

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

GOOGLE LLC,
Petitioner,

v.

SMARTWATCH MOBILE CONCEPTS, LLC,
Patent Owner.

Case No. IPR2024-00852
Patent No. 10,362,480

DECLARATION OF DAVID H. WILLIAMS

Google Exhibit 1003 Google v Smartwatch
--

TABLE OF CONTENTS

I.	PERSONAL AND PROFESSIONAL BACKGROUND	1
II.	MATERIALS REVIEWED AND CONSIDERED	8
III.	MY UNDERSTANDING OF PATENT LAW	9
	A. Anticipation	11
	B. Obviousness.....	11
IV.	PERSON OF ORDINARY SKILL IN THE ART (“POSA”).....	14
V.	BACKGROUND OF THE TECHNOLOGY.....	16
	A. Form Factors.....	17
	B. Location Services	19
	C. Biometric Sensors and Associated Applications.....	22
	D. User Authentication.....	24
VI.	THE ’480 PATENT	26
	A. Introduction to ’480 Patent.....	26
	B. Prosecution History of the ’480 Patent.....	28
	C. The Challenged Claims	28
VII.	CLAIM INTERPRETATION	30
	A. “at least one of”	30
	B. Other Matters of Claim Interpretation.....	32
VIII.	GROUND 1: CLAIMS 1-5 ARE OBVIOUS OVER AGRAFIOTI ALONE OR WITH BERNEY	32
	A. Agrafioti (EX1011).....	32
	B. Berney (EX1008).....	38
	C. Combining Agrafioti and Berney	40
	D. Claim 1	43
	1. [1PRE]: “A method for enabling a wearable device user to access secured electronic systems”	43
	2. [1A] “placing a wearable device in contact with a user”	43
	a. [1A-1] “said wearable device including a telecommunications carrier access identification module”	44

b. [1A-2] “a cellular RF communications module”	46
c. [1A-3] “said wearable device including...a short-range RF communications module”	48
3. [1B] “achieving secured, short-range RF communication between the wearable device and a secured electronic system”	49
4. [1C] “authenticating the user with at least one of [1C-1] the wearable device, [and] [1C-2] a remote server via cellular communications”	52
a. [1C-1] “the wearable device”	52
b. [1C-2] “a remote server via cellular communications supported by the telecommunications carrier access identification module and the cellular RF communications module”	53
i. User Authentication Through Biometric Authentication Server.	54
ii. User Authentication Through the AAD.....	55
5. [1D] “providing the user with access to or through the secured electronic system once authenticated”	58
6. [1E] “wherein said wearable device comprises a smartwatch including a microphone and skin illumination and measurement hardware”	60
7. [1F] “and wherein authentication of the user is based on biometric information obtained from the user via at least one of the microphone and the skin illumination and measurement hardware”	62
E. Claim 2	63
1. Location.....	63
2. [2E]: “said wearable device includes a GPS module for determining location of the wearable device user with respect to the secured electronic system”	65
3. [2F] “the step of providing a user access to or through the secured electronic systems is also dependent on the location of the wearable device user”	67
F. Claim 3	69

1. [3PRE] – [3D]	69
2. [3E] “said wearable device further comprises a registration module”	69
3. [3F]: “providing a user access to or through the secured electronic system is determined by at least one of the wearable device and the registration module based on at least one of: [3F-1] the user authenticated for access to secured electronic system by the wearable device, ... [3F-4] the user granted access based on location, and [3F-5] the user granted access based on proximity to a secured electronic system”	70
G. Claim 4 [PRE] The method of claim 2, [A] wherein said wearable device further comprises a smartwatch including a microphone and skin illumination and measurement hardware, [B] wherein authentication of the user is based on biometric information obtained from the user via at least one of the microphone and the skin illumination and measurement hardware.....	71
H. Claim 5 [PRE] The method of claim 1, [A] wherein said wearable device further comprises a GPS module for determining location of the wearable device user with respect to secured electronic systems, and [B] wherein access to the secured electronic systems is dependent on the location of the wearable device user in relationship to the secured electronic systems.	71
I. Claim 6 [PRE] The method of claim 3, [A] wherein said wearable device further comprises a smartwatch including a microphone and skin illumination and measurement hardware, [B] wherein authentication of the user is based on biometric information obtained from the user via at least one of the microphone and the skin illumination and measurement hardware.....	72
IX. GROUND 2: CLAIMS 1-9 ARE OBVIOUS OVER AGRAFIOTI, BERNEY, AND LEE	72
A. Lee (EX1009)	72
B. It Would Have Been Obvious to Combine Agrafioti, Berney, and Lee	73
C. Claims 1-6.....	74
1. [1E] (“wherein said wearable device comprises a smartwatch including a microphone and skin illumination and measurement	

