusawa.....	132
B.	Independent Claim 1	137
1.	Preamble [1P]: “Apparatus”	137
2.	Integrated Biometric Sensors [1A]	138
3.	Life Signs Detector [1B].....	141
4.	First Storage Unit [1C].....	144
5.	Authentication Unit [1D]	146
a)	Authentication Module	147
b)	“pre-recorded set of personal biological biometric identification parameters”.....	149
c)	Second Storage Unit	151
d)	Authentication Unit	153
e)	Authentication Unit Comprising the Second Storage Unit.....	156
6.	Processor [1E].....	156
7.	Matching of Personal Biological Biometric Identification Parameters [1F].....	158
8.	Critical Level Detection [1G]	160
C.	Claim 4 – Communicating With An External Device	162

TABLE OF CONTENTS

(continued)

Page iv

VIII. GROUND 4: KOHINATA, MIZUSAWA, AND ROSENBLATT RENDER OBVIOUS CLAIMS 15 AND 18.....	164
A. Motivation to Combine	165
B. Claim 15 – Encoder/Decoder And Wireless Transceiver Module.....	169
C. Claim 18 – GPS Module	172
IX. CONCLUSION.....	173

I. Introduction

I, Andrew Wolfe, Ph.D., declare as follows:

1. I have been retained on behalf of Petitioners Samsung Electronics Co. Ltd. and Samsung Electronics America, Inc. (“Petitioners”) to provide this Declaration concerning technical subject matter relevant to the petition for *Inter Partes* Review (“Petition”) of U.S. Patent No. 8,401,875 (“the ’875 patent”; EX-1001).

2. I am over 18 years of age. I have personal knowledge of the facts stated in this Declaration and could testify competently to them if asked to do so.

3. I have been asked to provide my technical opinions regarding how a person of ordinary skill in the art (“POSITA”) would have understood the claims of the ’875 patent at the time of the alleged invention, which I have been asked to assume is the 2010 timeframe, as explained herein. For purposes of whether the teachings of the prior art render the claims of the ’875 patent obvious, I have been asked to assume that the priority date of the ’875 patent is March 12, 2010, which is the filing date of U.S. Provisional Application No. 61/313,145, to which the ’875 patent claims priority (’875 patent, Cover Page (60) (Related U.S. Application Data)). I have also been asked to provide my technical opinions on how concepts in the ’875 patent specification relate to claim limitations of the ’875 patent.

4. In reaching the opinions provided herein, I have considered the '875 patent, its prosecution history, and the materials cited in my Declaration and the Appendix. I have also drawn on my own education, training, research, knowledge, and personal and professional experience.

5. In general, I have been asked to cite to the specification of a patent or patent publication using the following formats: (Patent, Col:Line Number(s)) or (Patent Publication, Paragraph Number(s)). For example, the citation ('875 patent, 1:1-10) points to the '875 patent specification at column 1, lines 1-10. Unless otherwise noted, all emphasis by bold or underline and figure annotations have been added, and all quoted language of the claims of the '875 patent has been italicized.

6. I am being compensated for my time at my standard consulting rate. I am also being reimbursed for expenses that I incur during the course of this work. My compensation is not contingent upon the results of my study and analysis, the substance of my opinions, or the outcome of any proceeding involving the '875 patent. I have no financial interest in the outcome of this matter or in any litigation involving the '875 patent.

II. Qualifications

7. I am well-qualified to render useful opinions on this matter. I will briefly summarize my knowledge, training, and experience here. A copy of my curriculum vitae that fully sets forth my qualifications is filed in the proceeding as

EX-1004. Below is a summary of my education, work experience, and other qualifications.

8. In 1985, I earned a B.S.E.E. degree in Electrical Engineering and Computer Science from The Johns Hopkins University. In 1987, I received an M.S. degree in Electrical and Computer Engineering from Carnegie Mellon University. In 1992, I received a Ph.D. in Computer Engineering from Carnegie Mellon University. My doctoral dissertation proposed a new approach for the architecture of a computer processor.

9. I have more than 35 years of experience as a computer architect, computer system designer, personal computer graphics designer, educator, and executive in the electronics industry.

10. In 1983, I began designing touch sensors, microprocessor-based computer systems, and I/O (input/output) cards for personal computers as a senior design engineer for Touch Technology, Inc. During the course of my design projects with Touch Technology, I designed I/O cards for PC-compatible computer systems, including the IBM PC-AT, to interface with interactive touch-based computer terminals that I designed for use in public information systems. I continued designing and developing related technology as a consultant to the Carroll Touch division of AMP, Inc., where in 1986, I designed one of the first custom touch-screen

integrated circuits. I designed the touch/pen input system for the Linus WriteTop, which many believe to be the first commercial tablet computer.

11. From 1986 through 1987, I designed and built a high-performance computer system as a student at Carnegie Mellon University. From 1986 through early 1988, I also developed the curriculum and supervised the teaching laboratory for processor design courses.

12. In the latter part of 1989, I worked as a senior design engineer for ESL-TRW Advanced Technology Division. While at ESL-TRW, I designed and built a bus interface and memory controller for a workstation-based computer system, and also worked on the design of a multiprocessor system.

13. At the end of 1989, I (along with some partners) reacquired the rights to the technology I had developed at Touch Technology and at AMP and founded The Graphics Technology Company. Over the next seven years, as an officer and a consultant for The Graphics Technology Company, I managed the company's engineering development activities and personally developed dozens of touch screen sensors, controllers, and interactive touch-based computer systems.

14. I have consulted, formally and informally, for a number of fabless semiconductor companies. In particular, I have served on the technical advisory boards for two processor design companies: BOPS, Inc., where I chaired the board; and Siroyan Ltd., where I served in a similar role for three networking chip

companies—Intellon, Inc., Comsilica, Inc., and Entridia, Inc.—and one 3D game accelerator company, Ageia, Inc.

15. I have also served as a technology advisor to Motorola and to several venture capital funds in the U.S. and Europe. Currently, I am a director of Turtle Beach Corporation, providing guidance in its development of premium audio peripheral devices for a variety of commercial electronic products.

16. From 1991 through 1997, I served on the Faculty of Princeton University as an Assistant Professor of Electrical Engineering. At Princeton, I taught undergraduate and graduate-level courses in Computer Architecture, Advanced Computer Architecture, Display Technology, and Microprocessor Systems, and conducted sponsored research in the area of computer systems and related topics. I was also a principal investigator for DOD research in video technology and a principal investigator for the New Jersey Center for Multimedia Research. From 1999 through 2002, while a Consulting Professor, I taught a Computer Architecture course to both undergraduate and graduate students at Stanford University. At Princeton, I received several teaching awards, both from students and from the School of Engineering. I have also taught advanced microprocessor architecture to industry professionals in seminars sponsored by the Institute of Electrical and Electronics Engineers (“IEEE”) and the Association for Computing Machinery (“ACM”). I am currently an Assistant Teaching Professor at Santa Clara University

teaching courses on Microprocessor Systems, Integrated Circuit (“IC”) Design, PCB Design, Real-Time Computing, and Mechatronics.

17. From 1997 through 2002, I held a variety of executive positions at a publicly-held fabless semiconductor company originally called S3, Inc. and later called SonicBlue Inc. I held the positions of Chief Technology Officer, Vice President of Systems Integration Products, Senior Vice President of Business Development, and Director of Technology, among others. At the time I joined S3, the company supplied graphics accelerators for more than 50% of the PCs sold in the United States. At S3 I supervised the design of several PC graphics accelerators. During my time at SonicBlue we launched more than 30 new consumer electronics products including devices to support copy-protected video and many of the first commercial products to support copy-protected internet audio content. These included some of the first consumer products to support playback of encrypted content using digital rights management (DRM) based security such as the Rio 600 portable music player. I also worked with Universal Music Group and Sony Entertainment on the development of systems for distribution and management of secure, encrypted content including user-specific licensed downloads and streaming. I also worked on the development of handheld PDA devices, portable wireless tablets, portable CD players, and handheld video players.

18. I have published more than fifty peer-reviewed papers in computer architecture and computer systems and IC design. I also have chaired IEEE and ACM conferences in microarchitecture and integrated circuit design and served as an associate editor for IEEE and ACM journals. I served on the IEEE Computer Society Awards committee. I am an IEEE Fellow, an IEEE Computer Society Distinguished Contributor, and a Member of ACM. I am a named inventor on at least fifty-seven U.S. patents and thirty-seven foreign patents, which are listed in my curriculum vitae. Some of these patents relate to encryption systems.

19. In 2002, I was the invited keynote speaker at the ACM/IEEE International Symposium on Microarchitecture and at the International Conference on Multimedia. From 1990 through 2005, I have also been an invited speaker on various aspects of technology and the PC industry at numerous industry events including the Intel Developer's Forum, Microsoft Windows Hardware Engineering Conference, Microprocessor Forum, Embedded Systems Conference, Comdex, and Consumer Electronics Show, as well as at the Harvard Business School and the University of Illinois Law School. I have been interviewed on subjects related to computer graphics and video technology and the electronics industry by publications such as the Wall Street Journal, New York Times, Los Angeles Times, Time, Newsweek, Forbes, and Fortune as well as on CNN, NPR, and the BBC. I have also spoken at dozens of universities including MIT, Stanford, University of Texas,

Carnegie Mellon University, UCLA, University of Michigan, Rice University, and Duke University.

III. Understanding of Relevant Legal Principles

20. I am not a lawyer, and I will not provide any legal opinions. Although I am not a lawyer, I have been advised that certain legal standards are to be applied by technical experts in forming opinions regarding the meaning and validity of patent claims.

21. I understand that a patent claim is invalid if it is anticipated or obvious in view of the prior art, and that a claim can be unpatentable even if all of the requirements of the claim cannot be found in a single prior-art reference. I further understand that invalidity of a claim requires that the claim be anticipated or obvious from the perspective of a person of ordinary skill in the art at the time the invention was made.

22. I have been informed that a patent claim is invalid if it would have been obvious to a person of ordinary skill in the art. In analyzing the obviousness of a claim, I understand the following factors may be taken into account: (1) the scope and content of the prior art; (2) the differences between the prior art and the claims; (3) the level of ordinary skill in the art; and (4) any so called “secondary considerations” of non-obviousness, if they are present. I am not aware of any evidence of secondary considerations of non-obviousness relevant to the ’875 patent.

I reserve the right to supplement this Declaration if Patent Owner (“PO”) introduces evidence of secondary considerations of non-obviousness.

23. I understand that to prove that prior art or a combination of prior art renders a patent obvious, it is necessary to:

- (1) identify the particular references that, singly or in combination, make the patent obvious;
- (2) specifically identify which elements of the patent claim appear in each of the asserted references; and
- (3) explain why a person of ordinary skill in the art would have combined the references, and how they would have done so, to create the inventions claimed in the patent. I further understand that exemplary rationales that may support a conclusion of obviousness include:

- combining prior art elements according to known methods to yield predictable results;
- simple substitution of one known element for another to obtain predictable results;
- use of known technique(s) to improve similar devices (methods or products) in the same way;
- applying a known technique to a known device (method or product) ready for improvement to yield predictable results;

- “obvious to try” – choosing from a finite number of identified, predictable solutions with a reasonable expectation of success; known work in one field of endeavor may prompt variations of the work for use in either the same field or a different field based on design incentives or other market forces if the variations are predictable to a person of ordinary skill in the art; and
- some teaching, suggestion, or motivation in the prior art that would have led a person of ordinary skill in the art to modify the prior art reference or to combine prior art reference teachings to arrive at the claimed invention.

24. I have been informed that, in considering obviousness, hindsight reasoning derived from the patent-at-issue may not be used.

IV. '875 Patent

25. The '875 patent is titled “Secured personal data handling and management system” and is generally directed to “system, method and personal apparatus for managing highly secured personal data.” ('875 patent, Abstract.)

A. Technical Background

26. The technologies described in the '875 patent related to the storage of secured data and specific mechanisms for permitting authorized access to that secured data. (See '875 patent, Abstract.) Data security has a long history as a field

and includes practices that range from highly theoretical mathematics to a variety of more practical and sometimes even mundane engineering practices. In order to facilitate communications within the field, certain concepts and terms are well understood and consistently used among practitioners. In order to better understand the issues it will be useful to begin with a simplified explanation of basic concepts and vocabulary.

27. The security concept useful to provide background for understanding this technology is “authentication.” Authentication is used to determine whether or not one is permitted to data. It is like a lock on the door of a safe. The contents are protected, but generally unaltered. The contents are protected from unauthorized access but do not participate, themselves, in providing security.

28. The term “authentication” as used in the art of data security has a specific meaning, but is generally related to the plain, English meaning of the word. In ordinary conversation, authentication is generally the process of determining if something is genuine or real. In data security systems, the objective of authentication is to determine if the party trying to access secured data is genuinely who they represent themselves to be, i.e. one who is permitted to access the secure data. In other words, an intruder should not be able to masquerade as someone else. (See Bruce Schneier, “*Applied Cryptography*,” 4, 5-11, 2nd ed. 2006 (“*Applied Cryptography*”; EX-1017).) This is reflected, for example, in the definition for

authentication as “the process by which the system attempts to ensure that the person logging on is the same person to whom the account was issued.” (Bryan Pfaffenberger, “*Webster’s New World Computer Dictionary*,” 4, 10th ed. 2003 (“Webster’s Computer Dictionary”; EX-1018).)

29. This definition reflects the simplified explanation presented above. Authentication is a process by which a system verifies that a user is permitted access to a computer system resource such as protected data. The methods for authentication and commonly grouped into three categories (or “factors”): (1) knowledge-based authentication (*i.e.*, something you know, such as a password), (2) token-based authentication (*i.e.*, something you have, such as a security badge or key FOB), and (3) biometric-based authentication (*i.e.*, something you are, such as unique fingerprints or facial features). (See Ross Anderson, “*Security Engineering*,” 31, 2nd ed. 2008 (“Anderson”; EX-1019); Richard E. Smith, “*Authentication From Passwords to Public Keys*,” 4-6, 7 (2002) (“Smith”; EX-1020); Anil K. Jain et al., “*An Introduction to Biometric Recognition*,” 4 (2004) (“Jain”; EX-1006).) In each case, the general objective is the same. The authentication process distinguishes those who are permitted to access data, documents, and files from those who are not and grants access only to those who are authorized. The same processes are useful whether the protected computer resource is a computer system, a network, or a single data file or document stored on a storage device.

30. Biometric authentication was well known prior to the '875 patent. This includes the basic concepts of enrolling authorized users through initial receipt of biometric inputs, processing those input into unique data parameters, storing those parameters for later use, receiving biometric inputs from a person to be authentication, processing those inputs into data parameters, and comparing those to the data parameters previously received during enrollment to determine if they are a sufficient match to permit access to secured data or other protected resources. (See Smith, 7-35.) Systems and methods for performing biometric authentication using various physical characteristics unique to each individual were well known at the time of the '875 patent, including: fingerprints, facial features, eye features, such as retinal and iris patterns, and voice signatures. (See, e.g., Anderson, 461-476; Smith, 198-201.)

31. Implementing biometric authentication in portable electronic devices, such as cellular phones, was also well known prior to the '875 patent. (See, e.g., R. Ricci et al., *"THE 'SECUREPHONE' A Mobile Phone with Biometric Authentication and e-Signature Support for Dealing Secure Transactions on the Fly,"* 9 (2006) ("SecurePhone"; EX-1026) ("SecurePhone's primary aim is to realise a **mobile phone** prototype - the 'SecurePhone' - in which **biometrical authentication** enables users to deal secure, dependable transactions over a mobile network."); Jain, 4 ("A wide variety of systems requires reliable personal recognition

schemes to either confirm or determine the identity of an individual requesting their services. ... Examples of such applications include secure access to buildings, computer systems, laptops, **cellular phones**, and ATMs. ... **Biometric recognition** or, simply, biometrics refers to the automatic recognition of individuals based on their physiological and/or behavioral characteristics.”); U.S. Patent App. Pub. No 2009/0083847 to Fadell et al. (“Fadell”; EX-1007), Abstract (“This invention is directed to an electronic device with an embedded authentication system for restricting access to device resources. The authentication system may include one or more sensors operative to detect **biometric information** of a user.”), ¶3 (“Electronic devices, and in particular **portable electronic devices**, are used to store personal information.”); U.S. Patent No. 6,788,928 to Kohinata et al. (“Kohinata”; EX-1009), Abstract (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. ... The biodata authentication unit compares the obtained fingerprint data with the fingerprint data of the owner stored in a biodata storage unit 21, and judges whether the user is the proper user”).)

32. At the time of the ’875 patent, there were known problems with implementing single biometric authentication methods. For example,

Two samples of the same biometric characteristic from the same person (e.g., two impressions of a user's right index finger) are not exactly the same due to **imperfect imaging conditions** (e.g., **sensor noise** and **dry fingers**), changes in the user's physiological or behavioral characteristics (e.g., **cuts and bruises on the finger**), **ambient conditions** (e.g., **temperature and humidity**), and user's interaction with the sensor (e.g., finger placement).

(Jain, 6; *see also*, SecurePhone, 14 (“[O]perational conditions generate degradations of input signals due to the variety of environments encountered (ambient noise, lighting variations, ...), while the low quality of sensors further contributes to decrease system performance.”); U.S. Publication No. 2007/0241861 to Venkatanna et al. (“Venkatanna”; EX-1021), ¶7 (“Certain medications can also make biometric test results unreliable. For example, there are drugs, such as atropine, that dilate the eye, making iris identification impossible. Also, certain illnesses can lead to a user falsely being rejected by a biometric system. Having a head cold may change a user's voice sufficiently that he or she will be rejected by a voice-recognition system. Therefore, not all people can be enrolled or can use each biometric test.”).) Thus, it was also recognized that if “the authentication method is fixed to one, it is not possible to always maintain an optimal balance between authentication accuracy and burden on the person to be authenticated.” Certified Translation of Japanese Patent App. Pub. No. P2001-109855A to Mizusawa et al. (“Mizusawa”; EX-1011), ¶5.)

33. A well-known solution to these above problems was requiring authentication using more than one biometric method, commonly referred to as “multimodal” biometric authentication. (See, e.g., SecurePhone, 14 (“[M]ultimodality is expected to strongly enhance person authentication performance in real applications By fusing three different biometric traits, the effect of signal degradation can be counteracted.”); U.S. Publication No. 2010/0115607 to Pratt et al. (“Pratt”), Abstract (“A security processing element stores authentication data corresponding to a plurality of possible authentication modes. ... In an alternative embodiment, the security processing element can randomly select a plurality of authentication modes that are sequentially presented to the user. The user must successfully respond to each of the plurality of requested authentication modes.”), ¶13 (“FIG. 1 illustrates sample systems 100 used to implement the multi-modal authentication system.”); Fadell, ¶28 (“The electronic device may provide any suitable combination of authentication systems, including ... several biometric authentication systems... . In some embodiments, different authentication systems may be associated with different resources, such that a user may provide authentication information for several systems before finally accessing particular restricted resources... .”); Mizusawa, ¶7 (“To solve this problem, the present invention has 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.”); Venkatanna, Abstract (“Once the credentials are authenticated, then the user must take at least two biometric tests, which can be chosen randomly. ... Access desirably will be allowed when both biometric tests are passed.”).)

34. Implementing multi-modal biometric authentication in portable electronic devices, such as cellular phones, was also well known prior to the '875 patent. (*See, e.g.*, SecurePhone, 10 (“The SecurePhone is an innovative prototypal mobile phone platform that gives users the possibility to authenticate by means of a **multimodal ‘biometric recogniser’**, exchange, modify in real time and finally e-sign and securely transmit audio and/or text files. The biometric recognition is based on three modalities: voice, face and handwritten signature recognition.”); Pratt, ¶14 (“The wireless communication device 104 may be a **cell phone**, personal communications system, personal digital assistant (PDA), or the like.”); Fadell, ¶28 (“The **[portable] electronic device** may provide any suitable combination of authentication systems, including ... **several biometric authentication systems...**”).)

35. Another known problem at the time of the '875 patent was unauthorized users (e.g., “hackers”) bypassing biometric authentication through the use of biometrics from an incapacitated, deceased, or dismembered user, as well as use of non-living replicas of biometric inputs from an authorized user known as “spoofs.”

(*See, e.g.*, U.S. Publication No. 2008/0037001 to Yokoyama et al. (“Yokoyama”; EX-1023), ¶3 (“There is apprehension, however, that a possible **fraudulent impostor who steals the registered information to create a sophisticated imitation of a living body** (a **spoof** of finger, iris, or the like) using the stolen information, may disguise him or herself as an individual who he/she claims to be.”); U.S. Patent No. 5,719,950 to Osten et al. (“Osten”; EX-1024), 2:2-12 (“Existing devices can be circumvented by someone, other than the genuine person seeking authentication, actually presenting the biometric pattern of an authorized individual seeking biometric, personal authentication. [¶] For example, a **fingerprint analysis that does not recognize whether the finger is attached to a living human being can be circumvented** by electronic or photographic reconstructions of the fingerprint or dismemberment of the finger.”); Fadell, ¶57 (describing “**spoofing an authorized user’s skin patterns**, for example by placing an image (e.g., a printed image) or a three-dimensional structure (e.g., a polymer cast) adjacent to the authentication system sensor”).)

36. At the time of the ’875 patent, a well-known solution to this “spoofing” problem was the implementation of features to detect “liveness”—*i.e.*, methods to determine whether a biometric input received during an authentication operation came from a living human being. (*See, e.g.*, Yokoyama, ¶8 (“An object of the present invention is to provide a **biometric identification apparatus capable of**

accurately and rapidly performing liveness detection with a simpler structure than that of conventional technology... .”); Fadell, ¶57 (“The authentication system may include any suitable countermeasure for **preventing an unauthorized user from spoofing an authorized user’s skin patterns**, for example by placing an image (e.g., a printed image) or a three-dimensional structure (e.g., a polymer cast) adjacent to the authentication system sensor.”); Venkatanna, ¶75 (“Certain other ‘**anti-theft**’ techniques may be used. For example, the platen may record a temperature **ensuring that a valid live finger is presented; not a copy, not a detached finger.**”); Kohinata, 14:28-36 (“According to the invention, it is judged whether the temperature data obtained by the temperature obtaining units in the cellular phone are within a predetermined condition... . Therefore, the authentication operation is conducted automatically and reliably, but the **authentication does not succeed even when a fingerprint copied on an artificial material is used**, offering a sufficient degree of safety.”); Osten, Abstract (“A personal, biometric authentication system is disclosed. ... The system employs the combination of a unique, inherently specific biometric parameter recognized and compared with stored data and at least one **non-specific biometric parameter of a physiological characteristic recognized and compared with physiological norms**. Positive comparison results in authentication **of an individual that is not incapacitated, dismembered, or deceased.**”).)

B. Overview of the '875 Patent

37. The '875 patent claims priority to U.S. Provisional Application No. 61/313,145, filed on March 12, 2010. While I do not have an opinion about whether the '875 patent is entitled to this priority date, each applied reference was filed or published before March 12, 2010.

38. The '875 patent is titled “[s]ecured personal data handling and management system” and is generally directed to a “system, method and personal apparatus for managing highly secured personal data.” ('875 patent, Abstract.) The personal apparatus “includes a sensor module comprising a plurality of biometric sensors for reading a plurality of personal biological identification parameters of the user and an authentication unit for positive authentication of the user’s personal biological identification parameters stored in the authentication unit.” ('875 patent, Abstract.)

39. Figure 2 of the '875 patent, which I reproduce below, is an embodiment of the disclosed personal apparatus:

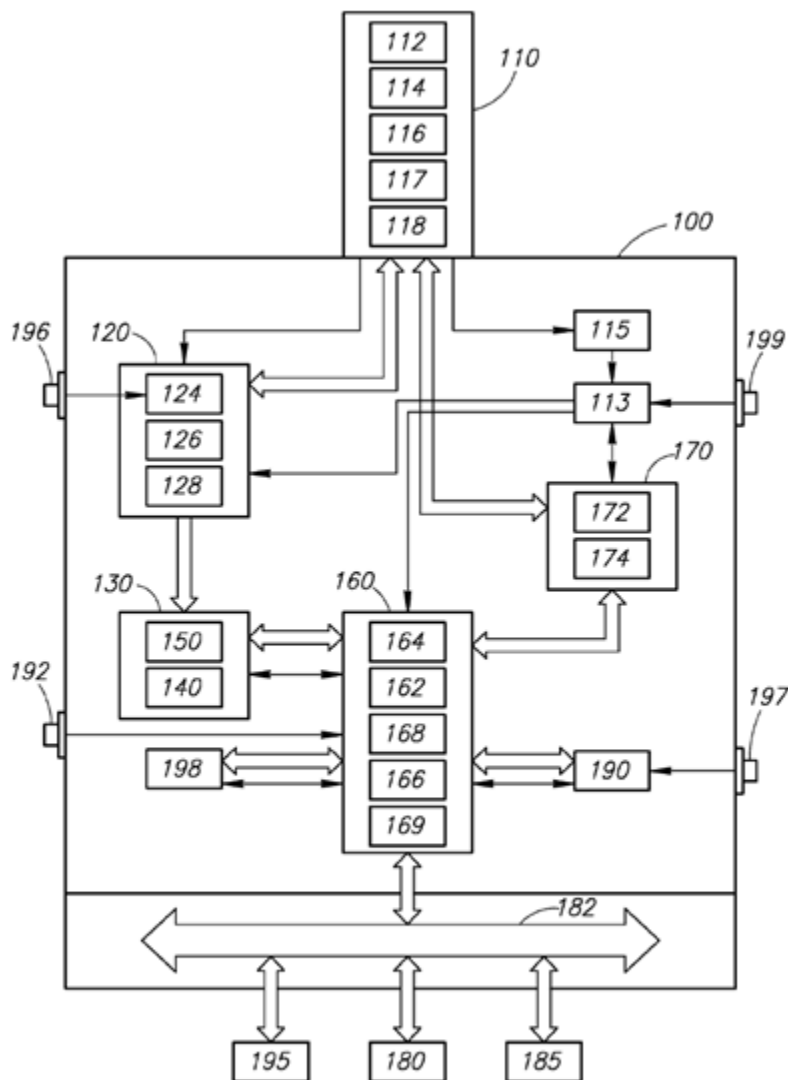


FIG.2

'875 patent, Figure 2

40. “FIG. 2 is a schematic illustration of an embodiment of the present invention block diagram related to one of its possible conceptual modular structure and the internal sub-modules layout and functionality of the present invention apparatus.” ('875 patent, 12:34-37.) Figure 2 illustrates apparatus 100 that is “comprised of at least 5 different main and essential sub modules and may be also

comprised of any combination of additional optional five sub modules.” (’875 patent, 17:3-5.)