hardware” / [4A] (“wherein said wearable device further comprises a smartwatch including a microphone and skin illumination and measurement hardware”) / [6A] (“wherein said wearable device further comprises a smartwatch including a microphone and skin illumination and measurement hardware”)	75
2. [1F] (“wherein authentication of the user is based on biometric information obtained from the user via at least one of the microphone and the skin illumination and measurement hardware”) / [4B] (“wherein authentication of the user is based on biometric information obtained from the user via at least one of the microphone and the skin illumination and measurement hardware”) / [6B] (“wherein authentication of the user is based on biometric information obtained from the user via at least one of the microphone and the skin illumination and measurement hardware”)	76
D. Claim 7	77
1. [7PRE] “A method for enabling a smartwatch user to access secured electronic systems”	77
2. [7A] “placing a smartwatch in contact with a user, the smartwatch including a registration module, a short-range RF communications module, a microphone, and skin illumination and measurement hardware”	77
3. [7B]-[7D] “achieving secured, short-range RF communication between the smartwatch and a secured electronic system”; [7C] “authenticating the user with at least one of the smartwatch and the secured electronic system using at least one biometric obtained from at least one of the microphone and the skin illumination and measurement hardware”; [7D] “providing the user with access to or through the secured electronic system once authenticated”	78
4. [7E] “a subscriber identification module (SIM) and a cellular communications module, wherein authentication of the user is also achievable by accessing a remote server via cellular communications supported by the SIM and the cellular communications module and matching the at least one biometric”	78
E. Claim 8	79

1.	[8A] “wherein the smartwatch wearable device includes a GPS module for determining location of the smartwatch user with respect to the secured electronic system”; [8B] “wherein the step of providing a user access to or through the secured electronic systems is also dependent on a location of the smartwatch user with respect to a location of the secured electronic system”	79
F.	Claim 9 “The method of claim 8, wherein providing a user access to or through the secured electronic system is determined by the registration module based on at least one of: [1] user authentication for access to secured electronic system by smartwatch, [2] user biometric authentication by a wireless carrier, [3] user biometric authentication by remote server, [4] user location, and [5] user proximity to a secured electronic system.”	80
X.	GROUND 3: CLAIMS 2, 5, 8 ARE OBVIOUS OVER AGRAFIOTI-	80
A.	Jun (EX1010).....	80
B.	Combining Agrafioti and Jun	81
C.	Claims 2, 5, 8.....	83
1.	[2E] (“wherein said wearable device includes a GPS module for determining location of the wearable device user with respect to the secured electronic system”)/ [5A] (“wherein said wearable device further comprises a GPS module for determining location of the wearable device user with respect to secured electronic systems”)/ [8A] (wherein the smartwatch wearable device includes a GPS module for determining location of the smartwatch user with respect to the secured electronic system”).....	83
2.	[2F] (“wherein the step of providing a user access to or through the secured electronic systems is also dependent on the location of the wearable device user”)/ [5B] (“wherein access to the secured electronic systems is dependent on the location of the wearable device user in relationship to the secured electronic systems”) / [8B] (“wherein the step of providing a user access to or through the secured electronic systems is also dependent on a location of the smartwatch user with respect to a location of the secured electronic system”)	84
XI.	GROUND 4: CLAIMS 1-9 ARE OBVIOUS OVER THARAPPEL-BERNEY	84

A. Tharappel (EX1007).....	84
B. Combining Tharappel and Berney	87
C. Claim 1	90
1. [1PRE] “A method for enabling a wearable device user to access secured electronic systems”	90
2. [1A] “placing a wearable device in contact with a user”	91
a. [1A-1] “said wearable device including a telecommunications carrier access identification module”	91
b. [1A-2] “a cellular RF communications module”	91
c. [1A-3] “said wearable device including...a short-range RF communications module”	92
3. [1B] “achieving secured, short-range RF communication between the wearable device and a secured electronic system”	94
a. Locked Smartphone as SES:.....	94
b. Other Types of SES.....	95
c. Achieving Secured, Short-Range RF Communication:.....	95
4. [1C] “authenticating the user with at least one of [1C-1] the wearable device, [1C-2] a remote server..., and [1C-3] the secured electronic system via the secured, short-range RF communication”	96
a. Authenticating with Wearable ([1C-1])	96
b. Authenticating with a Remote Server via Cellular Communications ([1C-2])	98
c. Authenticating with SES via Secured, Short-Range RF Communication ([1C-3]).....	99
5. [1D] “providing the user with access to or through the secured electronic system once authenticated”	100
6. [1E] “wherein said wearable device comprises a smartwatch including a microphone and skin illumination and measurement hardware”	101
7. [1F] “and wherein authentication of the user is based on biometric information obtained from the user via at least one of	

the microphone and the skin illumination and measurement hardware”	103
D. Claim 2	103
1. [2PRE]-[2D]	103
2. [2E] “said wearable device includes a GPS module for determining location of the wearable device user with respect to the secured electronic system”	104
3. [2F] “the step of providing a user access to or through the secured electronic systems is also dependent on the location of the wearable device user”	105
E. Claim 3	107
1. [3PRE]-[3D]	107
2. [3E] “said wearable device further comprises a registration module”	107
3. [3F] “providing a user access to or through the secured electronic system is determined by at least one of the wearable device and the registration module based on at least one of: [3F-1] the user authenticated for access to secured electronic system by the wearable device, ... [3F-4] the user granted access based on location, and [3F-5] the user granted access based on proximity to a secured electronic system”	108
F. Claim 4 “[PRE] The method of claim 2, [A] wherein said wearable device further comprises a smartwatch including a microphone and skin illumination and measurement hardware, [B] wherein authentication of the user is based on biometric information obtained from the user via at least one of the microphone and the skin illumination and measurement hardware.”	109
G. Claim 5 “[PRE] The method of claim 1, [A] wherein said wearable device further comprises a GPS module for determining location of the wearable device user with respect to secured electronic systems, and [B] wherein access to the secured electronic systems is dependent on the location of the wearable device user in relationship to the secured electronic systems.”	110
H. Claim 6 “[PRE] The method of claim 3, [A] wherein said wearable device further comprises a smartwatch including a microphone and skin illumination and measurement hardware, [B] wherein	

authentication of the user is based on biometric information obtained from the user via at least one of the microphone and the skin illumination and measurement hardware.”	110
I. Claim 7	110
1. [7PRE] “A method for enabling a smartwatch user to access secured electronic systems”	110
2. [7A] “placing a smartwatch in contact with a user, the smartwatch including a registration module, a short-range RF communications module, a microphone, and skin illumination and measurement hardware”	111
3. [7B] achieving secured, short-range RF communication between the smartwatch and a secured electronic system; [7C] authenticating the user with at least one of the smartwatch and the secured electronic system using at least one biometric obtained from at east one of the microphone and the skin illumination and measurement hardware; [7D] providing the user with access to or through the secured electronic system once authenticated; and	111
4. [7E] “a subscriber identification module (SIM) and a cellular communications module, wherein authentication of the user is also achievable by accessing a remote server via cellular communications supported by the SIM and the cellular communications module and matching the at least one biometric”	112
J. Claim 8 “[PRE] The method of claim 7, [A] wherein the smartwatch wearable device includes a GPS module for determining location of the smartwatch user with respect to the secured electronic system, and [B] wherein the step of providing a user access to or through the secured electronic systems is also dependent on a location of the smartwatch user with respect to a location of the secured electronic system.”	113
K. Claim 9 “The method of claim 8, wherein providing a user access to or through the secured electronic system is determined by the registration module based on at least one of: [1] user authentication for access to secured electronic system by smartwatch, [2] user biometric authentication by a wireless carrier, [3] user biometric	

authentication by remote server, [4] user location, and [5] user proximity to a secured electronic system.”	113
XII. GROUND 5: CLAIMS 1-9 ARE OBVIOUS OVER THARAPPEL-BERNEY-LEE.....	114
A. Tharappel-Berney-Lee.....	114
B. Claims 1-9.....	115
1. [1E] (“wherein said wearable device comprises a smartwatch including a microphone and skin illumination and measurement hardware”) / [4A] (wherein said wearable device further comprises a smartwatch including a microphone and skin illumination and measurement hardware”) / [6A] (“wherein said wearable device further comprises a smartwatch including a microphone and skin illumination and measurement hardware”) / [7A] (“placing a smartwatch in contact with a user, the smartwatch including a registration module, a short-range RF communications module, a microphone, and skin illumination and measurement hardware”).....	116
2. [1F] (“wherein authentication of the user is based on biometric information obtained from the user via at least one of the microphone and the skin illumination and measurement hardware”) / [4B] (“wherein authentication of the user is based on biometric information obtained from the user via at least one of the microphone and the skin illumination and measurement hardware”) / [6B] (“wherein authentication of the user is based on biometric information obtained from the user via at least one of the microphone and the skin illumination and measurement hardware”) / [7C] (“authenticating the user with at least one of the smartwatch and the secured electronic system using at least one biometric obtained from at least one of the microphone and the skin illumination and measurement hardware”)	116
XIII. GROUND 6: CLAIMS 2 AND 4 ARE OBVIOUS OVER THARAPPEL AND JUN	117
A. Combining Tharappel and Jun.....	117
B. Claim 2	118
1. [2PRE] “A method for enabling a wearable device user to access secured electronic systems”	118