41. Figure 2 of the ’875 patent shows that apparatus 100 includes module 120, which comprises sensors 124, 126, and 128. Sensor 124 “is an imaging camera based sensor that images the user specific face pattern or the user’s eye iris, and generates a set of parameters that are specific to the user face pattern, or his iris structure and pattern, and are based on processing and compressing the specific user face or eye iris pattern and colors.” (’875 patent, 17:53-58.) Imaging sensor 126 “is one or more fingerprint sensors that image and analyze the fingerprint of one or two of the user’s fingerprints.” (’875 patent, 18:7-9.)

42. Sensor 128 “is biological life sign detection and measurement dedicated electro optical sensor.” (’875 patent, 18:9-10.) Sensor 128 “measures the heart pulse rate of the user, while holding the apparatus in his palm and also measures the oxygen (O₂) content in % in the user blood at that moment.” (’875 patent, 18:14-16.) The ’875 patent further discloses that sensor 128 “will measure the heart bit rate every time the user will use it and will make a smart moving average of the heart pulse rate results change in time, to act as an adaptive threshold specifically adapted to the apparatus’s personal user typical or normal heart bit rate.” (’875 patent, 18:28-32.) The ’875 patent discloses other embodiments for sensor 128, including a “body temperature measurement sensor, a body pulse rate

measurement sensor, a body O₂ saturation level sensor, an electrodermal activity sensor and a respiration sensor.” (’875 patent, 26:4-7.)

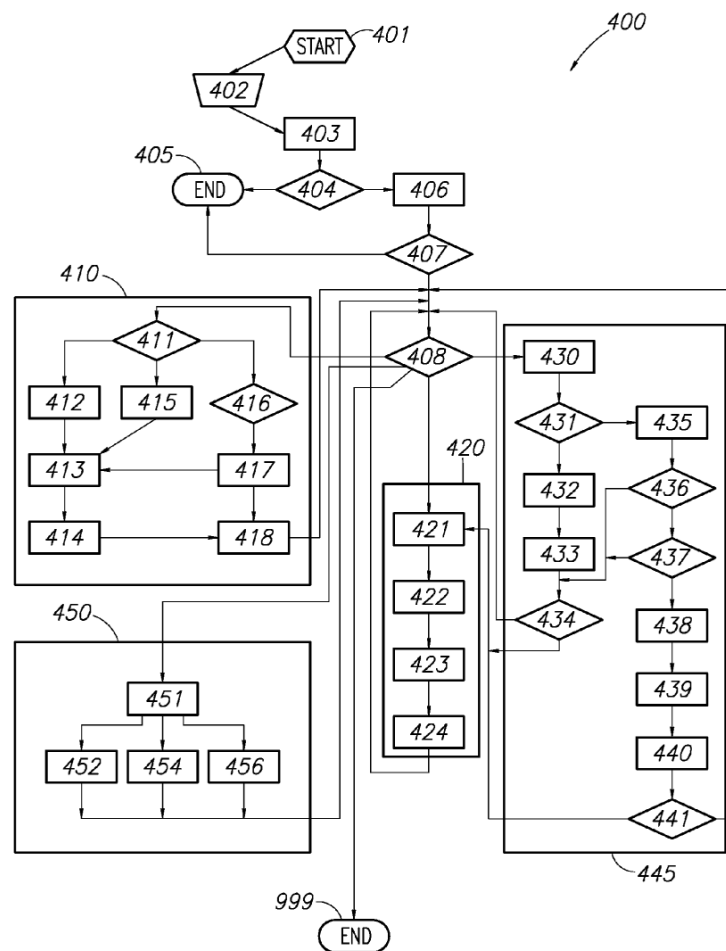
43. Apparatus 100 also includes “[m]ass memory secured data module 170,” which comprises sub-modules 172 and 174. (’875 patent, 21:52-22:2.) “[T]he encryption [software] and hardware sub-modules 172 that will encrypt and compress the user’s highly sensitive private and personal medical and financial data files, as well as carrying out the counter operations of decompression and deciphering of the sub-module stored secured personal data when needed.” (’875 patent, 21:52-21:57.) “The apparatus user sub-module 174 is a very large data storage medium based on solid state memory chips” (’875 patent, 22:3-5.)

44. Apparatus 100 also includes module 130, which “is a hardware and software combined module, containing the apparatus sub module 140 for carrying out the user final authentication by first digitizing and processing the output of module 120 set of sensors and then combining the measured results of the multi sensors tests output to a final “go/no-go” user’s authentication result. Positive authentication result is only achieved when positive results are derived from at least three biological parameters measuring sensors 124, 126, 128, as detailed herein.” (’875 patent, 19:6-14.) “Module 140 will store the registered user’s original, initial registration step, bio sensors measured output for reference and module 140 will also

process the authentication parameters output data formatted reference file from the sensors reference output.” (’875 patent, 20:32-36.)

45. Apparatus 100 also includes module 160, which “is the central controller and data processing unit for apparatus 100.” (’875 patent, 20:15-16.) “Module 160 will control the operation of all the apparatus sub-modules.” (’875 patent, 20:24-25.)

46. Figure 4 of the ’875 patent shows a process for the use of the apparatus “while interphasing [sic] to a cellular phone or a host personal computer for activation of various operations between the cellular phone and the apparatus.” (’875 patent, 12:42-48.)



'875 patent, Figure 4

47. Figure 4 illustrates a flow-chart of a process 400 for the use of the apparatus “while interphasing [sic] to a host personal computer, or to a cellular phone, for activation of various operations between the cellular phone/host computer and the apparatus[.]” ('875 patent, 26:24-29.)

48. The '875 patent discloses that “[i]n stage 403, the user is starting executing [sic] the apparatus 100 user’s authentication sequence through the execution of the holding user biometric required parameters testing process, which

is based on the measurement and processing of at least three biometric parameters....” (’875 patent, 26:40-45.) “In executing a biometric testing process: First tested parameter is a life sign indication sensor output either [sic] his pulse rate that should be normal in a predefined normal non active state range, say 50-80 PPM, or his O₂ saturation level that should be in the normal range of 90-100%, or both should be normal, or his body temperature that should be in a normal range of 36-41 degrees centigrade.” (’875 patent, 26:48-54.)

49. “Second tested parameter is to measure and evaluate the first one of the user’s two biometric measured parameters, such as one or two of his fingers fingerprints, and/or the apparatus holding user face pattern set of measured parameters and/or the user measured and analyzed iris pattern. Third tested parameter is to measure and evaluated [sic] the user second measured biometric parameter, such as one or two of the user fingerprints, and/or the apparatus holding user face pattern set of measured personal parameters, and/or the user’s detected eye iris pattern.” (’875 patent, 26:54-63.)

50. The ’875 patent discloses an embodiment of the apparatus in which “whenever any of the group of life sign indicators detects a critical level, the apparatus is configured to initiate an emergency call to any of a group of registered emergency centers, and send to the registered emergency centers any of a group of data files containing information associated with the user, including the

identification data file of the user, personal medical data file of the user, the measured set of life sign parameters of the user and location of the user.” (’875 patent, 10:54-62.)

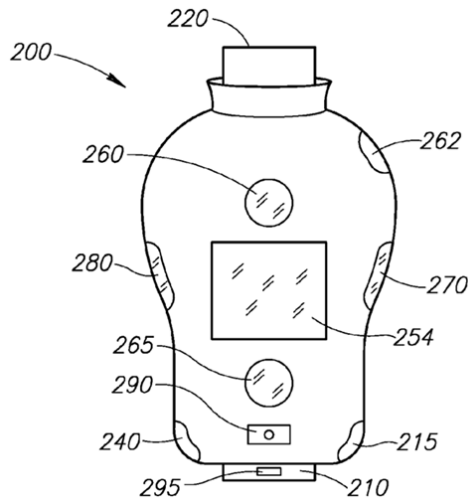
51. Returning to Figure 2, apparatus 100 also includes module 110, which “is the apparatus host terminals, cellular phones and other accessories connection support.” (’875 patent, 17:23-24.) “Module 110 may include any combination of standard USB type and/or non standard data connectors 112 extended out of the of the apparatus case, a wireless Bluetooth communication interphase [sic] 118, a RF medium to short range communication interphase [sic] 117 and another in-room IR communication interphase [sic] 114 data communication interphases [sic] with the outer world, that will support quick and affordable non-contact communication, as well as physical connection of the invention apparatus 100 to any computer terminal, mobile phone devices, ATM and vending machines Etc.” (’875 patent, 17:24-34.) “Such connectors could be ... compatible Mini USB data connectors 116 that one could find in all modern smart-phone cellular phones models.” (’875 patent, 17:34-38.)

52. Apparatus 100 also includes sub-module 190, which “is a RFID receiver and transmitter unit that enables remote identification of the apparatus and its user by other systems which have integrated RFID units.” (’875 patent, 22:24-26.) “Sub-module 190 may support the use of apparatus 100 as an electronic

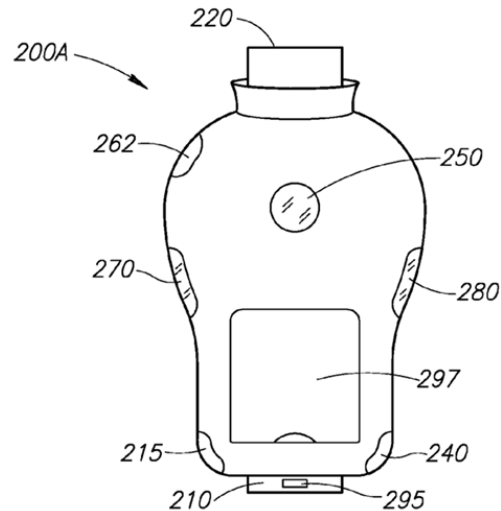
contactless key, to enable safe, secured and easy access through secured entrance gates and doors and in other cases also enables, by pressing the RFID button 197, the use of apparatus 100 for safely and remotely opening and locking private homes and offices keyless RF operated door locks and cars.” (’875 patent, 22:26-34.)

53. Apparatus 100 also includes module 195, which “is a cellular modem acting as the apparatus data communication module that when connected to the apparatus’s computer controller module 160 through data bus 182 and the interphase [sic] sub-module 169, it will support the full scale operation and the execution of all the apparatus 100 functions without the need for connection to an external host computer or to connect the apparatus to a cellular phone.” (’875 patent, 23:65-24:5.)

54. Figures 3A and 3B of the ’875 patent, which I reproduce below, illustrate an embodiment of the disclosed personal apparatus. “Apparatus front view 200 as appears in FIG. 3A, shows the front side view of a preferred embodiment and apparatus view 200A shows the rear side view of the same embodiment of apparatus 100.” (’875 patent, 24:21-24.)



'875 patent, Figure 3A



'875 patent, Figure 3B

55. Figures 3A and 3B include magnetic card element 210, which “is an extending magnetic card thin profile element, that enables interphasing [sic] the apparatus 100 with magnetic cards readers/writers such as those one can find in any shop, or gas stations or ATM machines.” ('875 patent, 24:26-29.) “The extension of the magnetic card element out of the apparatus 100 case can be carried out by the user fully pulling out and extending this element 210, only if first it is enabled by the apparatus controller 160” in Figure 2. ('875 patent, 24:35-39.)

56. Figures 3A and 3B also include element 220, which “is an extendable or fixed USB connector or any similar industrial level available data access connector.” ('875 patent, 25:7-9.)

57. Figures 3A and 3B also include element 295, which “is a fixed or an extendable mini USB data transfer connector or any other industry data mini size connector equivalent.” ('875 patent, 25:14-17.)

58. Returning to Figure 2, apparatus 100 also includes sub-module 198, which “is a RF Transceiver unit that can receive encoded RF commands from a remotely located apparatus’s dedicated charger and data backup unit 1000 described” in Figure 9 of the ’875 patent. (’875 patent, 22:34-37.)

59. Apparatus 100 also includes GPS module 180 “that connects to the controller module 160 through its data bus sub-module 182, wherein the GPS optional module 180 will enable apparatus 100 to accurately measure and calculate the momentary precise geographical position of the apparatus and its user.” (’875 patent, 22:60-65.)

60. The ’875 patent discloses two methods of determining a geographical location that it describes as precise. First, “the user location can be alternatively calculated and transmitted to the user apparatus 100 by the cellular service provider in case the user is connecting his apparatus 100 to a cellular phone 355.” (’875 patent, 23:40-44.) Second, GPS module 180 “is optional in cases of a need to get more precise user’s geographical allocation [sic] data and might be integrated into apparatus 100.” (’875 patent, 23:48-53.)

C. Level of Ordinary Skill in the Art

61. I understand that certain issues relating to the validity of the ’875 patent should be judged from the perspective of a person of ordinary skill in the relevant art, as I discuss below. I have been asked to define the level of a “person of ordinary

skill in the art” or “POSITA” at the time the alleged invention as claimed was made. In deciding the level of ordinary skill, I have considered the following factors, which I have been informed are relevant to the determination of the level of ordinary skill in the art.

- levels of education and experience of persons working in the field;
- types of problems encountered in the art;
- prior art solutions to these problems;
- rapidity with which innovations are made; and
- sophistication of the technology.

62. In my opinion, a person of ordinary skill in the art would have 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.

D. Prosecution Histories

1. U.S. Patent & Trademark Office (USPTO)

63. The ’875 patent issued from U.S. Patent Application Serial No. 12/849,971, filed August 4, 2010. It claims priority to U.S. Provisional Patent No. 61/313,145, filed March 12, 2010.

64. During prosecution, the Examiner rejected originally filed claims 1-37 as anticipated by U.S. Patent Application Publication No. 2009/0062887 to Mass et al. (“Mass”) in a Non-Final Office Action dated February 24, 2012. (Prosecution History of U.S. Patent No. 8,401,875 (“’875 PH”; EX-1002), 100-123.) Applicants filed a Response on June 25, 2012, amending claims 1-2, 6-8, 11-12, 14-15, 17-21, 24, 27, 32-34 and 36 to overcome these rejections, and adding new claim 38. (‘875 PH, 133-148.) Pending independent claim 1 was amended to add the limitations shown below, where the added limitations are underlined, and deleted limitations are struck through.

1. (currently amended) Apparatus for storing and managing personal and secured data and documentation files ~~stored in the apparatus~~ associated with a specific user, comprising:

~~a sensor module comprising~~ a plurality of biometric sensors for reading a plurality of personal biological identification parameters of the user holding the apparatus, said plurality of biometric sensors being integrated within the apparatus ~~said apparatus being uniquely identified with said user~~;

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

~~a processing module in communication with said sensor module for processing said personal biological identification parameters and for processing and managing the personal and secured data and documentation files associated with said user~~;

an authentication unit comprising a second storage unit, ~~in communication with the processing module configured to receive and authenticate the identity of said user by comparing said user's personal biological identification parameters read, by the sensor module and processed by the processing module, with~~ said second storage unit configured to store a pre-recorded set of personal biological identification parameters uniquely associated with the specific user stored in said authentication unit, 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 said second storage unit;

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

~~an encryption module in communication with said processing module for the encryption plus compression and/or decompression plus decryption of said user's data files;~~

~~memory module in communication with said processing module and said encryption module for the storage of said user's data and documentation files;~~

~~communication and data connection means in communication with said processing module for connecting said apparatus with an external device.~~

~~wherein access to the user's stored personal data and documentation files stored in said first storage unit associated with said unique user is only enabled after said authentication unit positively matches each of the plurality authentication of said user's personal biological identification parameters of the user holding the apparatus with the pre-recorded set of personal biological identification parameters stored in said second storage unit by said authentication unit.~~

'875 File History, 133-134

('875 PH, 133-134.) Applicant asserted that three limitations that were amended in claim 1 were not disclosed in Mass. ('875 PH, 149-151.)

65. On August 24, 2012, the Examiner issued a Final Rejection, rejecting pending claims pending 1-38 claims as obvious over Mass in view of U.S. Patent. No. 6,539,380 to Moran ("Moran"; EX-1008). ('875 PH, 161-184.) Examiner asserted Moran taught the three limitations, and that it "would have been obvious to one of ordinary skill in the art at the time the invention was made to combine wireless patient communicator for use as taught by Mass ('887; [A]bstract) and device, method for data access control as taught by Moran ('380; Abstract) in order to

authenticate the device and the combination would have yielded predictable result.”
(’875 PH, 162-163.)

66. Applicant initiated an interview with Examiner. After the interview, Applicant amended claim 1 to incorporate the “life signs detector” limitation of pending claim 3 and to include a new “critical level” limitation, as shown below.

1. (currently amended) Apparatus for storing and managing personal and secured data and documentation files associated with a specific user, comprising:

- 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;
- 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;
- a first storage unit for the storage of said user’s data and documentation files;
- 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;
- a processor in communication with said plurality of biometric sensors, said first storage unit and said authentication unit;
- 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

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.

'875 File History, 192-193

67. Similar amendments were made to independent claims 21 and 32. ('875 PH, 197-198, 202-203.)

68. The Examiner allowed the pending claims, stating in the Notice of Allowance that the prior art failed to disclose the “life signs detector” limitation.

However, the prior arts fail to disclose 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.

Claims 2, 4-20, 38-39 are dependent from claim 1 and are allowed for the same reason given above.

Claims 21-31 incorporate all the limitations of claim 1 and are allowed for the same reasons given above.

Claims 32-37 incorporate all the limitations of claim 1 and are allowed for the same reasons given above.

'875 File History, 222-223

69. The Examiner further explained that all other pending claims were allowed for the same reason. ('875 PH, 222-223.) However, as I explain below, the same claims that were allowed in the US were rejected and subsequently not allowed during prosecution in Europe in view of Fadell that was not in front of the USPTO Examiner during examination of the '875 patent.

2. European Patent Office (EPO)

70. On March 10, 2011, PO filed International Patent Application No. PCT/IB2011/051002, which claimed priority to the same provisional application to which the '875 patent claims priority: U.S. Provisional Patent Application No. 61/313,145 ("EPO PH"; EX-1005). (EPO PH, 1.) On July 12, 2012, PO entered this international application into the European phase before the European Patent Office, assigned as European Application No. 11/752,936.2. (EPO PH, 87.)

71. On April 29, 2013, before examination of the European patent application commenced, **Applicant amended the pending claims to match claims 1-15 of the '875 patent.** (EPO PH, 144-175.)

72. On May 2, 2014, the Examiner issued a European Search Opinion rejecting pending claims 1-15. (EPO PH, 188-192.) **The Examiner rejected pending claim 1 for lack of inventive step over U.S. Patent Application Publication No. 2009/0083847 A1 to Fadell et al. ("Fadell"; EX-1007). Fadell was not considered by the USPTO Examiner during prosecution of the '875**

patent. The remaining pending claims were rejected for lack of unity of invention. (EPO PH, 192-198.)

73. Separately, the Examiner asserted that pre-examination amendments “introduce subject - matter which extends beyond the content of the application as filed, contrary to Article 123 (2) EPC[.]” (EPO PH, 188.) For the “critical level” limitation of pending claim 1, the Examiner noted:

1.7. The applicant indicated originally filed claims 1 and 3 as basis for new claim 1. However, the last feature of present claim 1, namely, ‘whenever any of said life signs detectors detects a critical level... the apparatus is configured to prevent access...’ is not present neither in claim 1 nor in claim 3 in the originally filed set of claims.

(EPO PH, 190.)

74. Applicant responded on August 28, 2014, amending claim 1 and other claims in response to the Added Subject Matter objections and providing a table with support for the phrases Examiner identified as new subject matter. (EPO PH, 204, 208-209.) For the “critical level” limitation, Applicant identified 40:7-41:3 of the specification provided support. (EPO PH, 204.) Applicant further asserted that Fadell “fails to disclose each and every one of the following features of” amended claim 1, reciting the entire claim, but did not providing further explanation. (EPO PH, 204-205.)

75. On January 5, 2015, the Examiner issued a Communication from the Examining Division, maintaining rejection of claims 1-15. (EPO PH, 236-241.) Here, the Examiner found the claim 1 limitation “life signs detector detects a critical level ... prevent access” was “not present in the cited passage, nor is it directly and unambiguously derivable from it. This newly generated subject-matter is novel when compared with the original application[.]” (EPO PH, 238.) The Examiner also noted that Applicant argues Fadell “fails to disclose each and every one of the features of claim 1, without identifying the features he is actually disputing.” (EPO PH, 239-240.) The Examiner “carefully re-considered the arguments” from its previous communication and concluded that amended claim 1 lacked an inventive concept in view of Fadell and “matter[s] of general knowledge” that “cannot represent a single general inventive concept.” (EPO PH, 239-241.)

76. On May 14, 2015, Applicant submitted a Reply and amended the claims. (EPO PH, 242-272.) Among other amendments, Applicant amended claim 1 to remove the “life signs detector detects a critical level ... prevent access” limitation that was the subject of the Examiner’s added subject matter objection. (EPO PH, 261.)

77. The Examiner continued to maintain its objections to the pending claims, and the application was abandoned on December 12, 2018. (EPO PH, 713.)

78. Accordingly, the claims—as currently allowed in the US—failed to survive examination in Europe in view of Fadell, that was not in front of the USPTO Examiner.

E. Claim Construction

79. I understand that “claim construction” is the process of determining a patent claim’s scope and meaning. I understand that the Patent Office applies the same claim construction standard used in district courts which seeks to give claim terms their plain and ordinary meaning to a POSITA at the time of the claimed invention in view of the claims, specification, and prosecution history. I also understand that if the patent applicant gave a term a special meaning in the specification or during prosecution, then the special meaning should be used.

80. I understand that a “means-plus-function” claim term is a term that recites a particular function but does not recite a sufficient structure for performing that function. I understand that means-plus-function terms are limited to the function recited in the claim(s) and the specific structure disclosed in the patent’s specification for performing that function, as well as structures equivalent to the disclosed structures.

81. I understand a claim limitation is presumed to be a means-plus-function limitation when it explicitly uses the term “means for” and includes functional language. I further understand that, when a claim limitation lacks the word “means,”

although there is a presumption that it is not means-plus-function, the presumption can be overcome if the claim term fails to recite sufficiently definite structure or else recites function without reciting sufficient structure for performing that function.

82. I understand that the construction of a means-plus-function limitation is a two-step approach. The first step is to identify the claimed function, staying true to the claim language and the limitations expressly recited by the claims. The second step is to ascertain the corresponding structure(s) identified in the written description that perform those function(s). A disclosed structure is corresponding only if the specification clearly links or associates that structure to the function recited in the claim.

83. I have reviewed the claims, specification, and file history of the '875 patent. I did not find any explicit definition of claim terms.

84. I have also been asked to determine if there are any particular claim terms that should be construed for the Board to understand how the prior art references read on the challenged claims. I have not identified any such claim terms other than the “means-plus-function” terms analyzed below.

1. “first storage unit” (Claim 1)

85. This term appears in Claim 1 of the '875 patent. I was informed and I understand that this term is a “means-plus-function” term. As I discussed above, I understand that for “means-plus-function” terms, the proper claim construction must

include the claimed “function” and the “corresponding structure” that is disclosed in the specification of the patent (and equivalents). I set forth the function and structure below:

Function: “stor[ing] of said user’s data and documentation files.”

Structure: memory and equivalents.

86. The specification identifies (1) “memory sub-module 174” and (2) “sub-module 150” as “stor[ing] of said user’s data and documentation files.” (’875 patent, 20:24-29 (“Module 160 will control the operation of all the apparatus sub-modules, but also will do through sub-module 172 the encryption and the deciphering data processing work carried out by memory sub-module 172 upon storage and retrieval processes of all **the highly secured user’s personal data files, stored in the secured mass memory sub-module 174**.”); 19:14-16 (“[A] **sub-module 150** that stores a set of data files that are defined by the user as private, yet non-secured...”); 19:48-50 (“[T]he user’s name, his ID data and the user emergency medical data, **as stored in memory module 150**”).)

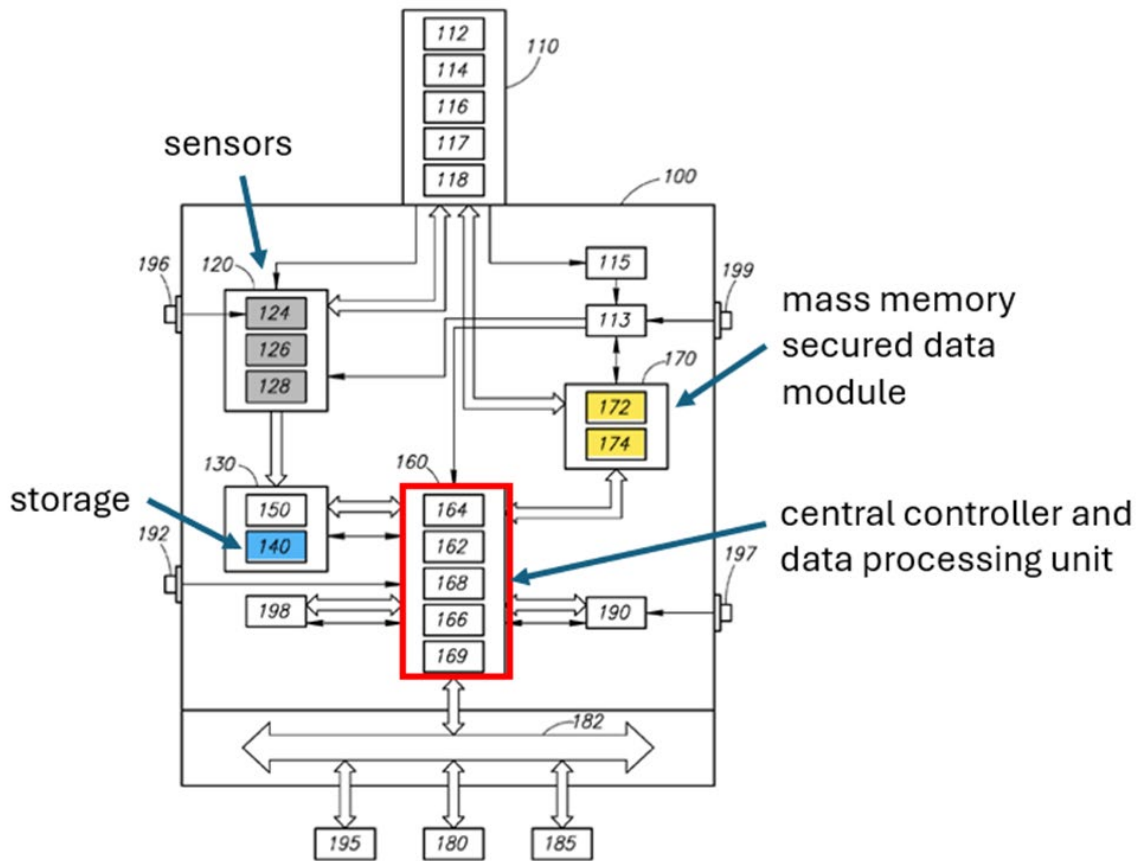


FIG.2

'875 patent, Figure 2

87. The specification describes that sub-module 174 stores encrypted data. ('875 patent, 20:24-29 ("Module 160 will control the operation of all the apparatus sub-modules, but also will do through sub-module 172 the encryption and the deciphering data processing work carried out by memory sub-module 172 upon storage and retrieval processes of all the highly secured user's personal data files, stored in the secured mass memory sub-module 174."); 21:61-63 ("[T]he encryption

keys required to encrypt and decipher the secured data in sub-module 174 will be stored in a separate special memory partition...”).)