2.	[2A] “placing a wearable device in contact with a user, said wearable device including [1] a telecommunications carrier access identification module, [2] a cellular RF communications module, and [3] a short-range RF communications module”	119
3.	[2B] “achieving secured, short-range RF communication between the wearable device and a secured electronic system”	119
4.	[2C] “authenticating the user with at least one of [1] the wearable device, [2] a remote server via cellular communications supported by the telecommunications carrier access identification module and the cellular RF communications module, and [3] the secured electronic system via the secured, short-range RF communication”	120
5.	[2D] “providing the user with access to or through the secured electronic system once authenticated”	121
6.	[2E] “wherein said wearable device includes a GPS module for determining location of the wearable device user with respect to the secured electronic system”	122
7.	[2F] “wherein the step of providing a user access to or through the secured electronic systems is also dependent on the location of the wearable device user”	123
C.	Claim 4	124
1.	[4A] “wherein said wearable device further comprises a smartwatch including a microphone and skin illumination and measurement hardware”	124
2.	[4B] “wherein authentication of the user is based on biometric information obtained from the user via at least one of the microphone and the skin illumination and measurement hardware”	124
XIV.	CONCLUSION.....	124
	CLAIM LISTING	127

I, David H. Williams, declare:

1. I have been retained by Wolf, Greenfield & Sacks, P.C., counsel for Petitioner Google LLC, to assess claims 1-9 (the “challenged claims”) of U.S. Patent No. 10,362,480 (“the ’480 patent”). I have personal knowledge of the facts and opinions set forth in this declaration and believe them to be true. If called upon to do so, I would testify competently thereto. I am being compensated for my time at my standard rate, plus actual expenses. My compensation is not dependent in any way upon the outcome of the *inter partes* review of the ’480 patent.

2. My analysis is based on my years of education, research and experience, as well as my investigation and study of relevant materials, including those cited herein.

I. PERSONAL AND PROFESSIONAL BACKGROUND

3. I am an expert in the fields of electrical engineering, electronic system security (including system access based on user location or proximity to the system), and user authentication techniques. I have studied, practiced, and researched in this field for over 35 years. More specifically, as of 2015, I had more than 13 years of industry experience in electronic systems security and access to such systems based on user authentication over the period from 1987 through 2010. I have summarized in this section my education background, work experience, and other relevant qualifications. My curriculum vitae, which I

understand has been designated EX1004, further describes my background and experience.

4. I earned a Bachelor of Science in Electrical Engineering degree (BSEE), with an emphasis on digital system design, from Purdue University in 1983. In 1987, I earned a Master of Business Administration degree (MBA), with a focus on information systems management, from The University of Texas at Austin.

5. From 1983 to 1985, I worked at Hughes Aircraft Company as an electrical engineer, where I focused on microcomputer and digital system design on the F-15 fighter radar system.

6. After completing my MBA, I worked for Deloitte Consulting (originally Touche Ross) as a Senior Manager from 1987 to 1991. At Deloitte, I provided consulting services for technology-intensive companies in developing business and product strategies.

7. From 1991 to 1993, I worked as a Senior Associate in the Information Technology Practice of Booz Allen & Hamilton, providing consulting services for communications industry and information technology-intensive companies.

From 1993 to 2002, I worked at Accenture as an Associate Partner in the Communications and High-Technology Strategy and Information and Technology Strategy groups. At Accenture, I led development of business, technology, and

product strategies for numerous communications and technology-centric companies looking to enter new markets. I specialized in new product design, development, and implementation, as well as network infrastructure design need to support next generation, high bandwidth-consuming digital media content and associated infrastructure.

8. In 2002, I founded E911-LBS Consulting, which was later renamed E911-LBS Forensics Engineering (“E911-LBS”). I am the president of E911-LBS, which provides services across the entire wireless value chain, particularly with respect to technology and business strategic planning and product design, development, implementation, and ongoing management and operations. (E911 refers to “enhanced 911,” which is a system for emergency dialing in which the caller’s location is automatically determined and provided to the emergency dispatcher. LBS refers to location-based services.)

9. I have worked on a wide variety of matters as a consultant through E911-LBS. Relevant to this matter, I managed the development of the Nextel (now Sprint/T-Mobile) Location-Based Services strategy, including researching and incorporating context-aware/presence concepts into product/device and network engineering plans. I also provided E911 consulting expertise in support of new spectrum regulatory approval and technical implementation issues for a

startup carrier and managed the design, collection, and analysis of E911 infrastructure deployment of western region of major wireless carrier.