88. The specification discloses that sub-module 150 can hold un-encrypted data. (’875 patent, 19:14-17 (“This module also includes a sub-module 150 that stores a set of data files that are defined by the user as private, yet non-secured, so they may be stored in the original digital format without encryption.”).)

89. Accordingly, the specification discloses that (1) encrypted data that can be stored on a storage medium based on solid state memory chips or erasable multiple-use memory device (sub-module 174) and (2) encrypted data can be stored in memory (sub-module 150).

90. I note that the *encryption unit*, that encrypts the data is introduced in dependent claim 20:

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

an **encryption unit** in communication with said processor **for the encryption** plus compression and for the decompression plus decryption of said user's data files.

91. The structure for sub-module 150 is “memory.” (’875 patent, 19:48-50.) The specification, likewise identifies examples of types of memory that can be used in specific sub-module 174. (’875 patent, 22:3-7 (“[S]ub-module 174 is a very large data storage medium based on **solid state memory chips**... [S]ub-module 174 may be a new generation of **erasable multiple-use memory**....”).)

2. “second storage unit” (Claim 1)

92. This term appears in Claim 1 of the '875 patent. I was informed and I understand that this term is a “means-plus-function” term. As I discussed above, I understand that for “means-plus-function” terms, the proper claim construction must include the claimed “function” and the “corresponding structure” that is disclosed in the specification of the patent (and equivalents). I set forth the function and structure below:

Function: “stor[ing] a pre-recorded set of personal biological biometric identification parameters uniquely associated with the specific user.”

Structure: memory and equivalents.

93. The specification identifies “sub-module 140” as “storing a pre-recorded set of personal biological biometric identification parameters uniquely associated with the specific user.” ('875 patent, 20:32-35 (“**Module 140** will store **the registered user's original**, initial registration step, **bio sensors measured output** for reference....”); 24:45-50 (“[W]hile comparing the measured bio sensed set of parameters of the apparatus present holder, to **the set of parameters, stored in the apparatus's authentication memory sub-module 140** in FIG. 2 for the relevant bio sensed parameters of the apparatus 100 legitimate user and owner.”).)

94. For sub-module 140, the specification describes it as a “memory module” or “memory unit.” (’875 patent, 24:47-48 (“[T]he set of parameters, stored in the apparatus’s authentication **memory sub-module 140** in FIG. 2....”); 27:1-3 (“[A]nalyzed and stored identical at least three parameters of the same apparatus owner stored in **memory unit 140**.”).)

3. “authentication unit” (Claim 1)

95. This term appears in Claim 1 of the ’875 patent. I was informed and I understand that this term is a “means-plus-function” term. As I discussed above, I understand that for “means-plus-function” terms, the proper claim construction must include the claimed “function” and the “corresponding structure” that is disclosed in the specification of the patent (and equivalents). I set forth the function and structure below:

Function: “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.”

Structure: memory and processor programmed to perform the recited function.

96. The specification identifies “sub-module 140” as “carrying out the user final authentication.” (’875 patent, 19:6-8.) The specification refers to “submodule

140” both as a “memory unit” (’875 patent, 27:3) and as “authentication sub-module.” (’875 patent, 20:37.) Accordingly, a POSITA would have understood that the corresponding structure of the “authentication unit” would include both components. Moreover, claim 1 recites that the “authentication unit *compris[es]* a second *storage unit*.”

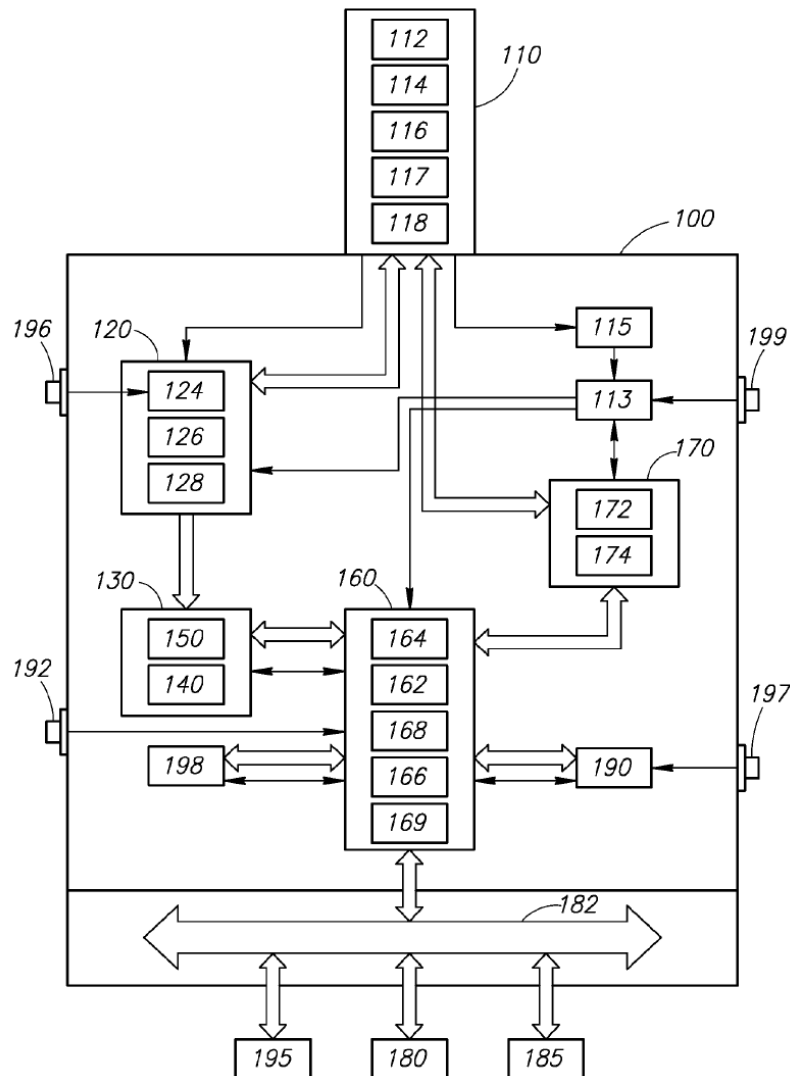


FIG.2

’875 patent, Figure 2

97. With regard to the “memory unit” component, it stores the “pre-recorded set of personal biological biometric identification parameters.” (’875 patent, 24:45-50 (“[C]omparing the measured bio sensed set of parameters of the apparatus present holder, to the set of parameters, stored in the apparatus's authentication memory sub-module 140 in FIG. 2 for the relevant bio sensed parameters of the apparatus 100 legitimate user and owner.”).) Accordingly, similar to the second storage unit, as I explained above the corresponding function and structure are:

Function: “stor[ing] a pre-recorded set of personal biological biometric identification parameters uniquely associated with the specific user.”

Structure: memory and equivalents.

98. With regard to the “authentication sub-module” component, the words “module” and “sub-module” are generic and do not convey any structure to a POSITA, while the modifier “authentication” would not attach a particular structure to “module” or “sub-module.” In such cases, I have been informed and understand that the corresponding structure is a processor programmed or configured to implement the algorithm or instructions disclosed in the specification that perform the claimed function.

99. In connection with Figure 4, the specification describes an algorithm for performing authentication, according to which, multiple personal biological

biometric identification parameters are compared to stored personal biological biometric identification parameters. Specifically, according to one embodiment, *at least three* parameters are compared to stored parameters. For example, the specification discloses that:

In stage 403, the user is starting executing the apparatus 100 user's authentication sequence through the execution of the holding user biometric required parameters testing process, which is based on the measurement and processing *of at least three biometric parameters* (as described herein in one preferred embodiment).

('875 patent, 26:40-45.)

In Stage 404, *the at least three presently measured parameters are authenticated when compared* and analyzed by the apparatus 100 internal controller and data processing unit 160. The *at least three presently measured parameters are compared to the previously measured, analyzed and stored identical at least three parameters of the same apparatus owner stored in memory unit 140*, Upon authentication a positive response is created by the apparatus 100 and it continues to stage 406.

('875 patent, 26:64-27:5.)

100. According to another embodiment, at least two parameters are compared to stored parameters. For example, the specification discloses that “in another embodiment, fewer biometric parameters, such as *at least two parameters*, may be processed.” ('875 patent, 26:46-48.)

101. Accordingly, authentication is conducted “based on the measurement and processing” of “biometric parameters.” (’875 patent, 26:40-45.) Therefore, the corresponding structure is memory and processor programmed to perform the recited function.

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)

102. This phrase appears in Claim 4 of the ’875 patent. As I discussed above, I understand that for “means-plus-function” terms, the proper claim construction must include the claimed “function” and the “corresponding structure” that is disclosed in the specification of the patent (and equivalents). I set forth the function and structure below:

Function: “communicating with an external device.”

Structure: any combination of data connectors extended out of apparatus case, 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.

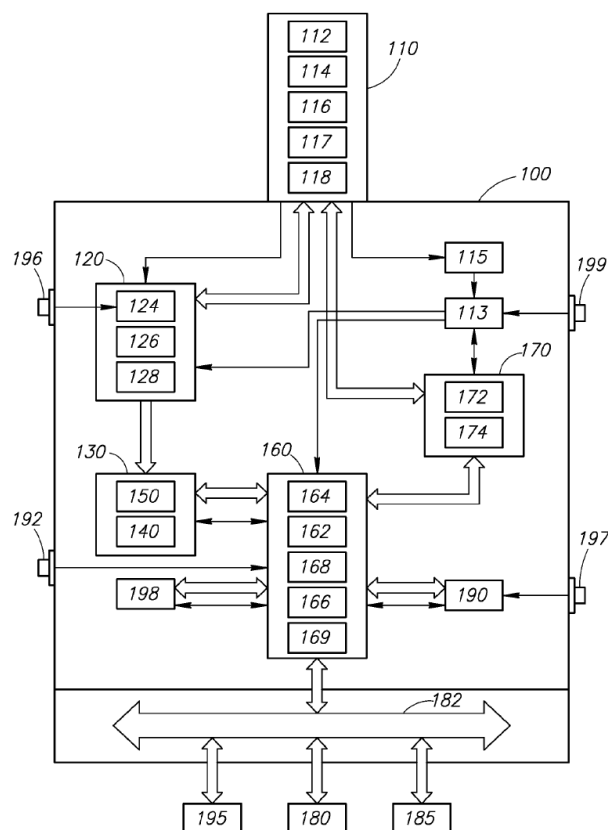


FIG.2

'875 patent, Figure 2

103. In connection with Figure 2, the specification states that controller module 160 “will control the operation of all the apparatus sub-modules.” ('875 patent, 20:24-25.) The specification further states that controller module 160 “also includes an embedded SW sub module 162 that has the function to support the apparatus 100 automatic adaptation required to enable two way communication with all commonly used Operating Systems (OS) software packages, resident on the external host computer or on the cellular phone that the user has linked his apparatus 100 to.” ('875 patent, 20:47-52.)

104. Also in connection with Figure 2, the specification identifies “[m]odule 110” as “the apparatus host terminals, cellular phones and other accessories connection support.” (’875 patent, 17:23-24.) The specification states that “[m]odule 110 may **include any combination of** standard USB type and/or non standard data connectors 112,” “a wireless Bluetooth communication interphase [sic] 118,” “RF medium to short range communication interphase [sic] 117,” “in-room IR communication interphase [sic] 114,” a “[m]ini USB data connectors 116.” (’875 patent, 17:24-37.) With regard to “module 110,” even though the word “module” is generic and does not convey any structure to a POSITA, the components included in module 110 individually would connote structures to a POSITA because they describe well-understood methods and protocols for communicating with external devices, including Bluetooth, radio frequency (RF) communication, infrared (IR) communication, RF Identification (RFID), and universal serial bus (USB). Further, the specification described exemplary external device for that apparatus 100 may communicate with through these structures:

Such connectors could be USB data connectors 112 integrated in most standard PC computers and laptops and mini USB, or compatible Mini USB data connectors 116 that one could find in all modern smart-phone cellular phones models. The preferred embodiment apparatus shown in this figure has in the terminal connection unit 110 a Bluetooth wireless communication interphase circuit 118 to enable easy and quick data communication and non-contact short range connection to most

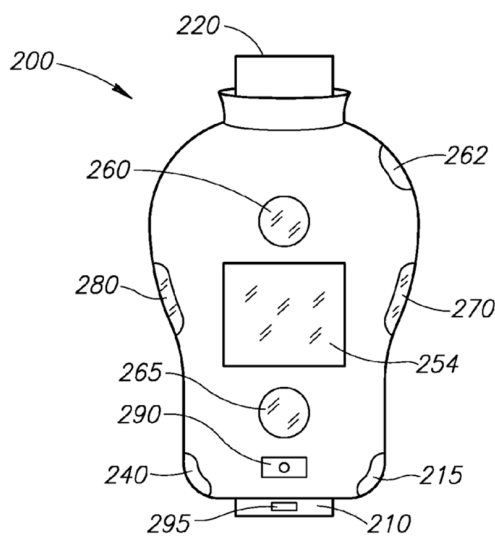
market's available cellular phones, to some models of laptops and notebooks that have built-in wireless Bluetooth data communication capability and through available Bluetooth USB plug-in, token/dongle type devices, that enable contact-less data communication with all modern PC and laptop/notebook, types of host computers.

('875 patent, 17:34-48.)

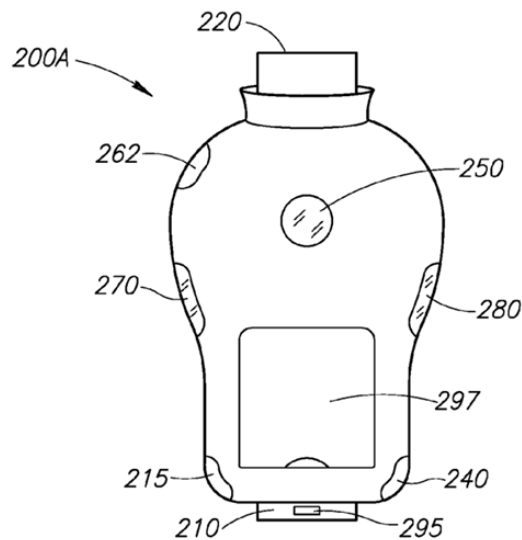
105. Also in connection with Figure 2, the specification identifies sub-modules 190 as “a RF Transceiver unit that can receive encoded RF commands from a remotely located apparatus’s dedicated charger and data backup unit 1000 described in FIG. 9.” ('875 patent, 22:34-37.) The specification similarly identifies sub-module 198 as “RF Transceiver unit that can receive encoded RF commands from a remotely located apparatus's dedicated charger and data backup unit 1000 described in FIG. 9.” ('875 patent, 22:34-39; *see also* '875 patent, 22:52-59 (“Power supply unit 113 ... may provide the voltages required to the sensors unit 120 and to the RF transceiver and RF ID units 198 and 190.”).)

106. With regard to the “sub-module” component of sub-modules 198 and 190, even though the word “sub-module” is generic and does not convey any structure to a POSITA, the specification’s description of these sub-modules as RF transceiver and RF ID units” would have connoted structure to a POSITA. ('875 patent, 22:52-59.)

107. Also in connection with Figure 2, the specification identifies module 195 as “a cellular modem acting as the apparatus data communication module that when connected to the apparatus’s computer controller module 160 through data bus 182 and the interphase sub-module 169.” (’875 patent, 23:65-24:2.) Again, with regard to the “module” component of module 195, even though the word “module” is generic and does not convey any structure to a POSITA, the specification’s description of these module 190 as a “cellular modem” would have connoted structure to a POSITA. (’875 patent, 23:65-24:2.)



’875 patent, Figure 3A.



’875 patent, Figure 3B.

108. In connection with Figures 3A and 3B, element 210 is identified as “an extending magnetic card thin profile element, that enables interphasing [sic] the apparatus 100 with magnetic cards readers/writers such as those one can find in any

shop, or gas stations or ATM machines.” (’875 patent, 24:25-29; *see also* ’875 patent, 24:29-35 (“Magnetic card element 210 ... can be extended out of the housing by the user for easy interphasing [sic] to and interaction with any magnetic card reader and then exchanging data and further enabling the execution of a transaction through any ATM machine or any purchasing point magnetic card reader.”).)

109. With regard to the “element” component of the “extending magnetic card thin profile element,” even though the word “element” is generic and does not convey any structure to a POSITA, the specification’s description of these element 210 as an “extending magnetic card thin profile” would have connoted structure to a POSITA. (’875 patent, 24:25-29.)

110. In connection with Figures 3A and 3B, the specification identifies element 220 as “an extendable or fixed USB connector or any similar industrial level available data access connector.” (’875 patent, 25:7-9.) Element 220 “can be used when the user wants to connect the apparatus 100 to his host PC computer or to connect to any multi-user computerized server based system, using a computer terminal that has data interphasing [sic] capability with a data connector of any kind integrated into the computer terminal.” (’875 patent, 25:9-14.)

111. In connection with Figures 3A and 3B, the specification identifies element 295 as “a fixed or an extendable mini USB data transfer connector or any other industry data mini size connector equivalent, that is integrated into all modern

cellular phones, a connector that can be used when the apparatus 100 user wants to connect to the outer world through his cellular phone.” (’875 patent, 25:14-20.)

112. Finally, claim 10, which depends from claim 4 where this claim term appears, recites is full:

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.

(’875 patent, Claim 10 (40:43-52).)

113. For purposes of my analysis here, I do not believe express claim constructions are necessary for the other terms of the challenged claims, because the prior art renders the claims obvious under any of the proposed constructions identified above or any other reasonable construction. Accordingly, my analysis below discusses these proposed constructions and explains why, under each of them, the limitations are disclosed and rendered obvious by the prior art.

V. GROUND 1: The Combination of Fadell and Moran Renders Obvious Claims 1, 4, 7, 10, 14, and 19

114. Fadell, which published March 26, 2009, and Moran, which issued March 25, 2003, disclose or at least suggest every limitation of claims 1, 4, 7, 10, 14, and 19.

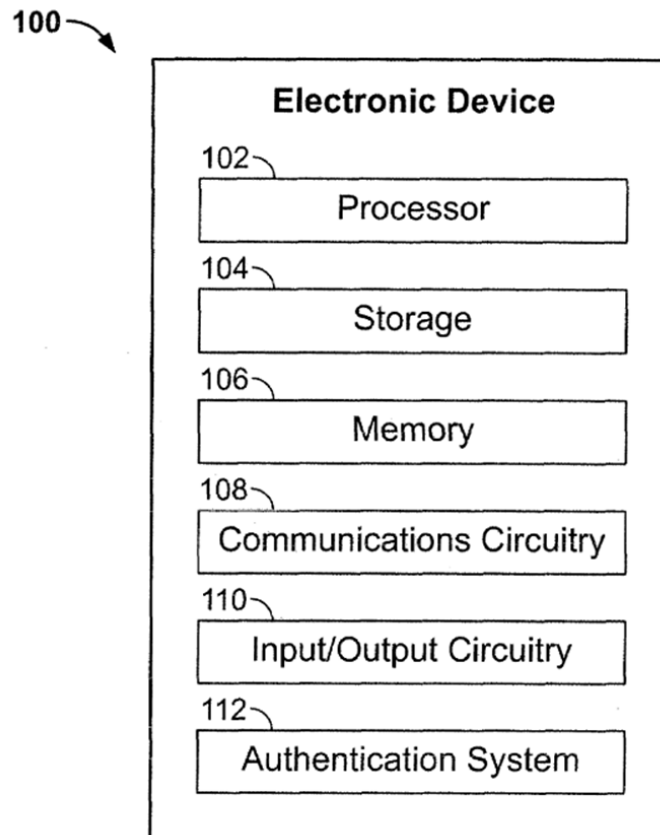
A. Overview of the Combination

1. Fadell

115. Fadell explains that electronic devices, such as cellular telephones, PDAs, smartphones or similar devices “are used to store personal information” including “contacts, e-mail, calendar information, documents, and other information.” (Fadell, ¶3.) Fadell notes that even for non-confidential information, users may still wish to keep the information confidential. (Fadell, ¶3.) Fadell is therefore “directed to an electronic device with an embedded authentication system for restricting access to device resources.” (Fadell, Abstract.)

116. 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. (Fadell, ¶29.) Although Figure 1 only shows one authentication system 112, Fadell teaches the electronic device “may provide any suitable combination of authentication systems, including ... several biometric authentication systems.” (Fadell, ¶28; *see also*, Fadell, ¶41 (“For example, the electronic device may require

a user to satisfy several authentication systems prior to providing access to an application or data”), ¶52 (“A user may in addition select one or more authentication systems to satisfy before providing access to the resource”).)



Fadell, Figure 1

117. Control processor 102 “include[s] any processing circuitry operative to control the operations and performance of electronic device 100.” (Fadell, ¶30.) Memory 106 “stor[es] data used to operate electronic device applications, or any type of data that may be stored in storage 104.” (Fadell, ¶32.) Communications

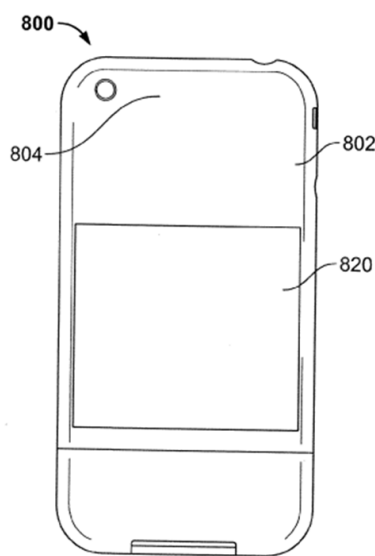
circuitry 108 may permit electronic device 100 “to communicate with one or more servers or other devices using any suitable communications protocol.” (Fadell, ¶33.)

118. Storage 104 stores “media data ... , application data ... , firmware, user preference information data (e.g., media playback preferences), authentication information (e.g. libraries of data associated with authorized users), lifestyle information data ... , exercise information data (e.g., information obtained by exercise monitoring equipment), transaction information data (e.g., information such as credit card information), wireless connection information data (e.g., information that may enable electronic device 100 to establish a wireless connection), subscription information data (e.g., information that keeps track of podcasts or television shows or other media a user subscribes to), contact information data (e.g., telephone numbers and email addresses), calendar information data, and any other suitable data or any combination thereof.” (Fadell, ¶31.)

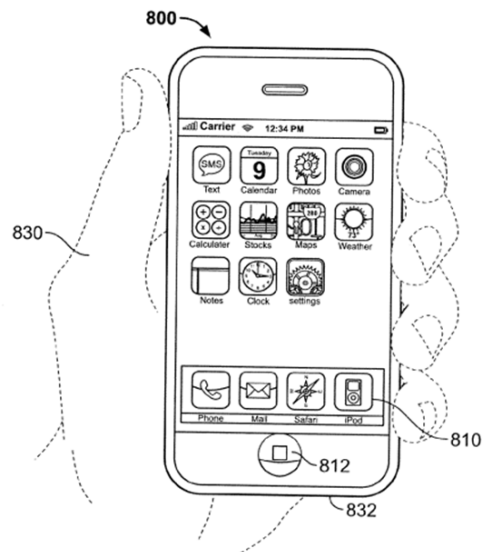
119. Authentication system 112 “include[s] any suitable system or sensor operative to receive or detect an input identifying the user of device 100.” (Fadell, ¶39.) For example, authentication system 112 includes “a skin-pattern sensing mechanism, an optical system for identifying users based on their 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.” (Fadell, ¶39.) Fadell describes

several exemplary implementations of these authentication system sensors in electronic devices.

120. Fadell describes an electronic device integrating sensors used for authenticating handprints and fingers. (See Fadell, Figures 8A-8B (below).) In this exemplary device, sensor 820, which may “include a two-dimensional sensor”, is embedded in the device’s back surface 804. (Fadell, ¶67.) A sensor, “placed behind a home button of a portable media player or cellular telephone (e.g., button 812, [Figure] 8B),” is “operative to detect features of a user's fingerprint to identify the user.” (Fadell, ¶64.)



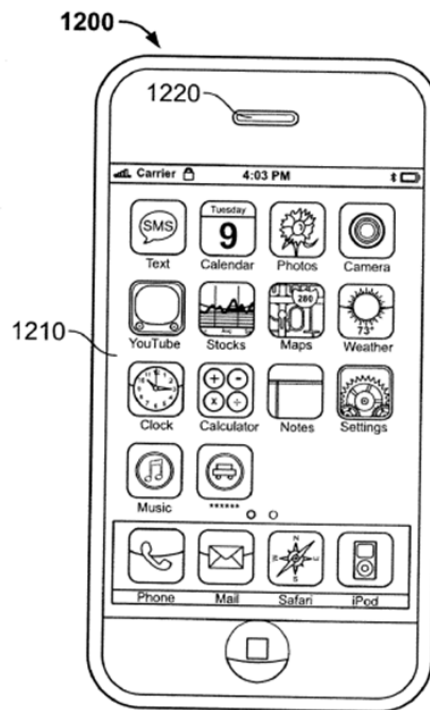
Fadell, Figure 8A



Fadell, Figure 8B

121. Fadell also describes an electronic device incorporating sensors used for authenticating a user’s face. (Fadell, Figure 12.) The sensor for detecting facial

features “may include a camera or other sensor provided with the electronic device for a different purpose (e.g., an embedded webcam for chatting)” and “may be located at any suitable position on the electronic device.” (Fadell, ¶73.) Fadell teaches that the processing component of authentication system 112 “identif[ies] faces by analyzing the relative to position and size of a user’s head, nose, mouth, ears, cheekbones, jaw, or any other attribute of the user’s face.” (Fadell, ¶72.)



Fadell, Figure 12

122. Authentication system 112 also includes sensors usable to “authenticate users based on attributes or qualities of their voices,” including detection of “a particular voice pitch or voice signature.” (Fadell, ¶77.) To authenticate a user based on attributes or qualities of their voice, “any suitable component for authenticating

a user, including for example a microphone” that “may be primarily used for other purposes (e.g., telephone communications or video conferencing).” (Fadell, ¶77.)

123. 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.” (Fadell, ¶57.)

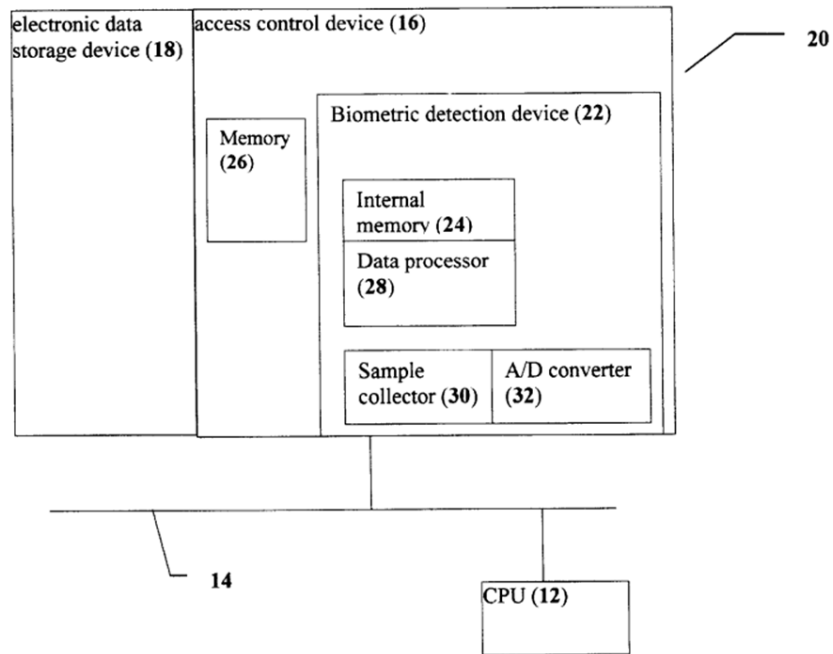
124. “To prevent unauthorized access to data or information stored in memory or storage, the electronic device may direct an authentication system to identify the user and authorize access to requested resources.” (Fadell, ¶41.) Specifically, a user “select[s] one or more authentication systems to satisfy before providing access to the resource.” (Fadell, ¶52.) For example, based on user configurations, “the electronic device may require a user to satisfy several authentication systems prior to providing access to an application or data.” (Fadell, ¶41.) When specified, the “several authentication systems may be used sequentially before access to particular restricted resources is provided.” (Fadell, ¶91.)

2. Moran

125. Fadell “is directed to an electronic device with an embedded authentication system for restricting access to device resources.” (Fadell, Abstract.) Fadell broadly describes that the “authentication system” includes “a system operative to detect and authenticate a user” based on biometric features of the user. (Fadell, ¶25, *see also*, Fadell, ¶41 (“To prevent unauthorized access to data or information stored in memory or storage, the electronic device may direct an authentication system to identify the user and authorize access to requested resources.”) Fadell teaches that the authentication system includes “any suitable system or sensor operative to receive or detect an input identifying the user of” a device. (Fadell, ¶39.) However, Fadell fails to disclose other implementation details including implementation of the portion of the system performing the user authentication process/analysis. Moran provides details of a system that performs biometric authentication.

126. Moran, like Fadell, is directed to “data access control, particularly for 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.” (Moran, 1:11-14.) Moran’s system, illustrated in Figure 3 below, includes an “access control device 16” which is “implemented as a chip, with a non-volatile memory which is both readable and writable, such as a flash memory device

for example, some type of input for receiving a request for data, and a microprocessor.” (Moran, 7:6-13.)



Moran, Figure 3

127. Access control device 16 includes memory 26 and biometric detection device 22 which has an internal memory 24, data processor 28, sample collector 30, and A/D converter 32. Biometric detection device 22 is directly associated with the type of biometric being performed. For example, biometric detection device may be “any type of device which is capable of capturing 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, devices for measurement of ECG/EEG,

pressure measurements on one or more body organs, voice recognition, skin or other body chemical analysis.” (Moran, 4:62-67.)

128. The sample collector 30 of a biometric detection device “collect[s] a sample of the biological parameter.” (Moran, 11:3-5.) For example, when the biometric detection device is a fingerprint detection device, sample collector 30 “preferably includes a thermal imaging fingerprint sensor for collecting the fingerprint data.” (Moran, 11:5-7.) Moran’s sample collector 30 is therefore equivalent to Fadell’s sensors.

129. Data processor 28 performs the authentication processing for the biometric detection device. (*See, e.g.*, Moran, 11:31-33 (describing that digitized collected data is sent to data processor 28 for analysis).) For example, in the context of a fingerprint detection device, Moran teaches that the collected “fingerprint data is then optionally analyzed by biometric detection device 22, and more specifically by a software module which is stored in internal memory 24 and which is operated by data processor 28.” (Moran, 11:8-11.)

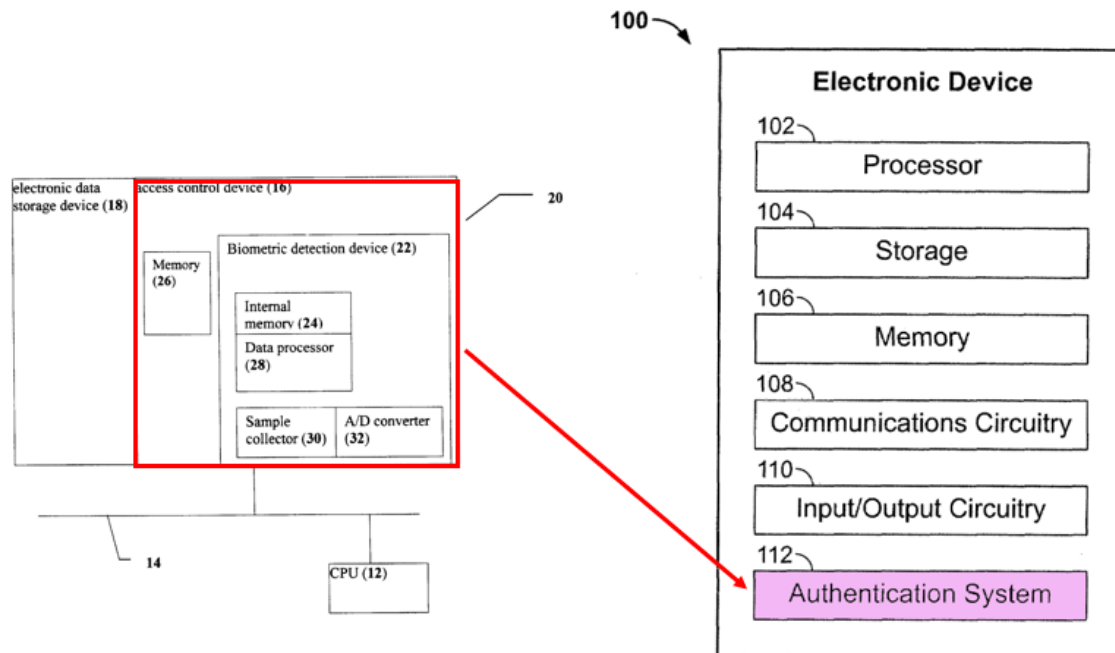
130. Internal memory 24 stores “instructions” on the biometric scan being performed and on the “interpretation of” the scanned data “with regard to stored” biometric data. (Moran, 10:60-64.) Specifically, Moran discloses that the “user is presumed to have provided a measurement of [] a biological parameter previously, in order for this information to be stored for later comparison.” (Moran, 12:22-25.)

This “stored identification information of a permitted user” (e.g., permitted user’s fingerprint data) is stored in the internal memory 24 of the biometric detection device or alternatively stored in memory 24 internal to the access control device. (Moran, 10:64-67.)

3. Motivation to Combine Fadell and Moran

131. A POSITA would have been motivated to combine Moran’s teachings regarding implementation of an access control unit having an integrated biometric detection device with Fadell’s device having one or more authentication system. For example, a POSITA would have been motivated to implement Fadell’s multiple authentication systems within an access control unit having a memory and a biometric detection device, as taught by Moran. Fadell teaches “one or more of electronic device components 100 may be combined.” (Fadell, ¶32, *see also*, Fadell, ¶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. (Fadell, ¶40.)



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

132. A POSITA would have been motivated to make this combination for numerous reasons. First, a POSITA would have been motivated to make the above combination because Fadell is silent regarding implementation details of its authentication system, other than the types of supported sensors. A POSITA would have therefore been motivated to search for references providing implementation details, particularly associated with structures for providing the authentication processing performed by Fadell's authentication systems 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.” (Moran, 1:10-14.)

133. Second, a POSITA would have also been motivated to make the above combination to improve security, a motivation expressly stated in Moran. Moran teaches that access control device 16 is “implemented as a chip, with a non-volatile memory which is both readable and writable.” (Moran, 7:9-11.) Moran stresses that 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.” (Moran, 7:52-55.) In fact, Moran stresses that its system “provides a more secure solution for the controlling access to data, which is useful for substantially any type of data storage device.” (Moran, 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.*, U.S. Patent No. 7,587,595 to Scarlata, et al. (“Scarlata”; EX-1015), 1:32-36 (“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 of the processing system.”), 8:6-7 (“Another set of services the TPM provides is the secure storage of keys and other data.”), 8:53-55 (“Non-volatile memory (NV memory or NVM): The NVM is the storage within the TPM where persistent keys, secrets, and other state of the TPM

are stored.”).) In fact, such architecture was included in industry standards for almost a decade before the ’875 patent.

134. Third, a POSITA would have also been motivated to use Moran’s teachings of an access control (biometric authentication) device having a dedicated processor and memory to improve the operation and efficiency of Fadell’s authentication process. For example, the authentication system of the combination does not have to wait for access to the device’s processor or storage unit, e.g., wait for the processor to finish reading or writing other data to or from the storage unit. (*See, e.g.*, U.S. Patent No. 8,495,020 to Nasserbakht, et al. (“Nasserbakht”; EX-1013), 4:66-5:1 (“By providing separate memory for each functional unit, the majority of issues with memory bottleneck are eliminated” because “[e]ach functional module has its own dedicated memory”))

135. Fourth, a POSITA would have also been motivated to use Moran’s teachings of an authentication unit having a dedicated memory to implement different levels of security for security sensitive information. For example, a dedicated memory storing biometric information can implement a higher level of security compared to a memory storing public or non-sensitive user information. (*See, e.g.*, U.S. Patent No. 7,313,825 to Redlich, et al. (“Redlich”; EX-1014), 33:47-53 (“[M]ultiple filters may be useful in the operation of the system with a plurality of security levels. Each filter could filter out different levels of security sensitive

items and each bundle or group of security sensitive items (from each distinct filter) could be stored at different computer storage locations.”.)

136. 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 as I discuss below. And, a POSITA would have been motivated to make the combinations for the reasons discussed above.

137. A POSITA would have had a reasonable expectation of success in the combination and the results of the combination would have been predictable. Combining Fadell with Moran would merely integrating one or more component (e.g., a chip) having a dedicated processor and storage component into Fadell’s device to handle biometric authentication. Moran expressly discloses that its teachings apply to the portable devices, like the electronic device of Fadell. (*See, e.g.,* (Moran, 4:38-53 (describing that the “computer” includes “a PalmPilot™, a PilotPC™, a cellular phone, a digital camera, or any other handheld device”).) Moran further discloses that access control device (and its associated biometric detection device) can be “directly integrated” into device for which it controls access (e.g., in Moran, the data storage device 18.) (Moran, 7:32-33.) 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 earliest priority date of the ’875 patent.

138. Fadell and Moran are both in the same field of the ’875 patent—managing access to user information (e.g., data or files). (*See* ’875 patent, Abstract (“A system, method and personal apparatus for managing highly secured personal data.”); Fadell, Abstract (“[A]n electronic device with an embedded authentication system for restricting access to device resources”), ¶41 (“To prevent unauthorized access to data or information stored in memory or storage, the electronic device may direct an authentication system to identify the user and authorize access to requested resources”); Moran, 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...” (’875 patent, 4:28-31.)

B. Independent Claim 1

1. Preamble [1P]: “Apparatus”

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

139. Fadell “is directed to an electronic device,” illustrated in Figure 1, “with an embedded authentication system for restricting access to device resources.” (Fadell, Abstract.) Fadell’s device, as modified by Moran, is the recited “*apparatus*.”

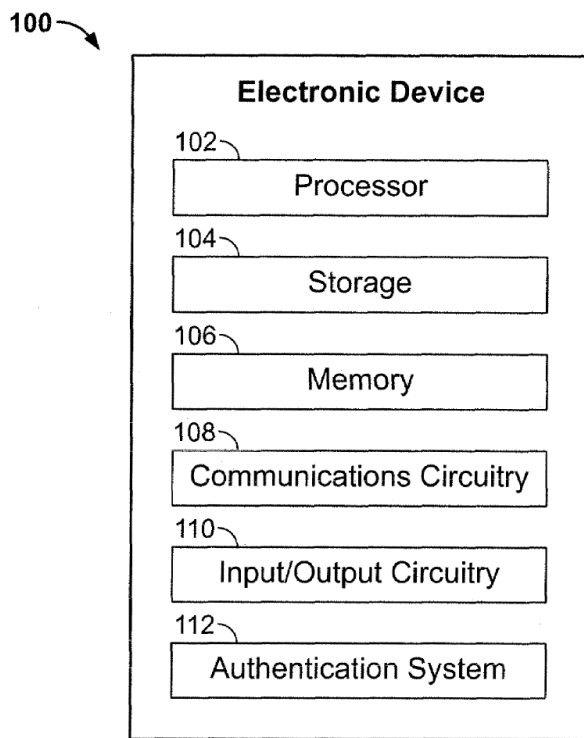


FIG. 1

Fadell, Figure 1

140. Fadell’s device stores “*personal and secured data and documentation files associated with a specific user*.” Outside the claims and the summary of the invention section, the ’875 patent does not use the term “*documentation files*.” Generally, documentation is information that describes and explains a product or service. Here, a “*documentation file[] associated with a specific user*” appears to simply be information describing or associated with a user.

141. Fadell discloses such information. For example, storage 104 stores “user preference information data (e.g., media playback preferences), authentication information (e.g. libraries of data associated with authorized users), lifestyle information data (e.g., food preferences), exercise information data (e.g., information obtained by exercise monitoring equipment), transaction information data (e.g., information such as credit card information), ... subscription information data (e.g., information that keeps track of podcasts or television shows or other media a user subscribes to), contact information data (e.g., telephone numbers and email addresses), calendar information data, and any other suitable data or any combination thereof.” (Fadell, ¶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. (See, e.g., Microsoft Corporation, “*Microsoft Computer Dictionary*,” 5, 5th ed. 2002 (“Microsoft Dictionary”; EX-1025) (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. (Fadell, Abstract (“a user may access restricted files”), ¶24 (“[a]ccess to any suitable electronic resource may be restricted, including for example access to files or data store on ... the device”), ¶31 (associating “media data” with “files”), ¶41 (“the electronic device may require different levels of authorization before providing access to different applications or different data or files associated with

different applications”), ¶42 (“As another example, each option may be associated with particular data or files available to the user”), ¶52 (“If the resource is not public (e.g., not a default application or file to remain available to all users)”).) The above listed items are therefore each examples of “personal data” and “documentation files” associated with the user. (Fadell, ¶51.)

142. User preference information data, lifestyle information data, exercise information data, subscription information data, contact information data are therefore each examples of both “*personal data*” and “*documentation files*” associated with the user. (Fadell, ¶31.) This data, as well as other data (e.g., authentication information), is “*secured*” because only authenticated individuals can obtain access. (Fadell, ¶52.)

143. Fadell further teaches that its device “*manag[es]*” access to this “*personal and secured data and documentation files associated with a specific user*” as I discuss further in my analysis of claim 1. For example, Fadell manages “access to or use data or resources that are personal to one or more users” by “require[ing] the user to authenticate.” (Fadell, ¶43.) 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.**” (Fadell, ¶24.)

144. The combination of Fadell and Moran discloses an “*apparatus for storing and managing personal and secured data and documentation files associated with a specific user.*”

2. Integrated Biometric Sensors [1A]

[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;

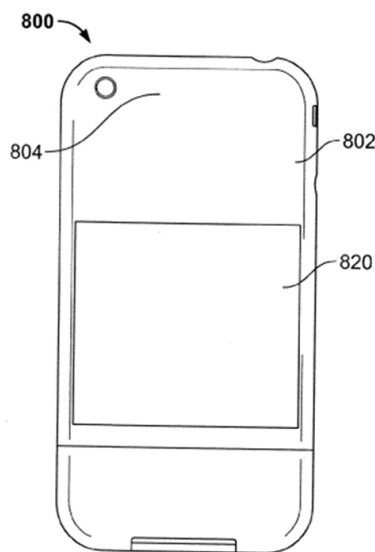
145. Fadell’s device is an “**embedded** authentication system” with “**one or more sensors operative to detect biometric information of a user.**” (Fadell, Abstract.) Fadell describes a wide variety of sensors “*integrated within*” the body of the electronic device (“*apparatus*”) used to read biometric data. For example, Fadell discloses authentication system 112 may include “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.” (Fadell, ¶39.) I describe several exemplary sensors below but note that other sensors not discussed (e.g., odor, DNA sensors), but disclosed by either Fadell or Moran, are equally applicable.

146. **Fingerprint sensor:** Fadell describes an optical and a capacitive sensor for detecting features of a user’s skin (i.e., fingerprints). (Fadell, ¶¶55-56, 59.) The sensor “may be place at any suitable location within the electronic device.” (Fadell, ¶60.) Fadell describes that the sensor “may be assembled, printed or etched directly

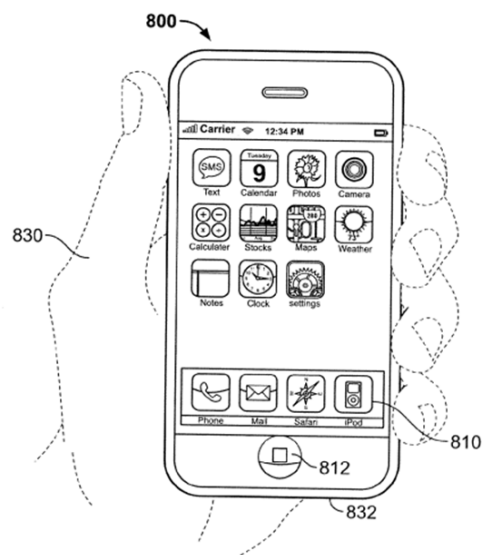
on display 600 (e.g., etched on glass) such that the user cannot see the fingerprint scanner.” (Fadell, ¶62.) In an alternative embodiment, the sensor “may be placed in, adjacent to or behind any button or other physical input that a user may press in an electronic device.” (Fadell, ¶65.) In use, “[w]hen a user’s finger is placed over the array of cells” associated with the sensor, the sensor “distinguish[es] the cells over which a valley (e.g., a fingerprint valley) and a ridge (e.g., a fingerprint ridge) are placed from the different capacitance values of each cell (i.e., cells under a valley will have a lower capacitance than cells under a ridge).” (Fadell, ¶56.) For the capacitance values detected in each cell, the capacitive sensor generates “an image or a representation of the skin placed over the sensor that can be compared to a library of images or representations available to the electronic device.” (Fadell, ¶56.) The user’s fingerprint is a “*personal biological identification parameter of the user*” and therefore the fingerprint (e.g., optical or capacitive sensor) is a “*biometric sensor[] for reading [] personal biological biometric identification parameters of the user holding the apparatus*” which is “*integrated within*” the device.

147. **Handprint sensor:** Fadell also discloses a sensor for detecting features of a user’s palm or hand, e.g., to detect a user’s handprint. (Fadell, ¶67.) Handprint sensor 820 may be “**embedded in back surface 804** and operative to detect features of a user’s palm or hand.” (Fadell, ¶67.) When in use, the user’s hand is “cupped around housing 802 leaving display 810 visible such that at least the user’s palm 832

is placed against back surface 804.” (Fadell, ¶67, Figures 8A-8B (below).) Thus, this sensor is used “[w]hen a user holds electronic device 800.” (Fadell, ¶67.) The user’s palm or handprint is a “*personal biological identification parameter of the user*” and therefore the handprint sensor is a “*biometric sensor[] for reading [] personal biological biometric identification parameters of the user holding the apparatus*” which is “*integrated within*” the device.



Fadell, Figure 8A



Fadell, Figure 8B

148. **Under skin feature sensor:** Fadell also discloses a sensor that “detect[s] the pattern of a user’s veins, arteries, follicle distribution, or any other suitable feature underneath the user’s skin.” (Fadell, ¶69.) Suitable under skin feature sensors include “an optical sensor (e.g., a camera) located on the surface of the electronic device” that is “positioned so as to detect a feature underneath any suitable

portion of the user's skin when the electronic device is in use,” that is, when the user is holding the device. (Fadell, ¶69.) The pattern of the under skin feature is a “*personal biological identification parameter of the user*” and therefore the under skin feature sensor is a “*biometric sensor[] for reading [] personal biological biometric identification parameters of the user holding the apparatus*” which is “*integrated within*” the device.

149. **Facial feature sensor:** Fadell also discloses a sensor such as “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. (Fadell, ¶71.) The sensor is “located at any suitable position on the electronic device” and “may include a camera or other sensor provided with the electronic device for a different purpose (e.g., an embedded webcam for chatting).” (Fadell, ¶73.) For example, the face sensor “detect[s] radiation emitted or reflected by one or more distinctive features of the user’s face when “the user's face is placed opposite the sensor.” (Fadell, ¶71; *see also* Fadell, ¶72.) Although not explicit, a POSITA would have understood that the user is holding the device during this scan in a “selfie-style” position. The user’s facial feature is a “*personal biological identification parameter of the user*” and therefore the facial feature sensor is a “*biometric sensor[] for reading [] personal biological biometric identification parameters of the user holding the apparatus*” which is “*integrated within*” the device.

150. **Eye feature sensor:** Fadell also discloses a sensor that “scan[s] a user’s retina, iris or retinal blood vessels to detect unique patterns of the user.” (Fadell, ¶74.) Exemplary eye sensors include “a light source operative to emit light, for example infrared light, to be reflected by the user’s eye and detected by a lens or optical sensor.” (Fadell, ¶74.) The eye sensor “analyze[s] the received light to create a representation of the user’s eyes that can be compared with a library of authorized user’s eyes.” (Fadell, ¶74; *see also* Fadell, ¶75.) Although not explicit, a POSITA would have understood that the user holds the device while the embedded sensor performs the scan. The user’s eye feature is a “*personal biological identification parameter of the user*” and therefore the eye feature sensor is a “*biometric sensor[] for reading [] personal biological biometric identification parameters of the user holding the apparatus*” which is “*integrated within*” the device.

151. **Voice sensor:** Fadell also discloses a sensor for detecting attributes or qualities of a user’s voice. (Fadell, ¶77.) This sensor can be “any suitable component for authenticating a user, including for example a microphone” that “detect[s] a particular voice pitch or voice signature.” (Fadell, ¶77.) Fadell notes that the microphone “may be primarily used for other purposes (e.g., telephone communications or video conferencing).” (Fadell, ¶77.) Although not explicit, a POSITA would understand that the user holds the phone when speaking into the sensor/microphone. The user’s voice signature is a “*personal biological*

identification parameter of the user” and therefore the voice sensor is a “biometric sensor[] for reading [] personal biological biometric identification parameters of the user holding the apparatus” which is “integrated within” the device.

152. **Ear feature sensor:** Fadell also discloses sensors for detecting features of a user’s ear. (Fadell, ¶77.) This sensor, located near a speaker, “authenticate[s] users from the shape of their ear canals” and may be a “sensor (e.g., optical, radar or sonar) operative to detect unique features of a user’s ear canal (e.g., shape and length).” (Fadell, ¶77.) Although not explicit, a POSITA would have understood the use holds the phone so that this embedded sensor can scan her ear. The user’s ear features is a “*personal biological identification parameter of the user*” and therefore the ear feature sensors is a “*biometric sensor[] for reading [] personal biological biometric identification parameters of the user holding the apparatus*” which is “*integrated within*” the device.

153. Fadell’s device include “*a plurality of*” the biometric sensors described above. Fadell’s device “may provide any suitable combination of authentication systems” including “several biometric authentication systems.” (Fadell, ¶28.) In Fadell, the device “may associate particular resources with one or more authentication systems.” (Fadell, ¶52.) Specifically, a user may “select one or more authentication systems to satisfy before providing access to the resource.” (Fadell, ¶52.) That is, the user/device may associate access to a first resource (e.g., contacts)

with one form of authentication (e.g., voice print) and a second resource (e.g., credit card information) with another form of authentication (e.g., fingerprint). Additionally, “the electronic device may require a user to satisfy several authentication systems prior to providing access to an application or data.” (Fadell, ¶41.) That is, the device may require multi-biometric (multi-modal) authentication before allowing access to requested resources. For example, the device may require both fingerprint and facial recognition before accessing specific resources (e.g., financial resources).

154. Accordingly, the combination of Fadell and Moran 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.*”

3. Life Signs Detector [1B]

[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;
--

155. Fadell discloses the use “any suitable countermeasure for preventing an unauthorized user from spoofing” an attribute of an authorized user by, e.g., “placing an image (e.g., a printed image) or a three-dimensional structure (e.g., a polymer cast) adjacent to the authentication system sensor.” (Fadell, ¶57.) Countermeasures disclosed by Fadell include components designed to detect the vital signs of a user—

e.g., pulse and temperature. (See, e.g., Fadell, ¶57.) For example, Fadell's device may include "a sensor for detecting a user's pulse, [or] 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)." (Fadell, ¶57.) The user's pulse and temperature are "*life sign parameters*" of the user and therefore the pulse sensor and temperature/heat sensor are each a "*life signs detector integrated within the apparatus.*"

156. Because pulse and temperature sensors are designed in Fadell to be a countermeasure to spoofing, a POSITA would understand that the user's life sign parameters are measured and recorded for comparison to confirm the presented biometric is associated with a live individual. Fadell teaches this with respect to the temperature sensor explaining the heat sensor "determin[es] if the temperature is within a range of expected human skin temperatures." (Fadell, ¶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*" of the combination of Fadell and Moran 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."