10. Additionally, from 2007 to 2010 I worked for AT&T Mobility, first in a consulting role as a Consumer LBS Product Realization Manager, then as a Senior Product Manager – Enterprise LBS. At AT&T Mobility, my work included design, troubleshooting, and implementation of AT&T location-related network, application, user interface, digital media and content delivery, and privacy infrastructure and associated issues such as accuracy and privacy. I also managed products including telematics, fleet/vehicle management, asset/freight management, and mobile resource management GPS/LBS apps on a variety of platforms such as Telenav, and played key role in design of company-wide location services product and implementation roadmap.

11. I have written a number of books on wireless location including: The Definitive Guide to IoT Sensors and IoT Use Cases (In Development), The Definitive Guide to GPS, RFID, Wi-Fi, and Other Wireless Location-Based Services (2005/2009 versions, new version in development), The Definitive Guide to Wireless E911, and (co-authored) The Definitive Guide to Mobile Positioning and Location Management.

12. I am the inventor or a co-inventor of nine issued U.S. patents and numerous pending applications. These include:

- “Method and apparatus for providing mobile social networking privacy.” (U.S. Patent Number 8,613,109, issued on December 17, 2013).
- “Systems and methods of using wireless location, context, and/or one or more communication networks for monitoring for, preempting, and/or mitigating pre-identified behavior.” (U.S. Patent Number 10,477,342, Issued November 12, 2019).
- “Systems and methods for monitoring for and preempting pre-identified restriction violation-related behavior(s) of persons under restriction.” (U.S. Patent Number 10,497,242, Issued December 3, 2019).
- “Systems and methods for providing location-based security and/or privacy for restricting user access.” (U.S. Patent Number 10,555,112, Issued February 4, 2020).
- “Systems and methods for developing, monitoring, and enforcing agreements, understandings, and/or contracts.” (U.S. Patent Number 10,853,897, Issued 12/1/2020).
- “Systems and methods for monitoring for and preempting pre-identified restriction violation-related behavior(s) of persons under

restriction.” (U.S. Patent Number 10,861,307, Issued December 8, 2020).

- “Systems and methods for monitoring for and lowering the risk of addiction-related or restriction violation-related behavior(s).” (U.S. Patent Number 11,388,546, Issued July 12, 2022).
- “Systems and methods for monitoring for and preempting the risk of a future occurrence of a quarantine violation.” (U.S. Patent Number 11,412,353, Issued August 9, 2022).
- “Dynamic and adaptive systems and methods for rewarding and/or disincentivizing behaviors” (U.S. Patent Number 11,636,941, Issued April 25, 2023).

13. Specifically, I have had much more than two years of industry experience or graduate-level experience with user authentication techniques for accessing secure electronic systems. In fact, as demonstrated by the examples below, as of 2015, I had more than 13 years of industry experience in electronic systems security and access to such systems based on user authentication over the period from 1987 through 2010. Specifically:

- 1987-1990 - As Senior Consultant at Deloitte and Touche, designed communications network and oversaw software design for from-scratch data center (mainframe) interfacing with 250+

- hotels and restaurants, including all security protocols for interfacing with POS hotel and restaurant systems (Brock Hotels, Chuck-E-Cheese). (2.5 years)
- 1991-1992 – As Senior Associate at Booz Allen & Hamilton, led Project Management Office for design of TravelBase (American Airlines system for travel agents), including oversight of design of security and authorization for using TravelBase. (1 year)
 - Mid-1990s – As Senior Manager at Accenture, designed and implemented AT&T Local Services Resale platform, including all aspects of user authentication and security. (approximately 2 years)
 - 1998-2000 – Led the development of Nextel's location-based services product strategy, and the design of the underlying network and IT architectures to support such products, including user authentication and security. (approximately 2 years)
 - 2004-2006 – Developed NAVTEQ web developer ecosystem, which included both the user authentication and security requirements and tools for various map data packages, as well as web developer access to overall platform. (approximately 2 years)
 - (2007-2010) - Led design finalization and implementation of several of AT&T's first generation of location-based services, as

well as design of underlying location enabler network. Became the only non-employee inventor on U.S. Patent Number 8,613,109, Method and Apparatus for Mobile Social Networking Privacy (issued December 17, 2013). (approximately 4 years)

- (2013-2014) – Provided expert services in assessing validity of GPS tracking bracelet/system in parole violation matters.