157. The combination of Fadell and Moran therefore 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.*”

158. I understand that in the infringement contentions in the co-pending litigation, PO takes the position that whether the user’s eyes are opened or closed is a “*life sign parameter.*” (“OSNH v. Samsung – OSNH’s ’875 Patent Infringement Contentions”; 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.”) I disagree with PO that the simple metric of a user’s eyes being opened without more is sufficient to determine a user is alive. Regardless, even if PO’s overly broad interpretation is adopted, the combination of Fadell and Moran still discloses additional “*life sign detectors.*” For example, Moran discloses “devices for measurement of ECG/EEG [and] pressure measurements on one or more body organs.” (Moran, 4:65-66.) Electroencephalography (EEG) and electrocardiography (ECG) were (and remain) widely used techniques for assessing brain and cardiac function—functions which are indicative of whether an individual is alive. And the most common example of a pressure measurement on a body organ is blood pressure which I note is also a vital sign of a user.

159. Fadell also discloses the use of a sensor to “detect movements of the user’s eyes.” (Fadell, ¶75.) Specifically, “[b]efore providing a user with access to

electronic device resources, the electronic device may direct the sensor to detect a predetermined eye movement set up by an authorized user.” (Fadell, ¶75.) For example, each authorized user may create an eye movement track by moving his eyes in a particular manner (e.g., up, down, left, right, blink, blink) while looking at the sensor” and “[w]hen a user of the device moves his eyes in a manner that matches a predetermined eye movement, the electronic device may unlock the device or provide access to restricted resources.” (Fadell, ¶75.) Movement of the eyes is an indicator that the user is alive.

160. Thus, should PO assert the same interpretation in the present proceeding, the combination of Fadell and Moran discloses this limitation for these additional reasons.

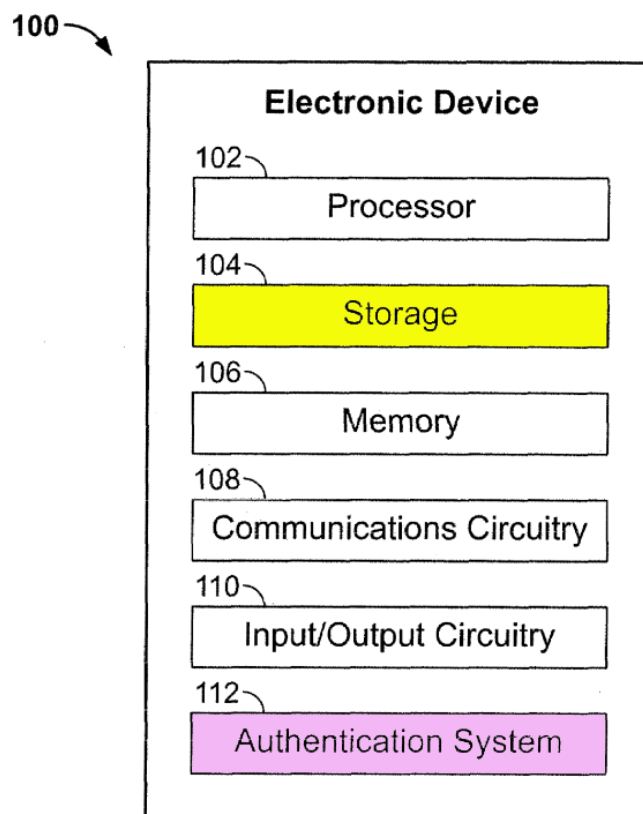
4. First Storage Unit [1C]

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

161. As I discussed in Section IV.E.1, “*first storage unit*” is a means-plus-function term with the function being “storing a user’s data and documentation files” and the structure being “memory.”

162. Fadell’s device, illustrated below, includes storage 104 (shaded yellow) which stores “user preference information data (e.g., media playback preferences), ... exercise information data (e.g., information obtained by exercise monitoring equipment), transaction information data (e.g., information such as credit card

information)..., subscription information data (e.g., information that keeps track of podcasts or television shows or other media a user subscribes to), contact information data (e.g., telephone numbers and email addresses), calendar information data, and any other suitable data or any combination thereof.” (Fadell, ¶31.) As I discussed in §V.B.1 (preamble), user preference information data, lifestyle information data, exercise information data, subscription information data, contact information data are each examples of both “*data*” and “*documentation files*” associated with the user. Thus, storage unit 104 performs the function of “storing a user’s data and documentation files.”



Fadell, Figure 1

163. Storage 104 includes “a hard-drive, solid state drive, flash memory, permanent memory such as ROM, any other suitable type of storage component, or any combination thereof.” (Fadell, ¶31.) Thus, storage unit 104 is a “memory”, meeting the structure of the “*first storage unit*” term.

164. Thus, under the proper construction, the combination of Fadell and Moran discloses “*a first storage unit for the storage of said user’s data and documentation files.*”

165. Should PO contend that “*first storage unit*” is not a means-plus-function term, the combination of Fadell and Moran disclose this limitation under plain meaning or any other reasonable construction for the same reasons discussed above.

5. Authentication Unit [1D]

[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;

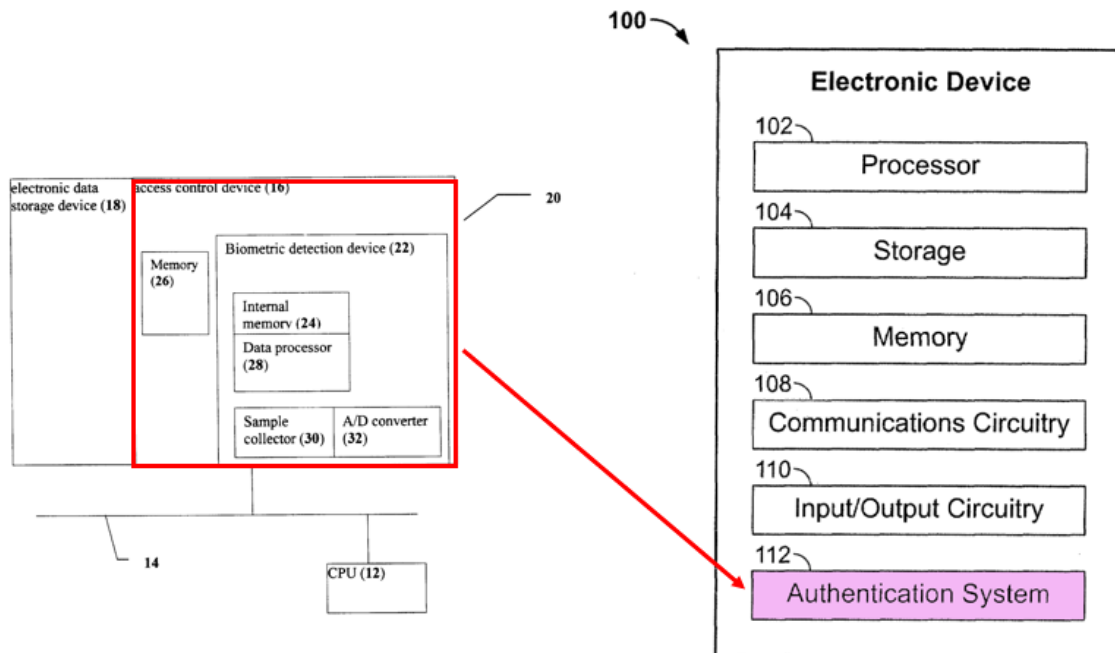
166. Limitation [1D] recites “*an authentication unit comprising a second storage unit.*” As I discussed in §IV.E.3, the term “*authentication unit*” is a means-plus-function term with the function being “comparing the plurality of personal

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” and the structure being “memory and processor programmed to” perform the function. And as I discussed in §IV.E.2, the term “*second storage unit*” is also a means-plus-function term with the function being “storing a pre-recorded set of personal biological biometric identification parameters uniquely associated with the specific user” and the structure being “memory.”

167. In this section, after an overview of integrated authentication system of the combined device, I turn next to the limitation “*pre-recorded set of personal biological biometric identification parameters*”, followed by the “*second storage unit*” and finally to the “*authentication unit*” limitations.

a) Integrated Authentication System

168. As I discussed in §V.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. This integrated authentication system, embedded in the device, is coupled to other device components via Fadell’s internal bus. (See §V.B.6.).



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

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

169. Both Fadell and Moran disclose a “*pre-recorded set of personal biological biometric identification parameters.*”

170. When using biometric authentication, a user must first enroll with the system by providing her biometric data. (*See, e.g., Jain, 6* (describing the enrollment process of a biometric system).) As discussed in §V.B.2, the combination of Fadell and Moran discloses use of multiple types of biometric authentication and therefore the user must enroll data for each type of biometric authentication being used. That is, the user has a “*set of personal biological biometric identification parameters.*”

Fadell describes an enrollment process. Specifically, Fadell teaches that “when a

user selects an authentication system to use with particular device resources, the electronic device may direct the user to **provide biometric information** (e.g., a fingerprint, eye scan, or DNA sequence) **to be stored in a library.**” (Fadell, ¶79.) During the authentication process, “detected biometric attributes” are compared “with a library of biometric attributes stored by or accessible to the electronic device.” (Fadell, ¶¶ 6, 79.) That is, the user’s reference biometric information is pre-recorded so that it can be used later during authentication process. Thus, Fadell discloses a “*pre-recorded set of personal biological biometric identification parameters.*”

171. Moran also discloses a process by which a user pre-stores identification information. Moran explains that 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.” (Moran, 12:21-25.) I note that during U.S. prosecution the Examiner found that Moran disclosed this limitation and Applicant did not traverse this finding, instead amending the claim to include the “*life signs detector*” limitation. Thus, as acknowledged by the Examiner and the Applicant, Moran also discloses “*a pre-recorded set of personal biological biometric identification parameters.*”

c) Second Storage Unit

[1D-2] second storage unit configured to store a pre-recorded set of personal biological biometric identification parameters uniquely associated with the specific user,

172. 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. As discussed above, “when a user selects an authentication system to use with particular device resources, the electronic device may direct the user to **provide biometric information** (e.g., a fingerprint, eye scan, or DNA sequence) **to be stored in a library.**” (Fadell, ¶79.) In Fadell, “[t]he user may then be authenticated by comparing the detected biometric attributes **with a library of biometric attributes stored by or accessible to the electronic device.**” (Fadell, ¶6; *see also*, Fadell, ¶79 (“[r]eceived biometric information stored in the library may be retrieved when a user attempts to authenticate, and compared to the biometric information provided by the user”), ¶73 (describing comparison of scanned facial features “with a library of features associated with authorized users), ¶74 (describing comparison of scanned eye features “with a library of authorized user's eyes”).)

173. Although Fadell discloses that “authentication information (e.g. libraries of data associated with authorized users)” is stored in storage 104 (Fadell, ¶31), a POSITA would have been motivated to store this reference information in

the dedicated internal memory of the integrated authentication system (e.g., chip), as taught by Moran. Moran teaches that the stored biometric reference data (e.g., fingerprint data) is “stored on internal memory 24 [of the biometric detection device]” of the access control device. (Moran, 10:64-67; *see also*, Moran, 12:17-24.) For example, a POSITA would have recognized that internal memory in the separate hardware system (e.g., implemented as a chip) provided improved security. Indeed, Moran notes the improved physical security stating that such an arrangement is “more difficult to ‘hack’.” (*See* Moran, 5:56-59.) A POSITA would have therefore been motivated to store sensitive reference data for authentication processing in this more secure location. 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 I discussed in §V.B.2.

174. Thus, internal memory 24 of the combined authentication processing component of Fadell and Moran 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.” Accordingly, the combination of Fadell and Moran discloses a “*second storage unit configured to store a pre-recorded set of personal biological biometric identification parameters uniquely associated with the specific user.*”

175. Should PO contend that “*second storage unit*” is not a means-plus-function term, the combination of Fadell and Moran discloses this limitation under plain meaning or any other reasonable construction for the same reasons discussed above.

d) Authentication Unit

[1D-1] an authentication unit ... 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;

176. The combination of Fadell and Moran performs the function of “comparing 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.”

177. As I discussed in §V.B.2 in my analysis of limitation [1A], the combination of Fadell and Moran includes “*a plurality of biometric sensors for reading a plurality of personal biological biometric identification parameters of the user holding the apparatus.*” And as I discussed above, the combination of Fadell and Moran discloses that a “*pre-recorded set of personal biological biometric identification parameters [is] stored in said second storage unit.*”

178. In Fadell, when an individual attempts to authenticate to the device, the reference “biometric information stored in the library may be retrieved ... and

compared to the biometric information provided by the user.” (Fadell, ¶79.) “If the provided biometric authentication information matches information stored in the library (e.g., information associated with a requested resource), the electronic device may provide access to a restricted resource.” (Fadell, ¶79.) For example, with fingerprint authentication, the fingerprint sensor “generate[s] an image or a representation of the skin placed over the sensor that can be compared to a library of images or representations available to the electronic device.” (Fadell, ¶56.) As an additional example, for authentication based on eye attributes, the associated sensor “analyze[s] the received light to create a representation of the user’s eyes that can be compared with a library of authorized user’s eyes.” (Fadell, ¶74.)

179. Similarly, Moran teaches that after the biological parameter has been collected from an individual, “the biological parameter data is analyzed” by extracting “at least one, and preferably a plurality of, features of the pattern of the biological parameter.” (Moran, 5:27-33.) These extracted features are then compared **“to stored data which was previously captured from the user.”** (Moran, 5:32-35.) If it is determined there **“is a sufficiently close match to the stored identification information** of a permitted user, such that the data operation with regard to the data storage device is permitted.” (Moran, 12:17-22.)

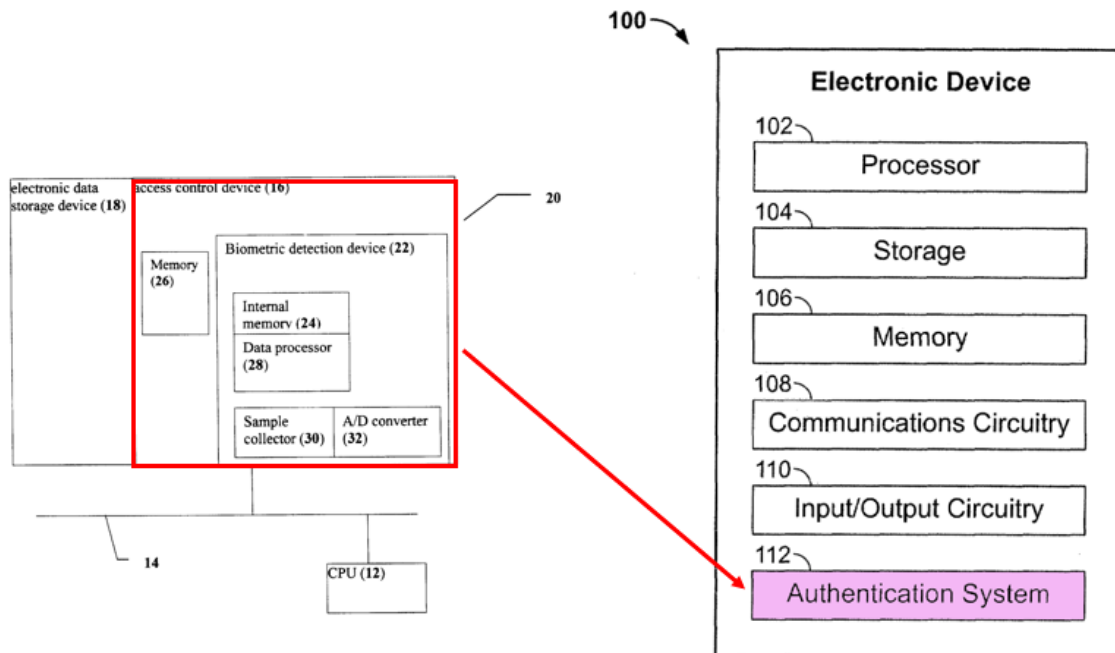
180. Thus, the combination of Fadell and Moran teaches that for each type of biometric authentication the authentication process component “*compare[s] [the]*

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

181. As I discussed in §V.B.2 in my analysis of limitation [1A], Fadell teaches that its device “may associate particular resources with one or more authentication systems.” (Fadell, ¶52.) Specifically, a user may “select one or more authentication systems to satisfy before providing access to the resource.” (Fadell, ¶52.) That is, the user/device may associate access to a first resource (e.g., contacts) with one form of authentication (e.g., voice print) and a second resource (e.g., credit card information) with another form of authentication (e.g., fingerprint). Additionally, “the electronic device may require a user to satisfy several authentication systems prior to providing access to an application or data.” (Fadell, ¶41.) Therefore, 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.

182. Thus, the combination of Fadell and Moran discloses performing 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.*”

183. Fadell does not explicitly describe the component that performs the authentication processing. In the combination of Fadell and Moran, the authentication processing for each type of authentication is performed by the internal data processor within the integrated authentication system that I discussed in §V.A.3 and illustrate again below. As I discussed in §V.A.3, in the combination of Fadell and Moran, the authentication system is implemented using the teachings of Moran, including a physical component having an internal memory and data processor. Moran specifically discloses that authentication processing is performed “by a software module which is stored in internal memory 24 and which is operated by data processor 28.” (Moran, 11:8-11, 11:31-34 (“digital signal is then optionally passed to data processor 28 for analysis”); *see also, e.g.*, Moran, claims 3-4.)



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

184. Thus, the combination of Fadell and Moran discloses the structure of the authentication unit—memory (internal memory 24) and processor (data processor 28) that performs the recited function. Accordingly, the combination of Fadell and Moran disclose or at least render obvious “*an authentication unit ... 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.*”

185. Should PO contend that “*authentication unit*” is not a means-plus-function term, the combination of Fadell and Moran discloses this limitation under

plain meaning or any other reasonable construction for the same reasons discussed above.

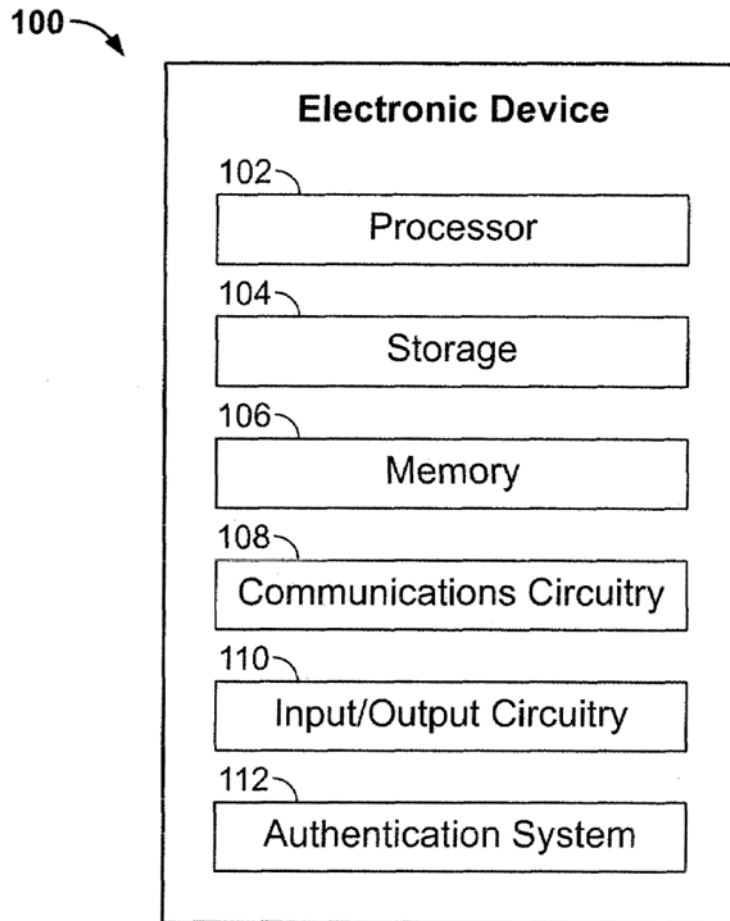
e) Authentication Unit Comprising the Second Storage Unit

186. As I discussed in the prior section, the integrated authentication system of the combination of Fadell and Moran 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.*”

6. Processor [1E]

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

187. Fadell’s electronic device 100 includes processor 102 which “control[s] the operations and performance of electronic device 100.” (Fadell, ¶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 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.” (Fadell, ¶40.)



Fadell, Figure 1

188. 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 by sending a command through bus 14 directly to data storage device 18” but “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.” (Moran, 6:63-7:4.) A POSITA would understand the device in the combination of Fadell and Moran operates in a similar manner. That is, a POSITA would have understood that for the

processor to control the operations of electronic device 100, the processor must communicate with the components of the device, including Fadell's biometric sensors, the storage unit (storing the data sought to be accessed), and the integrated authentication system (controlling access to the data stored in the storage unit).

189. Accordingly, the combination of Fadell and Moran discloses “*a processor in communication with said plurality of biometric sensors, said first storage unit and said authentication unit.*”

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

[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
--

190. As I explained in §V.A.3, the combination of Fadell and Moran discloses that the authentication unit performs the function of “*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.*”

191. Fadell's authentication system is configured to control (e.g., restrict) “[a]ccess to any suitable electronic device resource ... including for example access to files or data stored on or available to the device.” (Fadell, ¶24.) Specifically,

Fadell discloses that “[i]f the provided biometric authentication information matches information stored in the library (e.g., information associated with a requested resource), the electronic device **may provide access to a restricted resource.**” (Fadell, ¶79; *see also*, Fadell, ¶41 (“The electronic device may require authorization prior to providing access to any electronic device resource”).) For example, for facial recognition, Fadell discloses that “[i]f an authorized user is detected, electronic device 1100 may display or **provide access to restricted content 1112** on display 1110.” (Fadell, ¶73.) Moran similarly discloses the authentication unit determines if “access should be granted and the data read from the data storage device” based on result of biometric authentication. (Moran, 7:2-5.)

192. As I discussed in §V.B.5 in my analysis of limitation [1D-1], Fadell’s “electronic device may require a user to satisfy several authentication systems prior to providing access to an application or data.” (Fadell, ¶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).

193. Thus, the combination of Fadell and Moran 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.”

8. Critical Level Detection [1G]

[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.

194. As I discussed in §V.B.3 in my analysis of limitation [1B], Fadell discloses countermeasures “for preventing an unauthorized user from spoofing” an attribute of an authorized user by, e.g., “placing an image (e.g., a printed image) or a three-dimensional structure (e.g., a polymer cast) adjacent to the authentication system sensor.” (Fadell, ¶57.) Countermeasures disclosed by Fadell include components designed to detect the vital signs of a user—pulse and temperature. (*See, e.g.,* Fadell, ¶57.) For example, Fadell’s device may include “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.” (Fadell, ¶57.)

195. That is, although not explicit, Fadell teaches or at least suggests that access to requested data and/or files stored in its electronic device would be denied if the system detects biometric spoofing. 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.” (Fadell, ¶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.

196. 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.

197. Accordingly, the combination of Fadell and Moran disclose or at least 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.*”

C. Claims 4 and 7 – Communicating With An External Device/Server

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.

198. The combination of Fadell and Moran 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*” 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.*”

199. As I discussed in §IV.E.4, the term “*communication and data connection means*” is a means-plus-function term with the “function” being “communicating with an external device” and corresponding “structure” being 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.”

200. Fadell’s electronic device includes communications circuitry 108 that “permit[s] device 100 to communicate with **one or more servers or other devices** using any suitable communications protocol.” (Fadell, ¶33.) Fadell provides support for a wide range of protocols: “communications circuitry 108 may support Wi-Fi (e.g., a 802.11 protocol), Ethernet, **Bluetooth™..., radio frequency systems**, cellular networks (e.g., GSM, AMPS, GPRS, CDMA, EV-DO, EDGE, 3GSM, DECT, IS-136/TDMA, iDen, LTE or any other suitable cellular network or protocol), infrared, TCP/IP (e.g., any of the protocols used in each of the TCP/IP layers), HTTP, BitTorrent, FTP, RTP, RTSP, SSH, Voice over IP (VOIP), any other communications protocol, or any combination thereof.” (Fadell, ¶33.) Thus, communication circuitry 108 performs the function of “communicating with an external device.” Because communication circuitry includes Bluetooth interface, an RF medium and/or a cellular modem, communication circuitry 108 further discloses the structure of the “*communication and data connection means*.”

201. Thus, the combination of Fadell and Moran discloses a “*communication and data connection means for communicating with an external device*”

202. 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 electronic device 100.” (Fadell, ¶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.” (Fadell, ¶40.) That is, control processor 102 is in communication with the communication circuitry 108.

203. Thus, the combination of Fadell and Moran renders claim 4 obvious.

204. As I discussed above, Fadell’s communications circuitry 108 permits the device “to communicate with **one or more servers or other devices.**” (Fadell, ¶33.) Only two options exist for the server—it is either local or remote. 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.*” (Fadell, ¶43.) 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].” (Fadell, ¶73).

D. Claim 10 – Communicating With An External Device

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.