14. In addition to the above, I have also provided expert analysis in connection with patent proceedings in this field for clients such as Nest and VIVINT. I have also worked with wearables (including wearable tags and sensor tracking systems) for spatial orientation detection, health monitoring, and tracking. This includes, for example, expert services in connection of GPS tracking for parole violations, as well as my own research and development work related to data collection from wearable devices, including wrist wearable devices, as shown in my patents. *See* paragraph 12. I also have experience working with near-range communication, such as Bluetooth, RFID, and WiFi. This includes in my expert testimony work. This experience is set forth in my CV, EX1004.

II. MATERIALS REVIEWED AND CONSIDERED

15. My findings, as explained below, are based on my years of education, research, experience, and background in the field of electronic system security, as well as my investigation and study of relevant materials for this declaration. When

developing the opinions set forth in this declaration, I assumed the perspective of a person having ordinary skill in the art, as set forth in Section IV below. In forming my opinions, I have studied and considered the materials identified in Appendix A, Materials Considered.

III. MY UNDERSTANDING OF PATENT LAW

16. In developing my opinions, I discussed various relevant legal principles with Petitioner's attorneys. Though I do not purport to have prior knowledge of such principles, I understood them when they were explained to me and have relied upon such legal principles, as explained to me, in the course of forming the opinions set forth in this declaration. My understanding in this respect is as follows:

17. I understand that "*inter partes* review" (IPR) is a proceeding before the United States Patent & Trademark Office for evaluating the patentability of an issued patent's claims based on prior-art patents and printed publications.

18. I understand that, in this proceeding, Petitioner has the burden of proving that the challenged claims of the '480 patent are unpatentable by a preponderance of the evidence. I understand that "preponderance of the evidence" means that a fact or conclusion is more likely true than not true.

19. I understand that, in IPR proceedings, claim terms in a patent are given their ordinary and customary meaning as understood by a person of ordinary

skill in the art (“POSA”) in the context of the entire patent and the prosecution history pertaining to the patent. If the specification provides a special definition for a claim term that differs from the meaning the term would otherwise possess, the specification’s special definition controls. If a claim element is expressed as a “means” for performing a specified function, I understand that it covers the corresponding structure described in the specification and equivalents of the described structure. I have applied these standards in preparing the opinions in this declaration.

20. I understand that determining whether a particular patent or printed publication constitutes prior art to a challenged patent claim can require determining the effective filing date (also known as the priority date) to which the challenged claim is entitled. I understand that for a patent claim to be entitled to the benefit of the filing date of an earlier application to which the patent claims priority, the earlier application must have described the claimed invention in sufficient detail to convey with reasonable clarity to the POSA that the inventor had possession of the claimed invention as of the earlier application’s filing date. I understand that a disclosure that merely renders the claimed invention obvious is not sufficient written description for the claim to be entitled to the benefit of the filing date of the application containing that disclosure.

21. I understand that for an invention claimed in a patent to be patentable, it must be, among other things, new (novel—*i.e.*, not anticipated) and not obvious from the prior art. My understanding of these two legal standards is set forth below.

A. Anticipation

22. I understand that, for a patent claim to be “anticipated” by the prior art (and therefore not novel), each and every limitation of the claim must be found, expressly or inherently, in a single prior-art reference. I understand that a claim limitation is disclosed for the purpose of anticipation if a POSA would have understood the reference to disclose the limitation based on inferences that a POSA would reasonably be expected to draw from the explicit teachings in the reference when read in light of the POSA’s knowledge and experience.

23. I understand that a claim limitation is inherent in a prior art reference if that limitation is necessarily present when practicing the teachings of the reference, regardless of whether a person of ordinary skill recognized the presence of that limitation in the prior art.

B. Obviousness

24. I understand that a patent claim may be unpatentable if it would have been obvious in view of a single prior-art reference or a combination of prior-art references.

25. I understand that a patent claim is obvious if the differences between the subject matter of the claim and the prior art are such that the subject matter as a whole would have been obvious to a person of ordinary skill in the relevant field at the time the invention was made. Specifically, I understand that the obviousness question involves a consideration of:

- the scope and content of the prior art;
- the differences between the prior art and the claims at issue;
- the knowledge of a person of ordinary skill in the pertinent art; and
- if present, objective factors indicative of non-obviousness, sometimes referred to as “secondary considerations.” To my knowledge, the Patent Owner has not asserted any such secondary considerations with respect to the ’480 patent.

26. I understand that in order for a claimed invention to be considered obvious, a POSA must have had a reason for combining teachings from multiple prior-art references (or for altering a single prior-art reference, in the case of obviousness in view of a single reference) in the fashion proposed.

27. I further understand that in determining whether a prior-art reference would have been combined with other prior art or with other information within the knowledge of a POSA, the following are examples of approaches and rationales that may be considered:

- 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 a known technique to improve similar devices in the same way;
- applying a known technique to a known device ready for improvement to yield predictable results;
- applying a technique or approach that would have been “obvious to try,” *i.e.*, 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 it for use in either the same field or a different one based on design incentives or other market forces if the variations would have been predictable to one of ordinary skill in the art;
- some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill to modify the prior-art reference or to combine prior-art reference teachings to arrive at the claimed invention. I understand that this teaching, suggestion or motivation may come from a prior-art reference or from the knowledge or common sense of one of ordinary skill in the art.

28. I understand that for a single reference or a combination of references to render the claimed invention obvious, a POSA must have been able to arrive at the claimed invention by altering or combining the applied references.

IV. PERSON OF ORDINARY SKILL IN THE ART (“POSA”)

29. I have been informed and understand that for purposes of assessing whether prior-art references disclose every element of a patent claim (thus “anticipating” the claim) and/or would have rendered the claim obvious, the patent and the prior-art references must be assessed from the perspective of a person having ordinary skill in the art (“POSA”) to which the patent is related, based on the understanding of that person at the time of the patent claim’s priority date. I have been informed and understand that a POSA is presumed to be aware of all pertinent prior art and the conventional wisdom in the art, and is a person of ordinary creativity. I have applied this standard throughout my declaration.

30. The ’480 patent involves technology in the field of electronic systems security and access to such systems based on user authentication. I have been asked to provide my opinions as to the state of the art in this field by August 12, 2015. I use this timeframe because the face of the ’480 patent indicates an earliest claimed priority date of August 12, 2015. Whenever I offer an opinion in this declaration about the knowledge of a POSA, the manner in which a POSA would have understood the claims of the ’480 patent or its description, the manner in

which a POSA would have understood the prior art, or what a POSA would have been led to do based on the prior art, I am referencing the August 12, 2015 timeframe, even if I do not say so specifically in each case.

31. I understand that the Patent Owner may attempt to prove that the alleged invention recited in the challenged claims was conceived at some time prior to the earliest claimed priority date on the face of the patent. At the time of this declaration, I am unaware of the Patent Owner having alleged any earlier conception date or produced any evidence to establish any earlier conception date.

32. In my opinion, a person of ordinary skill in the art in the August 12, 2015 timeframe (“POSA”) would have had a bachelor’s degree in electrical engineering, computer science, or a related field, plus at least two years of industry experience or graduate-level experience with user authentication techniques for accessing secure electronic systems. This person would have been capable of understanding and applying the teachings of the ’480 patent and the prior-art references discussed in this declaration.

33. By 2015, I held a Bachelor of Science in Electrical Engineering (BSEE) degree with an emphasis in Digital System Design, in addition to a Master of Business Administration (MBA) in Information Systems Management, and I had over 13 years of experience with user authentication techniques for accessing secure electronic systems. *See* paragraph 13. Therefore, I was a person of more

than ordinary skill in the art during the relevant timeframe. Additionally, I worked with many people who fit the characteristics of the POSA, and I am familiar with their level of skill. When developing the opinions set forth in this declaration, I assumed the perspective of a person having ordinary skill in the art, as set forth above.

V. BACKGROUND OF THE TECHNOLOGY

34. The background of the various technical fields/disciplines associated with the '480 patent are straightforward, and all were well established prior to the 2015 priority date. Specifically, the following was well known to a POSA by that time:

- Numerous form factors of computer system-oriented electronic devices existed, including smartwatch-type forms, that could communicate with other systems using known methods;
- Such form factors could use well-known absolute and relative location techniques/technologies to be located and to locate other devices around them;
- Such form factors also incorporated other biometric-type sensors, including skin illumination; and
- All the above could be used for electronic system access/security purposes.

A. Form Factors

35. The concept of “wearables” in the form of electronics and computers has been around for decades. In fact, the first IEEE Symposium for Wearable Computers (ISWC) in 2022 celebrated its 25th anniversary of the first symposium in 1997.¹

36. The concept of, and use of the term, “Smartwatch” was known at least as early as 2007, with an article that introduced “our concept of a Smartwatch -- a wrist-worn form of a general-purpose wearable computer.”² These kinds of articles about smartwatches focused on a variety of factors, but generally they narrowed into two areas: how to get as much functionality into the form factor, and how to do so while making the user interface as friendly as possible.

37. Addressing both of these areas depended on, or at least utilized, some form of communications capabilities with other devices, such as people’s phones. As a consequence, smartwatch innovations incorporated various communications

¹ EX1042, “The 25th Edition of the International Symposium on Wearable Computers,” IEEE Pervasive Computing (April-June 2022).