205. 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 I discussed above for claim 4, Fadell’s communication circuitry 108 supports “Bluetooth” (Fadell, ¶33) and therefore Fadell discloses “*a Bluetooth communication interface.*”

206. The combination of Fadell and Moran 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,*” as recited in claim 4.

207. Thus, combination of Fadell and Moran renders claim 10 obvious.

E. Claim 14 – Secure Update Of User’s Data

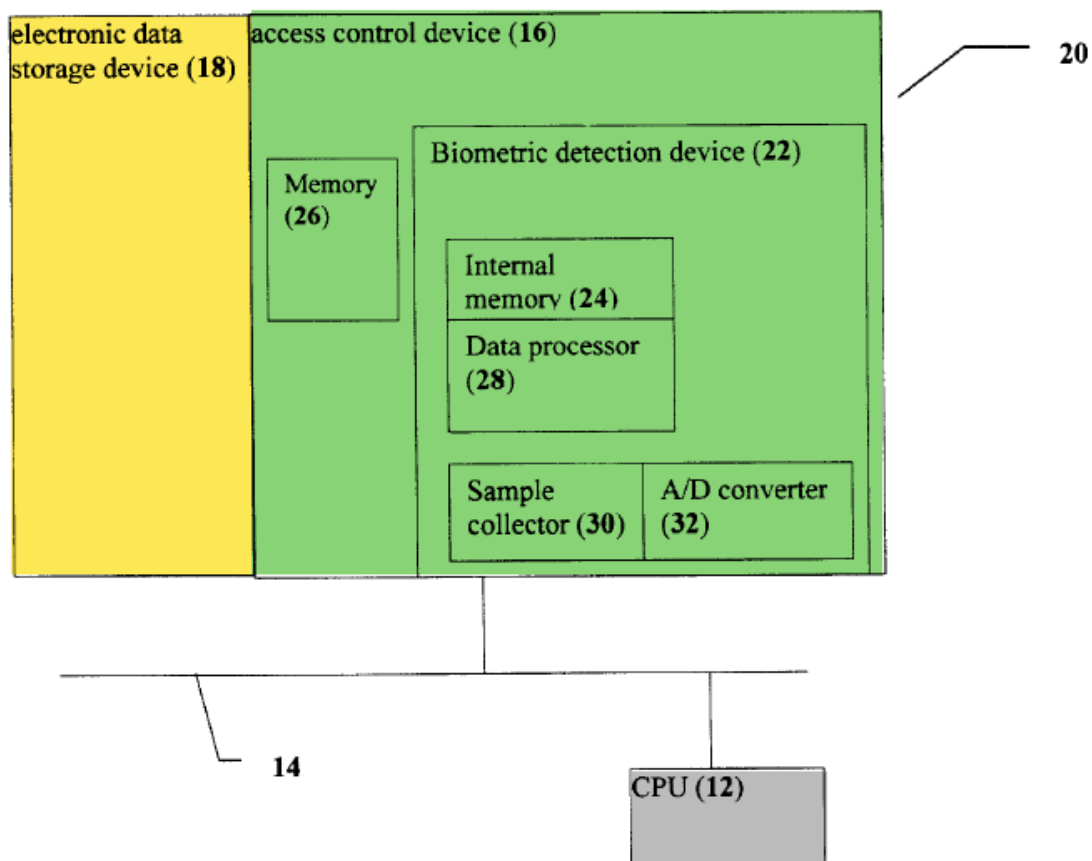
14. The apparatus according to claim 1, wherein the processor is configured to securely update the user’s data and documentation files.

208. The combination of Fadell and Moran discloses “*the processor is configured to securely update the user’s data and documentation files.*”

209. 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.” (Fadell, 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).” (Fadell, Abstract.) Fadell further teaches that a user can store “media data (e.g., music and video files)” in its storage. (Fadell, ¶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.

210. Moran explains this level of access control. Specifically, Moran discloses that, in a device secured through authentication, “[a] data storage device 18 is in communication with access control device 16, such that any attempts to access data in data storage device 18 must pass through access control device 16. Preferably, as shown, data storage device 18 is not in direct communication with bus 14.” (Moran, 6:59-63). Accordingly, as shown in Moran’s Figure 3 below, any

request by the processor (gray) to read from or write to data into data storage device 18 (yellow), must go through access control device 16 (green), which performs authentication. Moran stresses that “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.*”



Moran, Figure 3

211. In view of this teaching, A POSITA would have understood Fadell's data access restriction processing operates in the same manner. 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.

212. 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."*

F. Claim 19 – Cellular Modem, Flat Display, And Touch Screen

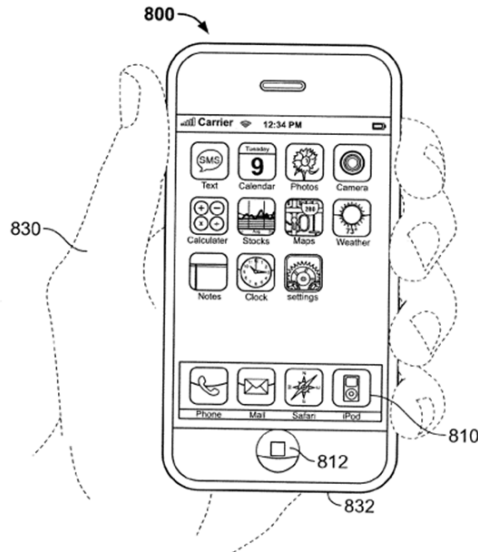
19. The apparatus according to claim 1, further comprising at least one of a group of units including a cellular modem and a flat display, and a touch screen for communication with the processor.

213. The combination of Fadell and Moran 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."

214. As I discussed above for claims 4 and 10, Fadell's electronic device includes communications circuitry 108 that "permit[s] device 100 to communicate with **one or more servers or other devices** using any suitable communications protocol." (Fadell, ¶33.) Fadell provides support for a wide range of protocols,

including corresponding data interfaces: “communications circuitry 108 may support Wi-Fi (e.g., a 802.11 protocol), Ethernet, Bluetooth™..., radio frequency systems, **cellular networks (e.g., GSM, AMPS, GPRS, CDMA, EV-DO, EDGE, 3GSM, DECT, IS-136/TDMA, iDen, LTE or any other suitable cellular network or protocol)**, infrared, TCP/IP (e.g., any of the protocols used in each of the TCP/IP layers), HTTP, BitTorrent, FTP, RTP, RTSP, SSH, Voice over IP (VOIP), any other communications protocol, or any combination thereof.” (Fadell, ¶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., Behzad Razavi, “*RF Microelectronics*,” (1998), 6-8 (“Razavi”; EX-1030), (describing general RF transmitter/receiver architecture); U.S. Patent No. 8,199,719 to Taneja (“Taneja”; EX-1029), 7:36-56.)

215. 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.



Fadell, Figure 8B

VI. GROUND 2: Fadell, Moran, and Rosenblatt Render Obvious Claims 15 and 18

216. Fadell discloses that its communication circuitry supports “Wi-Fi (e.g., a 802.11 protocol), ... Bluetooth™ ... radio frequency systems, [and] cellular networks (e.g., GSM, AMPS, GPRS, CDMA, EV-DO, EDGE, 3GSM, DECT, IS-136/TDMA, iDen, LTE or any other suitable cellular network or protocol)” which are each wireless protocols. (See Fadel, ¶133.) Thus, Fadell discloses its electronic device includes a “*wireless transceiver module*” as recited in claim 15. Fadell 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*”, as recited in claim 15. U.S. Patent Publication No.

2010/0082490 to Rosenblatt et al. (“Rosenblatt”; EX-1010), published April 1, 2010, discloses this missing feature.

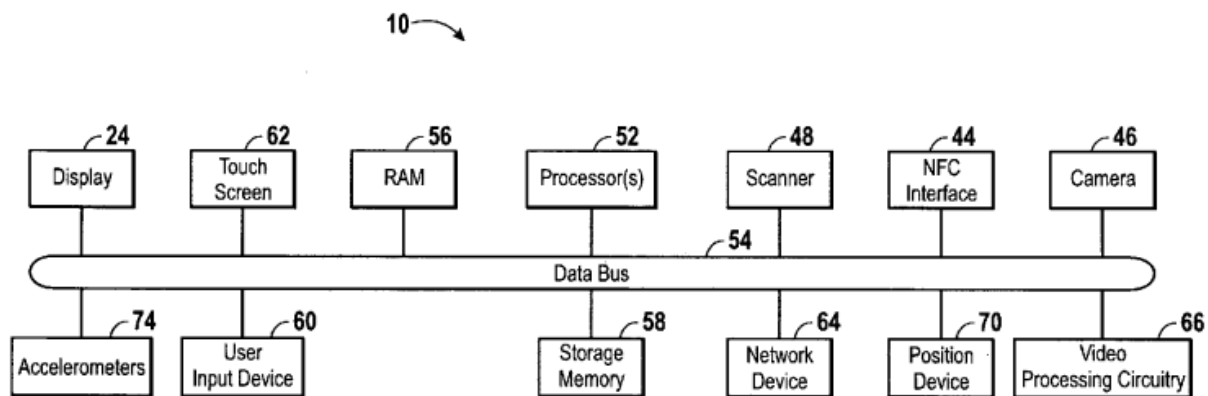
217. Additionally, neither Fadell nor Moran disclose a device comprising “*an integrated GPS module in communication with the processor to precisely locate the geographical position of the apparatus*” as recited in claim 18. I note that the integration of GPS modules within wireless devices was well-known before the earliest possible priority date of the ’875 patent. In fact, the ’875 patent admits that at the time of the alleged invention, GPS was “becoming a very common module in most smart phones.” (’875 patent, 16:58-60.) This feature is also disclosed by Rosenblatt.

A. Overview of the Combination

1. Rosenblatt

218. Rosenblatt describes “a method of conducting a wireless transaction” including “initiating a wireless transaction using a short range wireless communication system of a portable electronic device.” (Rosenblatt, Abstract.) Rosenblatt further discloses the devices performing the transaction use “[s]tandard security features,” including “one or more cryptographic protocols” for “transmitting payment information, such as credit card information or bank account information” and “a secure storage area that may have restricted access.” (Rosenblatt, ¶58.)

219. Rosenblatt’s electronic device 10, illustrated in Figure 3 (below), also includes near field communication (NFC) device 44, which “may allow for close range communication at relatively low data rates (424 kb/s), and may comply with standards such as ISO 18092 or ISO 21481, or it may allow for close range communication at relatively high data rates (560 Mbps), and may comply with the TransferJet® protocol.” (Rosenblatt, ¶41.) Rosenblatt’s NFC device is configured to “communicate with other NFC devices” and “to retrieve information from tags having radio frequency identification (RFID) circuitry.” (Rosenblatt, ¶41.) That is, NFC is a “*RFID based technique*” for communication between devices.

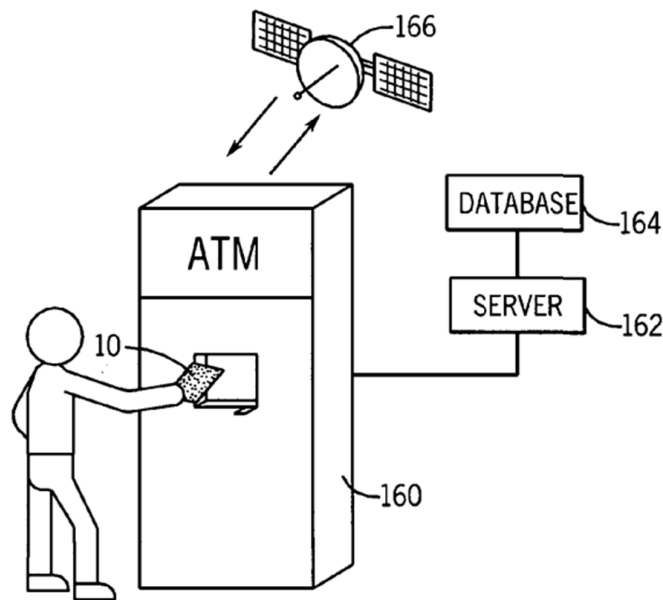


Rosenblatt, Figure 3

220. Rosenblatt further teaches its device includes “positioning device 70 used to determine a user’s geographical position” through “the global positioning system (GPS) implemented using satellite communications” (Rosenblatt, ¶55.)

221. Rosenblatt describes a transaction between a device and transaction terminal, such as an ATM, using NFC. (See, e.g., Rosenblatt, ¶¶63, 71.) As described

in Rosenblatt, “once the device 10 has initiated communications for transactions with the transaction terminal 130, the device 10 may be configured to authenticate itself in order to complete a transaction.” (Rosenblatt, ¶66.) When the transaction terminal is an ATM, as illustrated in Figure 9B (below), “authentication may be based on the location of the device 10.” (Rosenblatt, ¶71.) The location of electronic device “is determined based on information from the positioning device 70” within the device. (Rosenblatt, ¶71.) Server 162, coupled to the ATM, confirms the location of electronic device 10 coincides with the location of ATM 160, as determined by positioning system 70. (Rosenblatt, ¶71.)



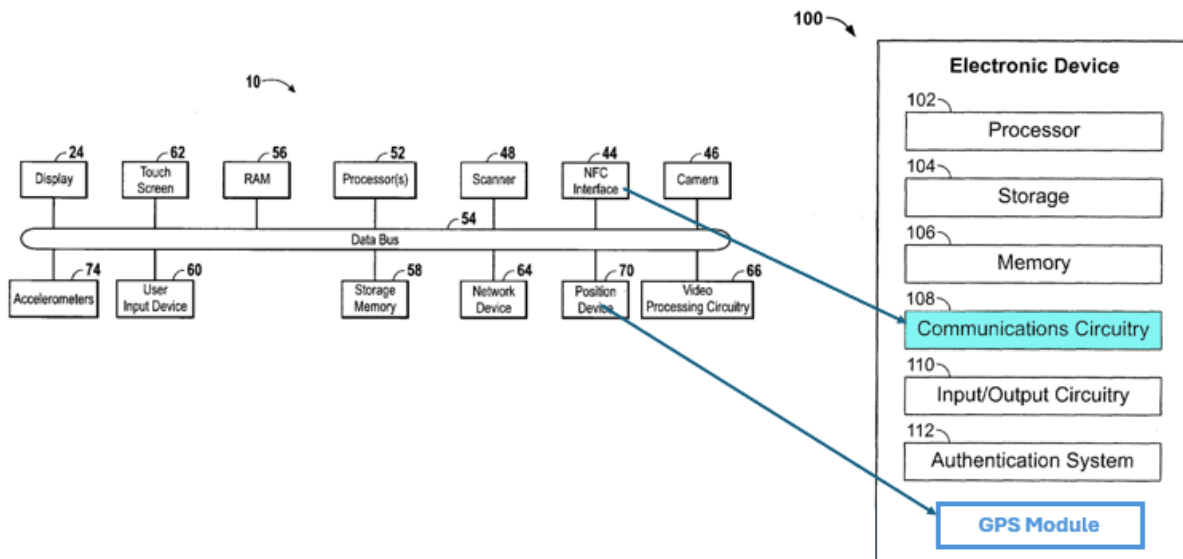
Rosenblatt, Figure 9B

222. After successful authentication of the device 10, as discussed above, the device “automatically select[s] a card, such as the ABC Bank card, for a

transaction with the transaction terminal 130, which may be an ATM.” (Rosenblatt, ¶76.) 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). (Rosenblatt, ¶79.)

2. Motivation to Combine

223. 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 Fadell’s electronic device. For example, a POSITA would have been motivated to include a wireless transceiver supporting NFC protocol and/or a GPS module in the device of Fadell and Rosenblatt, as illustrated below.



Rosenblatt, Figure 3; Fadell, Modified Figure 1

224. 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* '875 patent, 7:47-49 ("[T]he authenticated user and no other user will have the possibility to have access to the user's personal files and accounts and to be able do any kind of transaction with, or through them."); Fadell, Abstract ("[A]n electronic device with an embedded authentication system for restricting access to device resources"); Moran, Abstract ("A device, a method and a system for providing control of access to data which is stored in an electronic data storage device.")) Rosenblatt, ¶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.")) 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..." ('875 patent, 4:28-31.)

225. A POSITA would have been motivated to include a GPS module in the device of Fadell and Moran to enhance the features and applications available to a user. Rosenblatt discloses that the GPS module can precisely locate the geographical position of the device, e.g., by providing the longitude and latitude of the device and also by positioning the device on a map. (Rosenblatt, ¶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.,* Schiller, 85-88.) Additionally, inclusion of GPS in phones was motivated by the FCC’s mandate to provide enhanced emergency services. (*See, e.g.,* Schiller, 28.) These are features that a POSITA would have found beneficial and desirable.

226. A POSITA would have 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. Fadell also discloses communication circuitry which supports “radio frequency systems” and generally “any other communications protocol” (other than those listed). (Fadell, ¶33.) NFC is a form of RF communication. Rosenblatt confirms the motivation stressing that the “portability of the device 10 makes it particularly well suited to **performing transactions such as automatic teller machine (ATM) transactions, and purchase transactions.**” (Rosenblatt, ¶57.) A POSITA would understand the

ability to use a portable device as a debit or payment card enhances convenience to a user, permitting the user to not need to carry both a wallet and a wireless device.

227. 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).

228. 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. Moreover, both references are assigned to the same assignee ("Apple") and are directed to the same portable electronic device. (*Compare* Fadell, 1 ("Assignee: Apple Inc."), *with* Rosenblatt, 1 ("Assignee: Apple Inc.")). Therefore, a POSITA would have had an expectation of success combining a features designed for Apple wireless devices.

B. Claim 15 – Encoder/Decoder And Wireless Transceiver Module

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.

229. As I discussed above, Fadell also discloses communication circuitry which supports “radio frequency systems” and generally “any other communications protocol” (other than those listed). (Fadell, ¶33.) While Fadell does not explicitly mention an NFC protocol, a POSITA would have understood that the NFC protocols are “radio frequency” protocols that are envisioned by Fadell. As I discussed above, a POSITA would have been motivated to use Rosenblatt’s NFC interface 44 as the “*wireless transceiver module*” (communication circuitry) of the electronic device of the Fadell, Moran, and Rosenblatt.

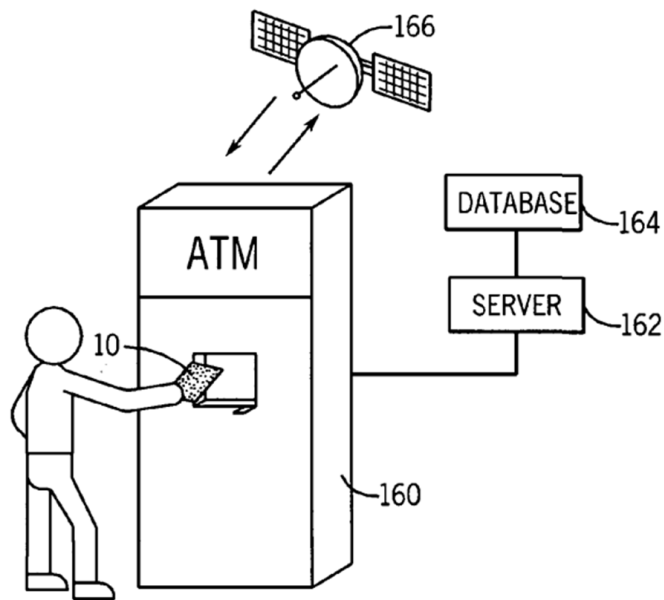
230. The combination of Fadell, Moran and Rosenblatt teaches or suggests that the communications circuitry includes an “*integrated digital data encoder/decoder*” in at least 2 ways. First, a POSITA would have understood that the NFC transceiver requires an encoder and decoder to communicate with another NFC device. (See, e.g., U.S. Publication No. 2008/0233880 to Rofougaran et al. (“Rofougaran”; EX-1032), ¶¶23-24; ISO/IEC 18092:2004(E) (EX-1027); ISO/IEC 21481:2005(E) (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. Second, Rosenblatt teaches that the device “may include one or more cryptographic protocols.” (Rosenblatt, ¶58.) Rosenblatt further discloses the use of an encryption key to “encrypt communications from the device 10 to the transaction terminal.” (Rosenblatt, ¶69.) That is, the device in the combination includes an encoder/decoder to encrypt and decrypt communication. Thus, the combination of Fadell, Moran, and Rosenblatt teaches or suggests “*an integrated digital data encoder/decoder and a wireless transceiver module*” that communicate “*using RFID base techniques.*”

231. The encoder/decoder and wireless transceiver which are part of the device’s communication circuitry communicate with processor 102. (Fadell, ¶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, storage 104, memory 106, communications circuitry 108, input/output circuitry 110 authentication system 112, and any other component included in the electronic device.”).) Thus, the combination discloses “*an integrated digital data encoder/decoder and a wireless transceiver module in communication with the processor.*”

232. Fadell contemplates use of it device in financial transactions, explaining that storage 104 stores a user’s credit card information, which Fadell

characterizes as “transaction information data.” (Fadell, ¶31 (“Storage 104 may store, for example, ...**transaction information data (e.g., information such as credit card information)**, wireless connection information data (e.g., information that may **enable electronic device 100 to establish a wireless connection**), ... and any other suitable data or any combination thereof.”). Fadell does not provide an details regarding how a financial transaction using its stored cards are performed. Rosenblatt discloses that “the portable electronic devices may be used to wirelessly transfer and receive ... sensitive or personal information, such as **the information to conduct a financial transaction.**” (Rosenblatt, ¶5, *see also* Rosenblatt, ¶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 as I discussed in the Rosenblatt overview. (*See, e.g.*, Rosenblatt, ¶¶63-79, Figure 9B.)



Rosenblatt, Figure 9B

233. Accordingly, the combination of Fadell, Moran, and Rosenblatt 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.”

C. Claim 18 – GPS Module

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.

234. As I discussed in the motivation to combine section, the device in the Fadell-Moran-Rosenblatt combination includes an integrated GPS module, as taught by Rosenblatt. (Rosenblatt, ¶55 (“The device 10 may also include a positioning device 70 used to determine a user's geographical position. ... The positioning device 70 may utilize the global positioning system (GPS) implemented using satellite communications”).)

235. Rosenblatt specifically discloses the GPS module can precisely locate the geographical position of the device, e.g., by providing the longitude and latitude of the device for location-based authentication and also by positioning the device on a map. (Rosenblatt, ¶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”).)

236. Thus, the combination of Fadell, Moran and Rosenblatt discloses “*an integrated GPS module in communication with the processor to precisely locate the geographical position of the apparatus.*”

VII. GROUND 3: Kohinata and Mizusawa Render Obvious Claims 1 and 4

237. U.S. Patent No. 6,788,928 to Kohinata et al. (“Kohinata”; EX-1009), issued September 7, 2004, and Japanese Patent Application Publication No. JP2001-109855 to Mizusawa et al. (“Mizusawa”; EX-1012), published on April 20, 2001, disclose every limitation of claims 1 and 4.

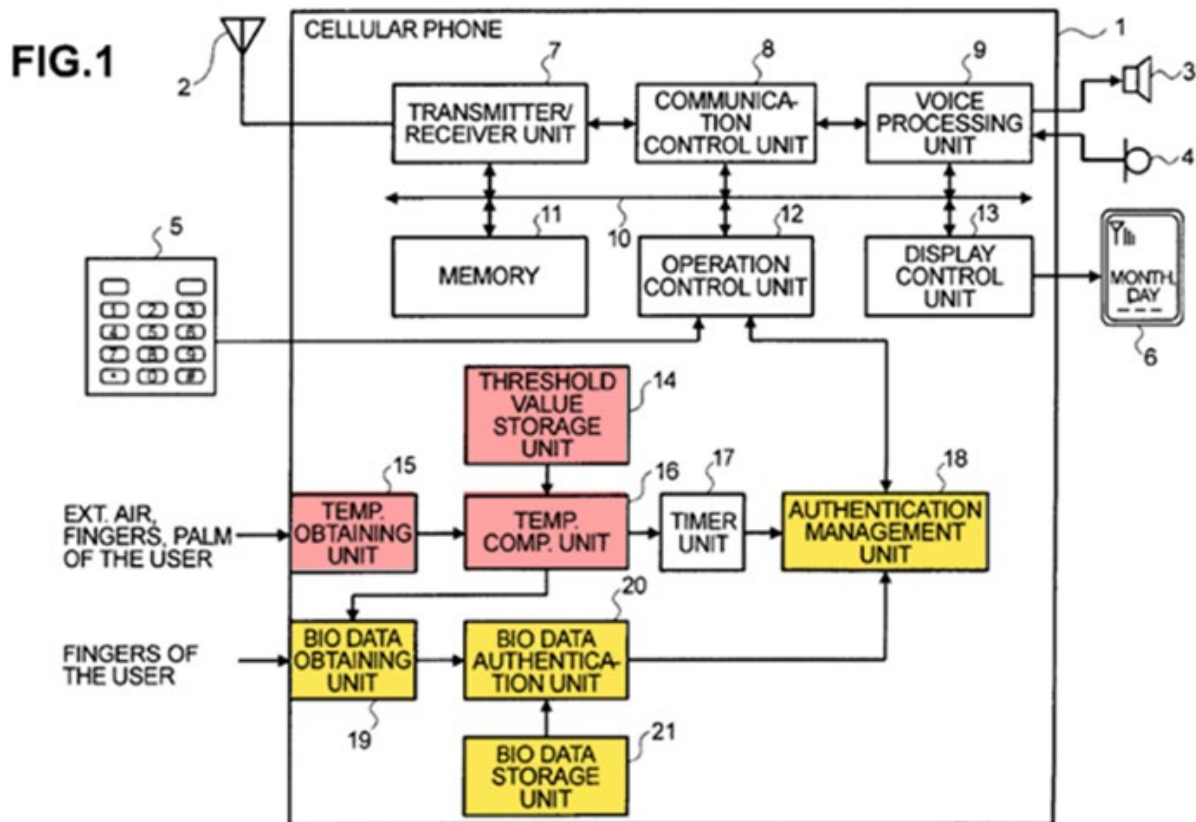
A. Overview of the Combination

1. Kohinata

238. Kohinata describes a cellular phone “capable of managing a variety of personal data related to the owner of the phone.” (Kohinata, 1:16-17; *see also*, Kohinata, 2:30-59.) Specifically, Kohinata describes an “easy to use” cellular phone “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.” (Kohinata, Abstract, Figure 1 (below).)

239. Kohinata’s phone includes an authentication module comprising biodata obtaining unit 19, biodata authentication unit 20, biodata storage unit 21, and authentication management unit 18. (*See* Kohinata, 5:41-6:29.) Authentication management unit 18 (shaded yellow) “controls the access to various kinds of data stored in the memory 11.” (Kohinata, 6:17-24.) Biodata obtaining unit 19 (shaded yellow) is a “dedicated device for imaging the fingerprint by using a small imaging device such as a CCD camera” that “obtains the fingerprint or the finger data such as feature quantity inherent in the fingerprint from a particular finger of the user of the cellular phone.” (Kohinata, 5:43-48.) Biodata authentication unit 20 (shaded yellow) “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.” (Kohinata, 6:6-10.) Biodata storage unit 21 (shaded yellow) “stores in advance the fingerprint data obtained from at least one or more fingers of the owner of the cellular phone.” (Kohinata, 5:55-57.) The fingerprint data can be registered and stored in biodata storage unit 21 “at the time when the cellular phone 1 is purchased (when the initial data are to be set) or after it has been purchased without using any particular or additional device.” (Kohinata, 5:57-61.)



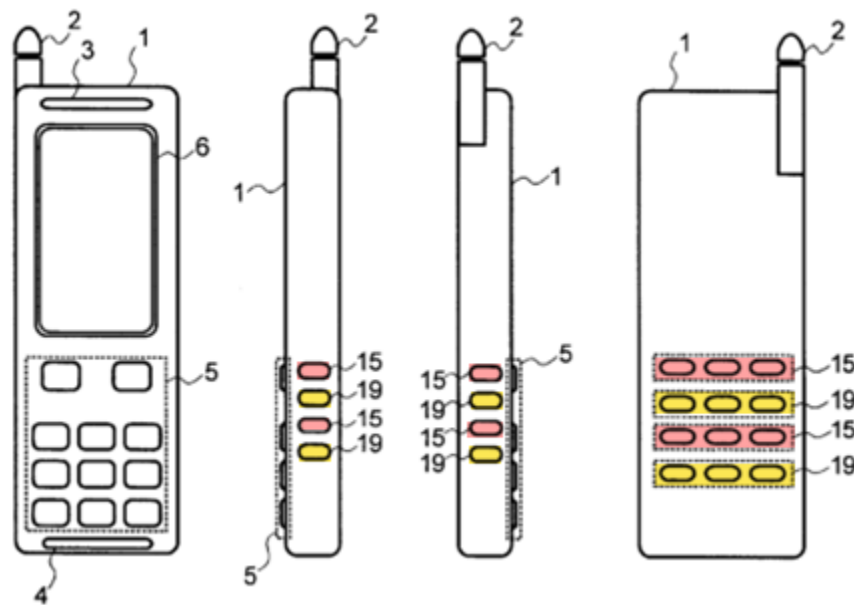
Kohinata, Figure 1

240. Kohinata cellular phone also includes a “use detection module” comprising threshold value storage unit 14, temperature obtaining unit 15, and

temperature comparator unit 16. (Kohinata, 4:29-5:40.) Threshold value storage unit 14 (shaded red) “stores threshold body temperatures of the owner of the cellular phone, i.e., stores the lower limit value only or both the upper-limit value and the lower-limit value.” (Kohinata, 4:40-43.) Temperature obtaining unit 15 (shaded red) “is constituted by a plurality of temperature sensors arranged on the surface of the cellular phone 1” and “plays the role of measuring the body temperature of the user when the temperature obtaining unit 15 is touched by the palm or fingers of hand of the user and measuring the ambient temperature of the cellular phone when it is not touched.” (Kohinata, 4:31-39.) Temperature comparator unit 16 (shaded red) “judg[es] whether the cellular phone 1 is touched by the user” by “compar[ing] the temperature data measured by the temperature obtaining unit 15 with the threshold temperatures stored in the threshold value storage unit 14” and “detect[s] that the temperature data lies within a range of the threshold temperatures.” (Kohinata, 4:54-62.) Upon detecting a temperature within the threshold range, temperature comparator unit 16 “issues an instruction to the biodata obtaining unit 19 to obtain the fingerprint of the user.” (Kohinata, 4:60-63.)

241. Figures 4A through 4D of Kohinata, which I reproduce below, illustrate “positions for disposing the temperature obtaining units 15 and the biodata obtaining units 19 with which the cellular phone 1” of Figure 1 is provided. (Kohinata, 9:26-30.) Temperature obtaining units 15 and biodata obtaining units 19 may be provided

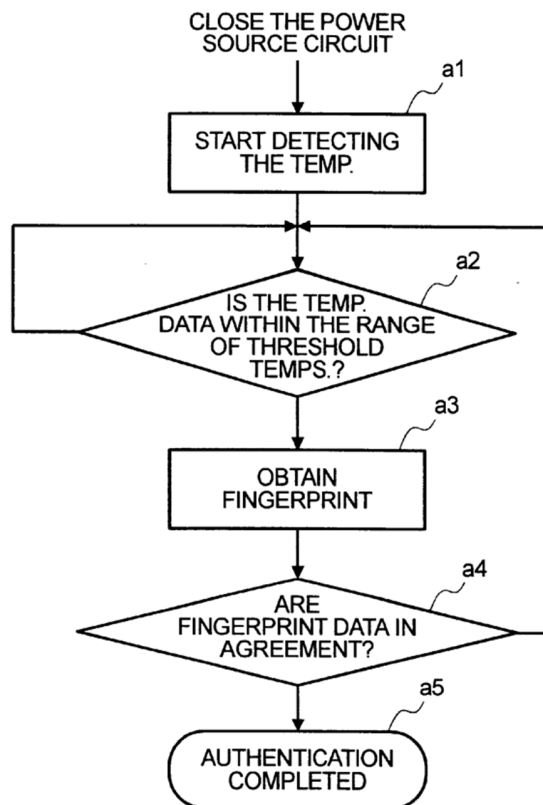
on “the right side portion of the housing” (Figure 4B), “the left side portion thereof” (Figure 4C), and “on the back surface portion” (Figure 4D). (Kohinata, 9:40-54.)



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

242. In operation, during authentication, temperature obtaining unit 15 “starts detecting the temperature” (a1). (Kohinata, 7:11-28, Figure 2.) Threshold temperatures stored in threshold value storage unit 14 “are compared with the temperature detected ... to judge if the temperature data are lying within the range of the threshold temperatures” (a2). (Kohinata, 7:14-19). If the temperature data is within the threshold range, the authentication operation proceeds to step a3, at which point biometric data obtaining unit 19 “obtains the fingerprint” of a user of cellular phone 1. (Kohinata, 7:15-20.) Next, biometric data authentication unit 20 “judge[s] if the fingerprint data obtained by” biometric data obtaining unit 19 “are in agreement with the

fingerprint data stored in” biodata storage unit 21. (Kohinata, 7:20-23.) “The authentication is completed” at step a5 “if the conditions of step a4 are satisfied as a result of judgement.” (Kohinata, 7:23-25.) “When the conditions of step a4 have not been satisfied, the routine returns back to step a2 to repeat the authentication operation again.” (Kohinata, 7:25-28; *see also*, Kohinata, 10:12-16 (“When the personal authentication has failed, the function of the cellular phone is limited to receiving a call only, preventing the unauthorized use by the third person and enabling the contents distributor to reliably offer the contents to the normal users.”).)



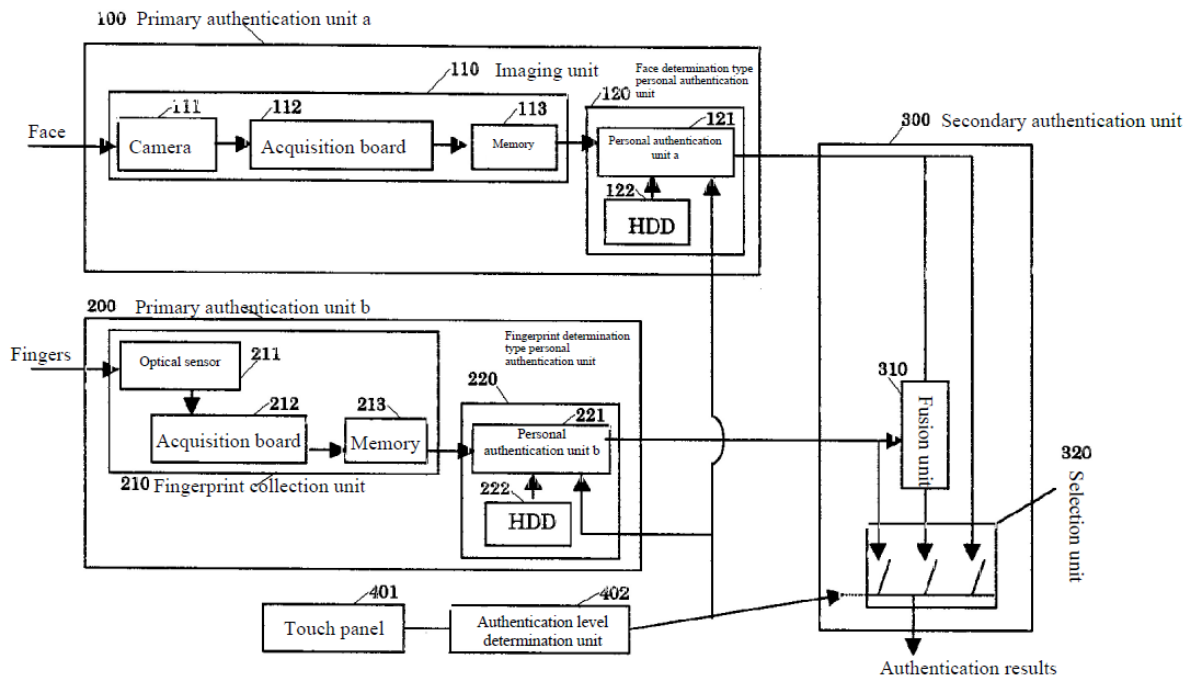
Kohinata, Figure 2

2. Mizusawa

243. The goal of Mizusawa “is to realize a personal authentication device that provides an excellent user interface that always minimizes the burden on the person being authenticated while maintaining the required authentication accuracy.” (Mizusawa, Abstract.) Mizusawa notes that personal authentication technology is often used “where there are demands for accuracy of authentication and system security against unauthorized attacks.” (Mizusawa, ¶4.) However, “[a]t the same time, it is also necessary to minimize the burden on those being certified.” (Mizusawa, ¶4.) Mizusawa explains that “[i]n the conventional technology, since the authentication method is fixed to one, it is not possible to always maintain an optimal balance between authentication accuracy and burden on the person to be authenticated.” (Mizusawa, ¶5.) That is, “to adopt a method capable of realizing the highest authentication accuracy required for the system, an excessive burden is imposed on the person to be authenticated even in cases where authentication accuracy is not required to be that high.” (Mizusawa, ¶5.)

244. Mizusawa addresses this problem through the a personal authentication device, illustrated in Figure 1 below, having “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.” (Mizusawa, ¶7.) The device depicted in Figure 1 uses a facial

authentication unit (unit a) and a fingerprint unit (unit b). However, Mizusawa teaches that unit b “may use, for example, an authentication unit that uses a voice print or an iris to authenticate an individual.” (Mizusawa, ¶21).



Mizusawa, Figure 1

245. In operation, the user selects a desired action via touch panel 401. (Mizusawa, ¶14.) The authentication level determination unit 402 outputs the “authentication level that has been set in advance” associated with the user action to secondary authentication unit 300 and both primary authentication units 100a, 100b.

246. Primary authentication unit 100 (facial authentication) includes imaging unit 110 “that captures a facial image of the person to be authenticated” and

face determination type personal authentication unit 120 “that authenticates the individual using” the captured facial image data “and performs a pre-set operation such as stop or normal authentication depending on the authentication level” received. (Mizusawa, ¶14.) Authentication unit 120 includes a HDD which includes a “previously recorded” authentication list (i.e., the user’s facial biometric references). (Mizusawa, ¶16.)

247. Primary authentication unit b200 includes fingerprint collection unit 210 “that captures the fingerprint of the person to be authenticated” and fingerprint determination type personal authentication unit 220 “that authenticates the individual using” the captured fingerprint data “and performs a pre-set operation such as stop or normal authentication depending on the authentication level” received.” (Mizusawa, ¶17.) Authentication unit 220 also includes an HDD which includes previously recorded authentication list of fingerprint data (i.e., user’s fingerprint biometric reference).

248. 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.” (Mizusawa, ¶20.) Depending on the authentication level set, the selection unit 320 outputs the results of primary unit a, the results of primary unit b, or the results of fusion unit 310. (Mizusawa, ¶20.)

3. Motivation to Combine Kohinata and Mizusawa

249. A POSITA would have been motivated to combine Mizusawa's teachings regarding a flexible, multi-biometric (multi-modal) authentication technique with the Kohinata's cellular phone. For example, Kohinata discloses an authentication module supporting fingerprint authentication. 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.

250. Mizusawa expressly motivates the combination noting that in devices where the "authentication method is fixed to one, it is not possible to always maintain an optimal balance between authentication accuracy and burden on the person to be authenticated." (Mizusawa, ¶5.) That is, in adopting "a method capable of realizing the highest authentication accuracy required for the system, an excessive burden is imposed on the person to be authenticated even in cases where authentication accuracy is not required to be that high." (Mizusawa, ¶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 request 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.

251. Moreover, Mizusawa stresses that its technique “provides an excellent user interface that always minimizes the burden on the person being authenticated while maintaining the required authentication accuracy.” (Mizusawa, ¶6.) This is consistent with the goal of Kohinata of providing an “easy to use” cellular phone “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.” (Kohinata, Abstract.)

252. A POSITA would have been further motivated to use Mizusawa’s multi-modal biometric authentication to improve reliability. It was well known that biometric systems that use only a single biometric characteristic have limitations including noise in the sensed data due to, for example, defective or improperly maintained sensors or unfavorable ambient conditions, nonuniversality (e.g., inability to extract features from fingerprints of certain individuals due to poor quality of ridges), and distinctiveness (i.e., inter-class similarities in the feature sets used to represent the trait). (Jain, 14.) A POSITA would have understood the use of multiple biometric modalities (e.g., face and fingerprint) provides more reliable security due to the presence of multiple, independent pieces of evidence.

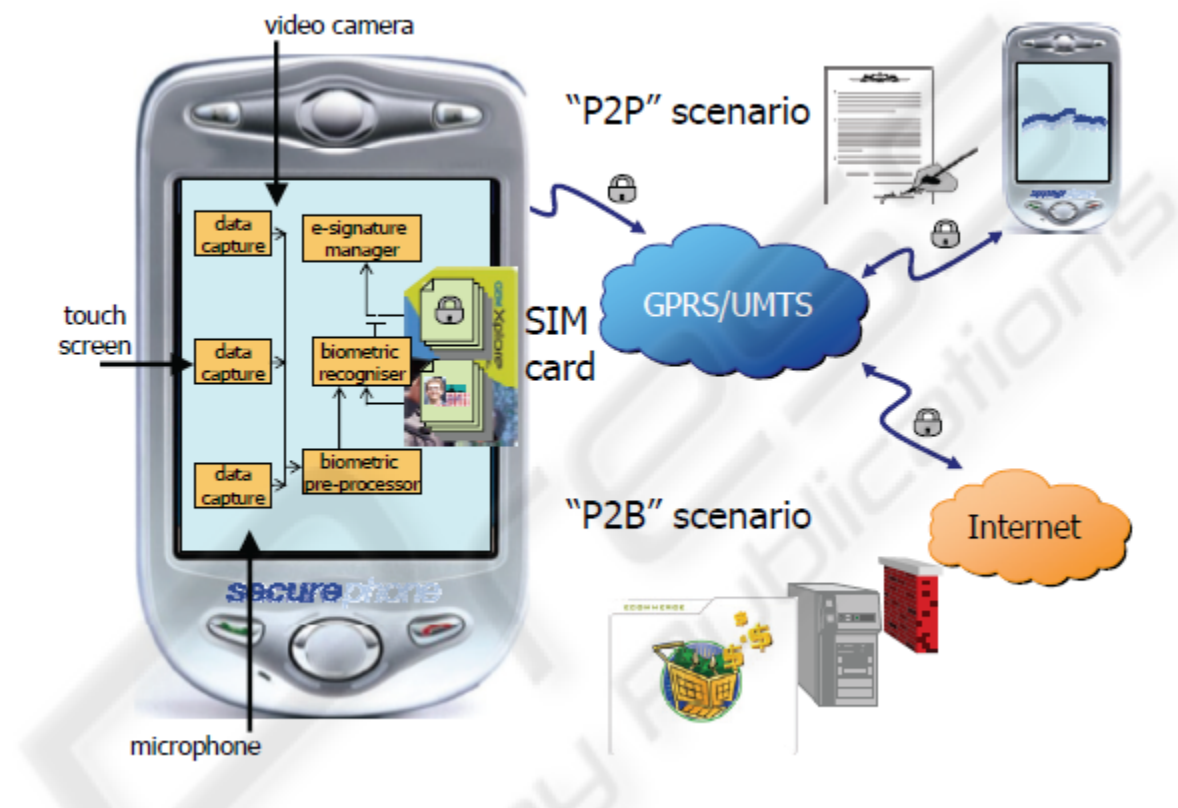
253. A POSITA would also have been motivated to include Mizusawa’s multi-modal authentication to enhance security for specific operations. Kohinata discloses that a “cellular phone is capable of managing a variety of personal data

related to the owner of the phone and conducting settlement, and thus offers functions equivalent to the cash and credit cards.” (Kohinata, 1:16-20.) Because of financial risks to the user due to unauthorized access to a phone which can be used as a credit or debit card, a POSITA would have been motivated to provide a strong level of security associated with financial transactions and would have been led to Mizusawa’s multi-modal biometric authentication, which provides heightened security with minimal user burden.

254. Finally, the combination is nothing more than the application of a known technique (using 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 a single biometric parameter or on two biometric parameters). The results of the combination would have been predictable as I discuss below. And, a POSITA would have been motivated to make the combinations for the reasons discussed above.

255. A POSITA would have had a reasonable expectation of success and the results of the combination would have been predictable because the integration of multi-biometric authentication measures into a mobile device was well-known long before the earliest possible priority date of the ’875 patent. For example, as I discussed in Ground 1, Fadell teaches the use of multiple biometric authentication

measures. Additionally, SecurePhone describes a prototype phone with multiple biometric authentication means. (See SecurePhone, 9.) In this system, illustrated below, facial authentication and voice authentication are used as primary authentication measures. (SecurePhone, 11.) This is consistent with Mizusawa which indicates that voice authentication can be used with facial recognition.



SecurePhone, Figure 1

256. 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 '875 patent, 7:47-49 ("[T]he authenticated user and no other user will have the possibility to have access to the user's personal files and accounts and to be able do

any kind of transaction with, or through them.”); Kohinata, 2:30-35 (“This invention therefore provides a cellular phone equipped with a security function which automatically and reliably authenticates the user and limits, the function of transmission when the user is not the owner, and offers a sufficient degree of safety relying upon a minimum degree of authentication operation.”); Mizusawa, ¶7 (“[T]he present invention has 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.”.) Kohinata and Mizusawa are also reasonably pertinent to the particular problem addressed by the ’875 patent’s invention is involved, i.e., enhancing security through biometric authentication. *Compare* ’875 patent, Abstract (“The apparatus, which is uniquely identified with a unique user, includes a sensor module comprising a plurality of biometric sensors for reading a plurality of personal biological identification parameters of the user and an authentication unit for positive authentication of the user’s personal biological identification parameters stored in the authentication unit”), *with* Kohinata, 7:20-25 (“It is, then, judged if the fingerprint data obtained by the biometric authentication unit are in agreement with the fingerprint data stored in the biometric storage unit (step a4). The authentication is completed if the conditions of step a4 are satisfied as a result of judgement.”), and *also with* Mizusawa, ¶17 (“The primary authentication unit b200 is composed of a

fingerprint collection unit 210 that captures the fingerprint of the person to be authenticated, and a fingerprint determination type personal authentication unit 220 that authenticates the individual using the fingerprint data captured by the fingerprint collection unit 210...”).)

B. Independent Claim 1

1. Preamble [1P]: “Apparatus”

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

257. The combination of Kohinata and Mizusawa discloses an “*apparatus for storing and managing personal and secured data and documentation files associated with a specific user.*”

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

259. Kohinata’s cellular phone stores “*personal and secured data and documentation files associated with a specific user.*” Specifically, Kamata’s memory 11 stores “electronic mails, browsers, software programs related to various applications such as personal schedule management, classified telephone directory, personal schedule data, transmitted and received mails, and data such as of automatic answering machine.” (Kohinata, 3:49-54.) Personal schedule data is an example of both “*personal data*” and “*documentation files*” associated with the user. (Microsoft

Dictionary, 5.) The user's transmitted and received mail are also examples of "*personal data*." This data is "*secured*" because only authenticated individuals can obtain access, as I discuss further below.

260. Kohinata further teaches that its cellular phone "*manag[es]*" access to this "*personal and secured data and documentation files associated with a specific user*" as I discuss further in my analysis of claim 1. For example, Kohinata's "cellular phone is capable of **managing** a variety of personal data related to the owner of the phone." (Kohinata, 1:16-18.) Kohinata's cellular phone "prevent[s] unauthorized use by conducting a minimum degree of required authentication operation which is not perceived by the user." (Kohinata, Abstract.) For example, in Kohinata, when "personal authentication has failed, the function of the cellular phone is limited to receiving a call only, preventing the unauthorized use by the third person." (Kohinata, 10:12-16; *see also* Kohinata, 2:30-59.)

261. The combination of Kohinata and Mizusawa discloses an "*apparatus for storing and managing personal and secured data and documentation files associated with a specific user*."

2. Integrated Biometric Sensors [1A]

[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;
--

262. The combination of Kohinata and Mizusawa 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.*”

263. As I discussed in §VII.A.3, the combination of Kohinata and Mizusawa combines Mizusawa’s teaching of multi-biometric (multi-modal) authentication with Kohinata’s authentication module. That is, as taught by Mizusawa, the cellular phone includes at least two authentication units, each supporting a different type of biometric authentication. Each authentication unit is associated with corresponding sensor used to collect the biometric data from the user. As discussed further below, the combination of Kohinata and Mizusawa discloses a plurality of biometric sensors that are “*integrated within*” the cellular phone.

264. **Fingerprint sensor:** Kohinata’s cellular phone includes fingerprint authentication. Specifically, the phone includes a “biodata obtaining unit 19” which “is a dedicated device for imaging the fingerprint by using a small imaging device such as a CCD camera.” (Kohinata, 5:44-46.) The “biodata obtaining unit ... obtains the fingerprint or the finger data such as feature quantity inherent in the fingerprint from a particular finger of the user of the cellular phone.” (Kohinata, 5:43-50.)

265. Mizusawa also discloses fingerprint authentication. Mizusawa’s fingerprint authentication, like Kohinata, uses a fingerprint collection unit 210 “that

captures the fingerprint of the person to be authenticated.” (Mizusawa, ¶17.) Fingerprint collection unit 210 “includes an optical sensor 211, an acquisition board 212, and a memory 213.” (Mizusawa, ¶18.) The “fingerprint of the individual to be authenticated is read by the optical sensor 211, and is converted into digital data by the acquisition board 212, and is stored in the memory 213 as fingerprint data.” (Mizusawa, ¶18.)

266. 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.

267. **Facial feature sensor:** Mizusawa discloses facial feature authentication. (See Mizusawa, ¶¶14-16.) Facial feature authentication uses an imaging unit 110 “that captures a facial image of the person to be authenticated.” (Mizusawa, ¶14.) Imaging unit 110 includes a “camera 111, an acquisition board 112, and a memory 113.” (Mizusawa, ¶15.) “The face of the individual to be authenticated is photographed by the camera 111, and the photographed image is converted into digital data by the acquisition board 112 and stored in the memory 113 as face image data.” (Mizusawa, ¶15.) Although not explicit, a POSITA would have understood that the user is holding the device in a “selfie-style” position when

the photo is capture. 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.

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

269. The cellular phone of the combination of Kohinata and Mizusawa discloses "*a plurality of biometric sensors*" because the combination uses "multiple primary authentication means that use different authentication methods", as taught by Mizusawa. That is, for example, the cellular phone requires both fingerprint and facial recognition before a user can access a specified resource.

270. Accordingly, the combination of Kohinata and Mizusawa 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.*"

3. Life Signs Detector [1B]

[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;
--

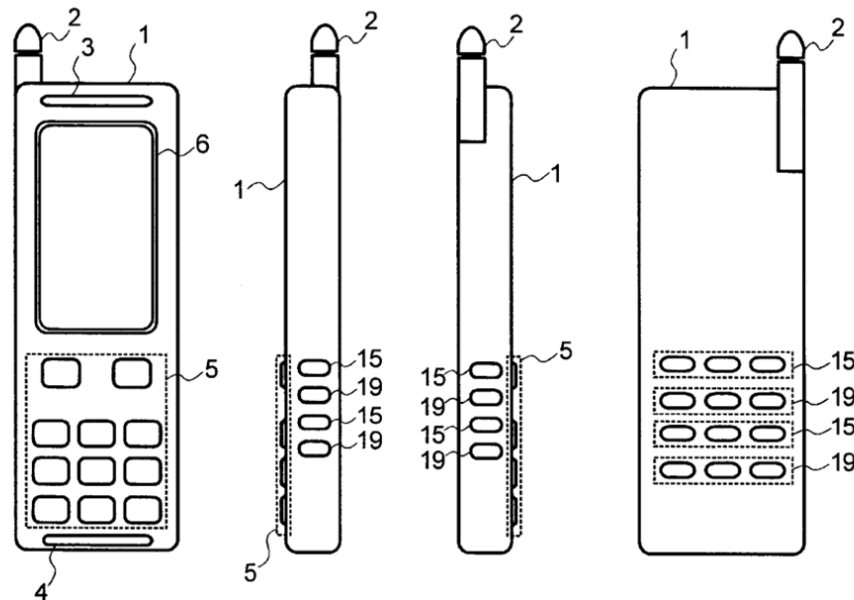
271. The combination of Kohinata and Mizusawa discloses “*at least one life signs detector integrated within the apparatus, said life signs detector being configured to measure and record at least one of said user’s life sign parameters.*”

272. Kohinata’s cellular phone includes a use detection module “for judging the state of contact to the user by measuring temperature.” (Kohinata, 2:56-57.) Use detection module includes a temperature obtaining unit 15, threshold value storage unit 14, and temperature comparator unit 16. (Kohinata, Figure 1.) Temperature obtaining unit 15 “is constituted by a plurality of temperature sensors on the surface of the cellular phone.” (Kohinata, 4:31-33.) Temperature obtaining unit 15 alone or in combination with the threshold storage unit 14 and/or comparator unit 16 is a “*life signs detector.*”

273. The temperature obtaining unit 15 “measur[es] the body temperature of the user when the temperature obtaining unit 15 is touched by the palm or fingers of hand of the user.” (Kohinata, 4:35-38.) The user’s temperature is a “*life sign parameter*” “*of the user.*” In operation, the temperature obtaining unit “starts detecting the temperature” and “the threshold temperatures stored in the threshold value storage unit are compared with the temperature detected.” (Kohinata, 7:13-17.) A POSITA would have understood that to perform the comparison, the measured temperatures are recorded. That is, the “*life signs detector*” of the combination of Kohinata and Mizusawa 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.”

274. The sensors of temperature obtaining unit 15 are “on the surface of the cellular phone.” (Kohinata, 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). (Kohinata, 9:40-54.) Thus, the temperature obtaining unit 15 (*“life signs detector”*) is *“integrated within the apparatus.”*



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

275. The combination of Kohinata and Mizusawa therefore 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."

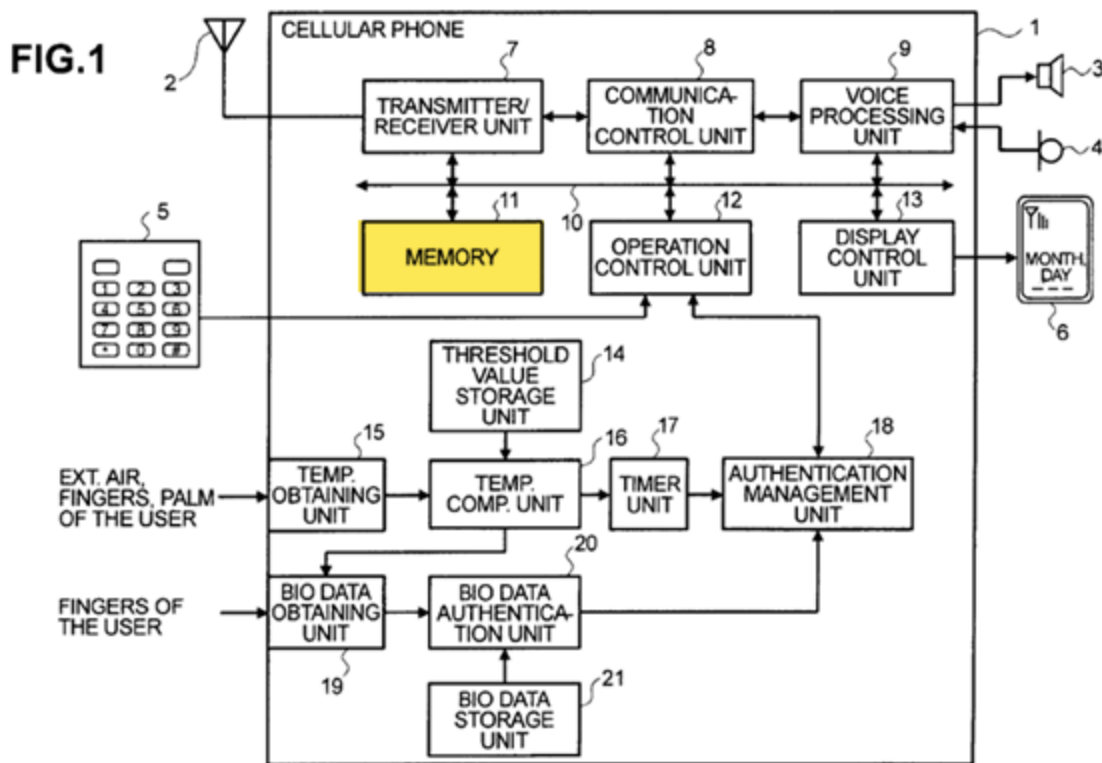
4. First Storage Unit [1C]

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

276. The combination of Kohinata and Mizusawa discloses "*a first storage unit for the storage of said user's data and documentation files.*"

277. As I discussed in Section IV.E.1, "*first storage unit*" is a means-plus-function term with the function being "storing a user's data and documentation files" and the structure being "memory."

278. Kohinata's cellular phone includes "**memory 11** [shaded yellow] comprising a ROM or a RAM for storing electronic mails, browsers, software programs related to various applications such as personal schedule management, classified telephone directory, personal schedule data, transmitted and received mails, and data such as of [sic] automatic answering machine." (Kohinata, 3:21-54.) As I discussed in §V.B.1, personal schedule data is both "*data*" and "*documentation files*" associated with the user and the transmitted/received mails are user "*data*." 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).



Kohinata, Figure 1

279. Thus, under the proper construction, the combination of Kohinata and Mizusawa discloses “a first storage unit for the storage of said user’s data and documentation files.”

280. Should PO contend that “first storage unit” is not a means-plus-function term, the combination of Kohinata and Mizusawa disclose this limitation under plain meaning or any other reasonable construction for the same reasons discussed above.

5. Authentication Unit [1D]

281. The combination of Kohinata and Mizusawa 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.*”

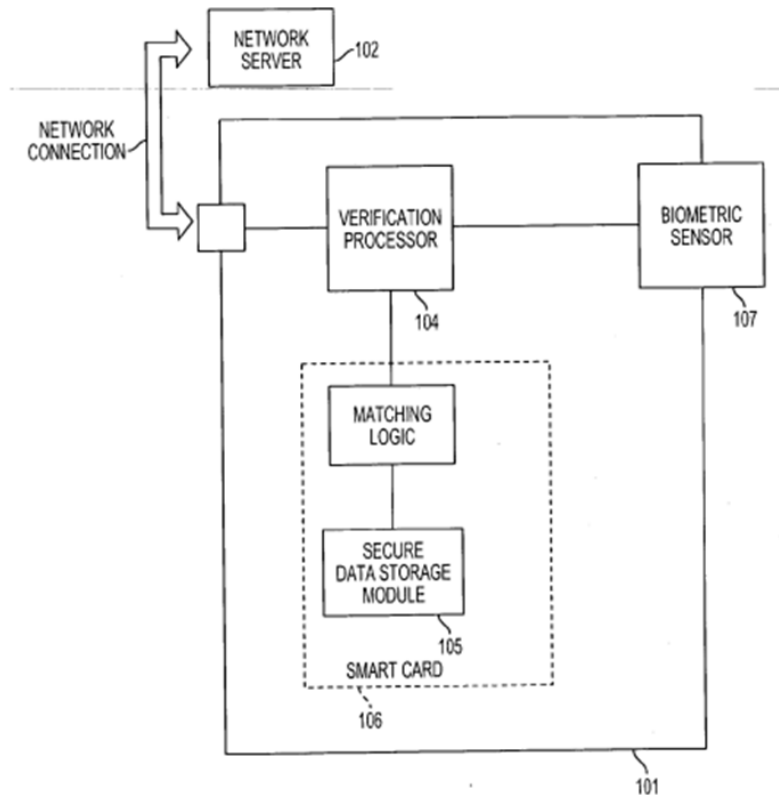
282. Limitation [1D] recites “*an authentication unit comprising a second storage unit.*” As I discussed in §IV.E.3, the term “*authentication unit*” is a means-plus-function term with the function being “comparing the plurality of personal biological biometric identification parameters of the user holding the apparatus with the pre-recorded set of personal biological biometric identification parameters stored in said second storage unit” and the structure being “memory and processor programmed to” perform the function. And as I discuss in §V.B.4, the term “*second storage unit*” is also a means-plus-function term with the function being “storing a pre-recorded set of personal biological biometric identification parameters uniquely associated with the specific user” and the structure being “memory.”

a) Authentication Module

283. Kohinata's cellular phone includes an authentication module including the biometric collection unit (biodata obtaining unit 19), biometric authentication unit 20, storage unit 21, and authentication management unit 18. (Kohinata, 5:42-6:30.) As I discussed in §VII.A.3, the combination of Kohinata and Mizusawa combines Kohinata's multi-biometric (multi-modal) authentication with Kohinata's authentication module. That is, the authentication module of the combined device includes two biometric authentication units (e.g., a facial unit as taught by Mizusawa and a fingerprint unit as taught by both Kohinata and Mizusawa) and integrates Mizusawa's secondary authentication unit (fusion and selection) with Kohinata's authentication management unit.

284. 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. For example, U.S. Patent Publication No. 2003/0115490 to Russo, et al. ("Russo"), published June 19, 2003, describes and motivates such an arrangement.

285. Russo, with reference to Figure 1 that I have reproduced below, 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.” (Russo, Abstract, ¶40.) 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.” (Russo, Abstract, ¶40.) The SecurePhone implementation also implemented multi-biometric authentication and stored its templates in a standalone physical component (SIM card) within the mobile phone. (SecurePhone, 11-12.)



Russo, Figure 1

286. Thus, Kohinata’s cellular phone, as modified by Mizusawa, the comparison processor and template storage of the “authentication module” is implemented in a separate hardware unit.

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

287. Both Kohinata and Mizusawa disclose a “*pre-recorded set of personal biological biometric identification parameters.*”

288. As I discussed in my analysis of Ground 1, when using biometric authentication, a user must first enroll with the system by providing her biometric data. (See, e.g., Jain, 6 (describing the enrollment process of a biometric system).)

As discussed in §VII.A.3, the combination of Kohinata and Mizusawa discloses use of at least two types of biometric authentication so 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.*”

289. 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.” (Kohinata, 5:55-57.) Kohinata teaches the enrollment (registering process) 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.” (Kohinata, 5:65-6:3.) That is, Kohinata teaches “fingerprint data can be registered to [enrolled in]... the biodata storage unit 21 at the time when the cellular phone 1 is purchased (when the initial data are to be set) or after it has been purchased.” (Kohinata, 5:57-60.)

290. 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.” (Mizusawa, ¶16.) This previously recorded facial image data is compared against the captured data.

Similarly, the fingerprint authentication unit includes “fingerprint data in an authentication list recorded in advance in the HDD 222.” (Mizusawa, ¶19.)

291. Thus, the combination of Kohinata and Mizusawa discloses a “*pre-recorded set of personal biological biometric identification parameters* [enrolled/registered biometric data associated with the user].”

c) Second Storage Unit

[1D-2] second storage unit configured to store a pre-recorded set of personal biological biometric identification parameters uniquely associated with the specific user,
--

292. 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.*”

293. As I discussed above, the authentication module of the combination of Kohinata and Mizusawa 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.” (Kohinata, 5:55-57.) Thus, the user’s enrolled/registered biometric data (“*pre-recorded 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*”).

294. Mizusawa similar 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” (Mizusawa, ¶16) and “fingerprint data in an authentication list recorded in advance in the HDD 222” (Mizusawa, ¶19). Thus, internal memory 24 of the combined authentication processing component of Fadell and Moran 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.”

295. Thus, internal memory of the authentication module of the combined device perform the function of “storing a pre-recorded set of personal biological biometric identification parameters uniquely associated with the specific user” and meet the structure of a “memory.” Accordingly, the combination of Kohinata and Mizusawa discloses a “*second storage unit configured to store a pre-recorded set of personal biological biometric identification parameters uniquely associated with the specific user.*”

296. Should PO contend that 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. Such a design would

have been well within the skill of a POSITA prior to the earliest possible priority date of the '875 patent.

297. Should PO contend that “*second storage unit*” is not a means-plus-function term, the combination of Kohinata and Mizusawa discloses this limitation under plain meaning or any other reasonable construction for the same reasons discussed above.

d) Authentication Unit

[1D-1] an authentication unit ... 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;

298. The combination of Kohinata and Mizusawa performs the function of “comparing 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.”

299. As I discussed in §VII.B.2 in my analysis of limitation [1A], the combination of Kohinata and Mizusawa includes “*a plurality of biometric sensors for reading a plurality of personal biological biometric identification parameters of the user holding the apparatus.*” And as I discussed above, the combination of Kohinata and Mizusawa discloses that a “*pre-recorded set of personal biological biometric identification parameters [is] stored in said second storage unit.*”

300. Kohinata discloses that a user provides biological biometric identification parameters, e.g., fingerprint data, when the user attempts to authenticate—suggesting that the user is holding the cellular phone—and that the provided biological biometric identification parameters are *compared* to biological biometric identification parameters that have been stored to Kohinata’s biodata storage unit 21:

The 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.

(Kohinata, 6:6-11.)

301. Mizusawa discloses that primary authentication unit a100 includes “a face determination type personal authentication unit 120 that authenticates the individual using the facial image data captured by the imaging unit 110.” (Mizusawa, ¶14.) Mizusawa also discloses that :

The face determination type personal authentication unit 120 includes a personal authentication unit a 121 and an HDD 122. The 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.

(Mizusawa, ¶16.)

302. Thus, the combination of Kohinata and Mizusawa teaches that for each type of biometric authentication logic/processor in the authentication module “*compare[s] [the] personal biological biometric identification parameter[] of the user holding the apparatus with the pre-recorded set of personal biological identification parameter[] stored in said second storage unit.*”

303. The combination of Kohinata and Mizusawa also discloses the corresponding structure. As I described above, each of Kohinata and Mizusawa discloses memories (biodata storage unit 21 and HDD 122) and a processor (authentication unit) 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 authentication units of both Kohinata and Mizusawa are each a processor or at least equivalent to a processor because both perform a comparison.

304. Thus, the combination of Kohinata and Mizusawa discloses the structure of the authentication unit—memory (internal memory 24) and processor (data processor 28) that performs the recited function. Accordingly, the combination of Kohinata and Mizusawa disclose or at least render obvious “*an authentication unit ... 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.”

305. Should PO contend that the authentication unit requires as single physical processor, a POSITA would have understood that 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).

306. Should PO contend that “*authentication unit*” is not a means-plus-function term, the Kohinata-Mizusawa combination discloses this limitation under plain meaning or any other reasonable construction for the same reasons discussed above.

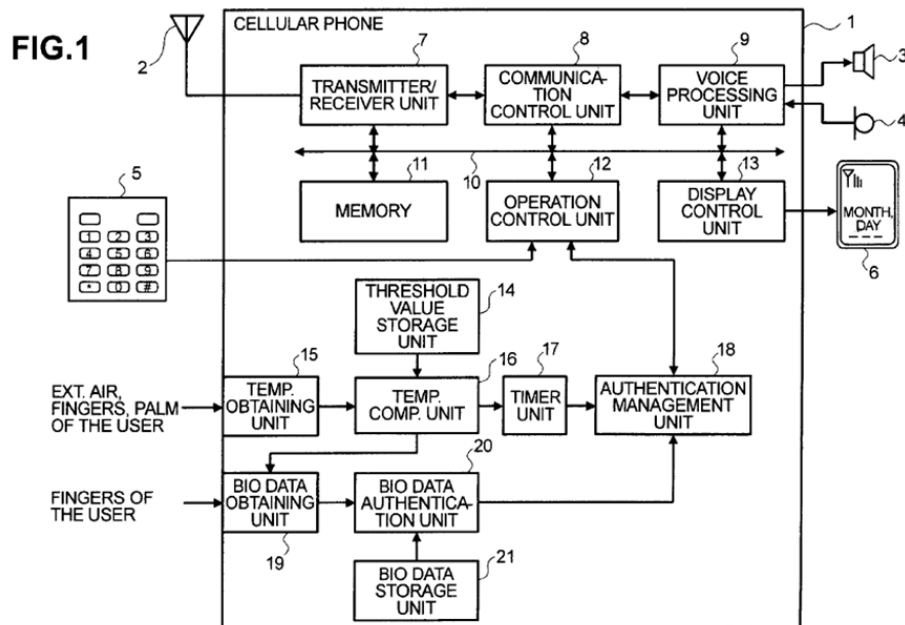
e) Authentication Unit Comprising the Second Storage Unit

307. As I explained in the prior sections (§§VII.B.5.(c)-(d)), the “*authentication unit*” (authentication module) in the combined cellular phone includes internal memory (biodata storage unit 21 and HDD 122). Thus, for the reasons discussed above, the combination discloses “*an authentication unit comprising a second storage unit.*”

6. Processor [1E]

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

308. Kohinata's cellular phone includes operation control unit 12 "comprising chiefly a CPU." (Kohinata, 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." (Kohinata, 3:58-60.) Control unit also "control[s] the temperature obtaining unit 15" (Kohinata, 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 ["*authentication unit*"]" (Kohinata, 10:44-48). To control these units, the CPU must communicate with them.



Kohinata, Figure 1

309. 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.” (Kohinata, 3:65-67.) And as shown above, control unit 12 is coupled to authentication management unit 18 in the authentication module (“*authentication unit*”).

310. The combination of Kohinata and Mizusawa discloses “*a processor in communication with said plurality of biometric sensors, said first storage unit and said authentication unit.*”

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

[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
--

311. 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.*”

312. As I explained in §VII.5.d, each authentication unit (e.g., facial authentication unit and fingerprint authentication unit) in combined device of Kohinata and Mizusawa “*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.*”

313. As discussed in §VII.A.3, the combination of Kohinata and Mizusawa 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 Mizusawa, ¶¶16, 19.) The secondary authentication unit includes fusion unit 310 and 320. “The fusion unit 310 merges the authentication results” of each authentication unit, “thereby authenticating the individual with a higher accuracy than if each authentication was performed separately.” (Mizusawa, ¶20.) The selection unit “outputs the results of the fusion unit 310” when the authentication level is set to the multi-biometric authentication. (Mizusawa, ¶20.)

314. In Kohinata, the authentication management unit 18 “controls the access to various kinds of data stored in the memory 11.” (Kohinata, 6:17-24.) The results of the authentication (e.g., the results of fusion 310) determine whether the access is granted. 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”), user is recognized as the cellular phone’s 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.”** (Kohinata, 6:6-16; *see also* Kohinata, 6:63-7:11, 11:64-12:12.) That is, in the combination, access to personal data and documentation files stored on the phone is only enabled after a positive result from each authentication unit.

315. Thus, the combination of Kohinata and Mizusawa 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.”*

8. Critical Level Detection [1G]

[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.
--

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

317. Kohinata teaches that 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.” (Kohinata, 4:54-63.) When the measured temperature is not within the range of the threshold temperature, authentication is not initiated. (*See, e.g.*, Kohinata, 4:54-63, 7:53-66.) 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.

318. Accordingly, the combination of Kohinata and Mizusawa disclose or at least render suggest “*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.*”

C. Claim 4 – Communicating With An External Device

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.

319. As I discussed in §IV.E.4, the term “*communication and data connection means*” is a means-plus-function term with the “function” being “communicating with an external device” and corresponding “structure” being 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.”

320. 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.” (Kohinata, 1:6-9.) Kohinata also explains the cellular phone receives a call. (Kohinata, 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.”

321. To communicate with an external device, Kohinata’s cellular phone includes a communication module having a transmitter/receiver unit 7, a control unit 8, and a voice processing unit 9. (Kohinata, 4:9-28.) The 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.” (Kohinata, 4:15-22.) Thus, Kohinata’s communication module includes a cellular modem, meeting the structure of the “*communication and data connection means*.”

322. Kohinata’s communication module is “*controlled by and in communication with said processor*.” Kohinata teaches that operation control unit 12 (“*processor*”) “control[s] the communication module.” (Kohinata, 3:57-58.) Accordingly, in Kohinata, the “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.” (Kohinata, 3:62-67.)

323. Thus, the combination of Kohinata and Mizusawa 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.”

VIII. GROUND 4: Kohinata, Mizusawa, and Rosenblatt Render Obvious Claims 15 and 18

324. 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*”, as recited in claim 15. Rosenblatt discloses this missing feature. I provided an overview of Rosenblatt in § VI.A.1.

325. 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*” as recited in claim 18. I note that the integration of GPS modules within wireless devices was well-known before the earliest possible priority date of the ’875 patent. In fact, the ’875 patent admits that at the time of the alleged invention, GPS was “becoming a very common module in most smart phones.” (’875 patent, 16:58-60.) This feature is also disclosed by Rosenblatt.

A. Motivation to Combine

326. 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 cellular phone of Kohinata and Mizusawa. For example, a POSITA would have been motivated to include a wireless transceiver supporting an NFC protocol and/or a GPS module in the cellular phone of Kohinata and Mizusawa.

327. 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 '875 patent, 7:47-49 ("[T]he authenticated user and no other user will have the possibility to have access to the user's personal files and accounts and to be able do any kind of transaction with, or through them."); Kohinata, 1:12-19 ("It is further becoming possible to obtain and watch the images and musical contents. In purchasing these contents, settlement can be done by using the cellular phone. ... [T]he cellular phone is capable of managing a variety of personal data related to the owner of the phone and conducting the settlement, and thus offers functions equivalent to the cash and credit cards."); Mizusawa, ¶7 ("[T]he present invention has 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.”); Rosenblatt, ¶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 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...” (’875 patent, 4:28-31.)

328. A POSITA would have been motivated to include a GPS module in the device of Kohinata and Mizusawa to enhance the features and applications available to a user. Rosenblatt discloses that its GPS module, positioning device 70, can precisely locate the geographical position of the device, e.g., by providing the longitude and latitude of the device and also by positioning the device on a map. (Rosenblatt, ¶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. As such, the positioning device may indicate **positioning on a map, such as a street map or building map**, for example.”).) 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.,* Schiller, 85-88.) Additionally, inclusion of GPS in phones was motivated by the FCC's mandate to provide enhanced emergency services. (*See, e.g.,* Schiller, 28.) These are features that a POSITA would have found beneficial and desirable. These are features that a POSITA would have found beneficial to implement in Kohinata's phone, and, therefore, a POSITA would have found motivation to provide in the phone of Kohinata and Mizusawa a GPS module as taught in Rosenblatt.

329. A POSITA would have further been motivated to include NFC communication module in the Kohinata-Misuzawa wireless device to provide ability for the wireless device to act as NFC financial card (e.g., a debit and credit card). Kohinata motivates the combination describing that a "cellular phone is capable of ... conducting the settlement, and thus offers functions equivalent to the cash and credit cards." (Kohinata, 1:16-19.) Kohinata however fails to provide details permitting the settlement and therefore a POSITA would have been motivated to search for techniques to provide this capability and would have been led to Rosenblatt. Rosenblatt confirms this motivation stressing that the "portability of the device 10 makes it particularly well suited to **performing transactions such as automatic teller machine (ATM) transactions**, and purchase transactions." (Rosenblatt, ¶57.) A POSITA would have found it beneficial to enable Kohinata's

device to communicate with NFC terminals such as ATMs and other payment terminals to enhance the services provided by the wireless device.

330. As another example, Rosenblatt motivates the combination by disclosing communicating with an ATM machine to perform a financial transaction using the user's credit card. (Rosenblatt, ¶57 ("The portability of the device 10 makes it particularly well suited to **performing transactions such as automatic teller machine (ATM) transactions**, and purchase transactions. In conducting such transactions, the device 10 may be used to transfer sensitive data including **credit/debit card information... .**").) A POSITA would have found it beneficial to enable Kohinata's cellular phone to communicate with an ATM machine as a way of performing a financial transaction.

331. The Kohinata, Mizusawa, and Rosenblatt combination would merely involve using Rosenblatt's implementation of a GPS module in Kohinata's cellular phone, such that Kohinata's cellular phone can be precisely located by providing the longitude and latitude of the device and also by positioning the device on a map. (Rosenblatt, ¶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. As such, the positioning device may indicate **positioning on a map, such as a street map or building map**, for example.").)

332. The combination is further merely the use of a 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).

333. 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.

B. Claim 15 – Encoder/Decoder And Wireless Transceiver Module

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.
--

334. The combination of Kohinata, Mizusawa, and Rosenblatt 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*

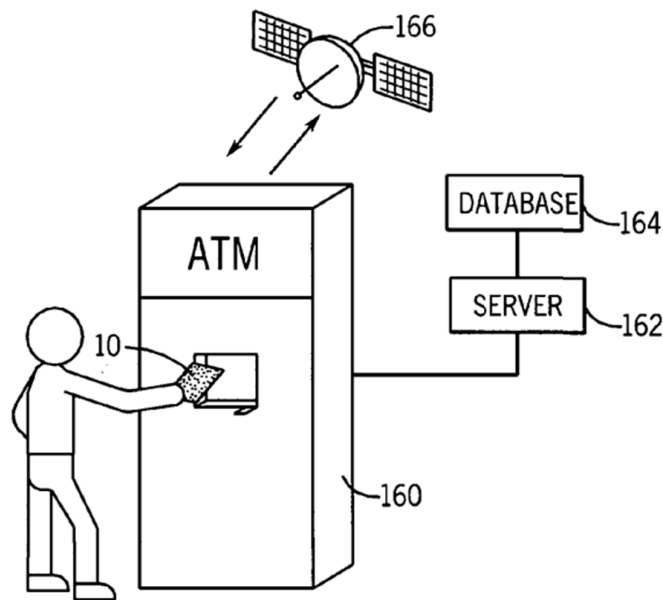
remotely operated electronic locks gates and doors opener using RFID based techniques.”

335. Kohinata’s cellular phone includes a communication module having a transmitter/receiver unit 7 (“*wireless transceiver module*”), a control unit 8, and a voice processing unit 9. (Kohinata, 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.” (Kohinata, 4:22-28.) Thus, Kohinata discloses “*an integrated digital data encoder/decoder.*” As I discussed in §VI.B, 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.*”

336. Kohinata discloses its cellular found is “capable of managing a variety of personal data related to the owner of the phone and **conducting the settlement**” (e.g., debit or credit card payment). (Kohinata, 1:12-19.) Rosenblatt discloses that “the portable electronic devices may be used to wirelessly transfer and receive ... sensitive or personal information, such as **the information to conduct a financial transaction.**” (Rosenblatt, ¶5, *see also* Rosenblatt, ¶31 (“The present disclosure is

directed to techniques for providing security **for wireless communications, including conducting a financial transaction, using a portable electronic device.”).**)

337. As I discussed above in §VI.A.1, Rosenblatt discloses the use of NFC protocol which is an “*RFID based technique*” to conduct a transaction with an ATM, as shown in Figure 9B, below.



Rosenblatt, Figure 9B

338. Accordingly, the combination of Fadell, Moran, and Rosenblatt 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.”

C. Claim 18 – GPS Module

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.

339. As I discussed above, the device in the Kohinata-Mizusawa-Rosenblatt combination includes an integrated GPS module, as taught by Rosenblatt. (Rosenblatt, ¶55 (“The device 10 may also include a positioning device 70 used to determine a user's geographical position. ... The positioning device 70 may utilize the global positioning system (GPS) implemented using satellite communications”).)

340. Rosenblatt specifically discloses that the GPS module can precisely locate the geographical position of the device, e.g., by providing the longitude and latitude of the device for location-based authentication and also by positioning the device on a map. (Rosenblatt, ¶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”).)

341. Thus, the combination of Kohinata, Mizusawa, and Rosenblatt discloses *“an integrated GPS module in communication with the processor to precisely locate the geographical position of the apparatus.”*

IX. Conclusion

342. In signing this declaration, I recognize that the declaration will be filed as evidence in a contested case before the Patent Trial and Appeal Board of the United States Patent and Trademark Office. I also recognize that I may be subject to cross-examination in the case and that cross-examination will take place within the United States. If required, I will appear for cross-examination at the appropriate time. I reserve the right to offer opinions relevant to the invalidity of the challenged claims at issue and/or offer testimony in support of this Declaration.

I hereby declare that all statements made herein of my own knowledge are true and that all statements are made on information and belief are believed to be true, and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 U.S.C. §1001.

Dated: February 20, 2025

Respectfully submitted,



A handwritten signature in dark ink, appearing to read 'A. Wolfe', is written over a horizontal line.

Andrew Wolfe, Ph.D.

APPENDIX

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”)
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”)
1017	Bruce Schneier, “ <i>Applied Cryptography</i> ” 2nd ed. 2006 (“Applied Cryptography”)

Exhibit	Description
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”)
1030	Behzad Razavi, “ <i>RF Microelectronics</i> ,” (1998) (“Razavi”)

Exhibit	Description
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”)