² EX1043, Pascoe, “On the Use of Mobile Tools in Everyday Life,” OZCHI '07: Proceedings of the 19th Australasian conference on Computer-Human Interaction: Entertaining User Interfaces, 39-47 (November 2007).

methods, including RF, Bluetooth, and others, such as described by 2001 patent application Berney (EX1008), enabling a variety of use cases such as its “authentiswatch” checkout capability, below:

Patent Application Publication Mar. 6, 2003 Sheet 3 of 7 US 2003/0046228 A1

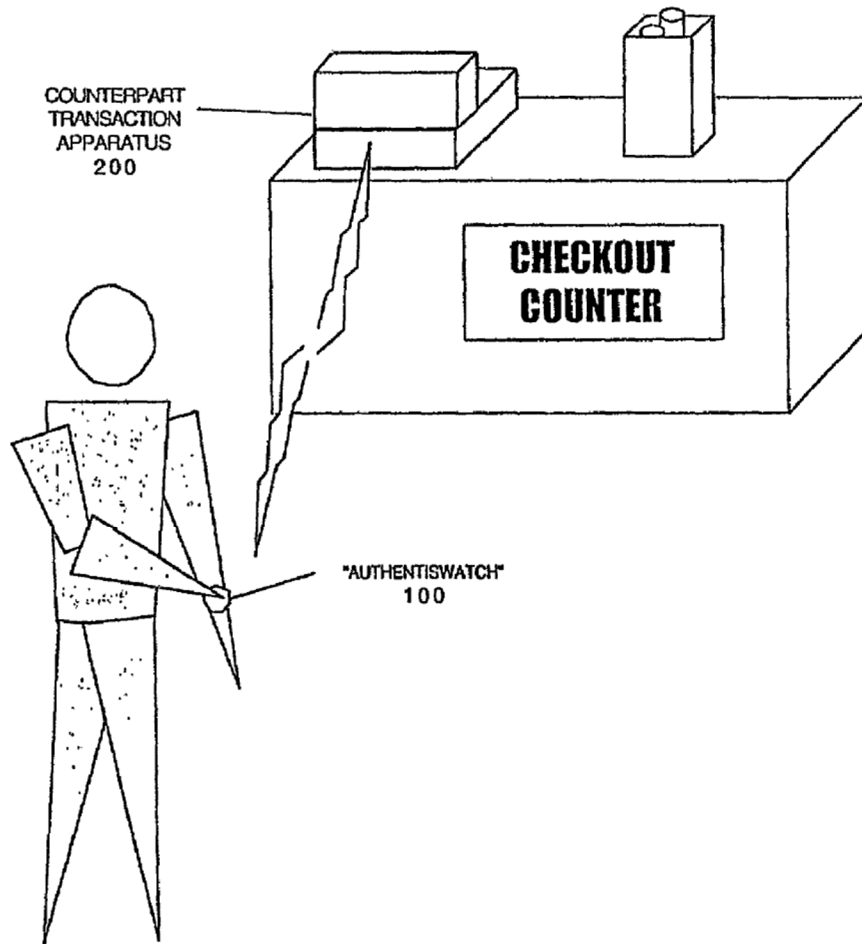


FIGURE 3

B. Location Services

38. One core aspect of mobile devices (including smartwatches), and key requirement in most mobile applications, is to take advantage of their mobility, e.g. use their location in some form to aid or add functionality.

39. Since the early days of mobile devices, and particularly since the passage of The 1996 Telecommunications Act, more and more devices and applications have had GPS and/or other location capabilities built in. For example, one of the first GPS-enabled phones was the Benefon Esc! launched in 1999.³

40. Location was not just limited to mobile phones; watches were a natural companion form factor. In fact, in 1927 there was a watch that used paper maps (manually) scrolled on a watch to help people navigate.⁴

³ EX1044, IT History Society, “Benefon ESC!,” available at <https://www.ithistory.org/db/hardware/benefon/benefon-esc>

⁴ EX1045, “(Sc)Rolling Down the Highway: Vintage 1927 Analog GPS,” available at <https://gajitz.com/scrolling-down-the-highway-vintage-1927-analog-gps/>

(Sc)Rolling Down the Highway: Vintage 1927 Analog GPS



41. Fast forwarding to modern times saw the 2003 Garmin Forerunner watch having GPS to enable a variety of location-based services:⁵

⁵ EX1046, “Garmin Forerunner,” available at <https://trigearlab.com/garmin-forerunner/>.

2003: Garmin Forerunner

WAREABLE



42. It is worth pointing out that location-enabled devices can utilize two types of locations: absolute and relative. Absolute location is a very specific location, such as a latitude and longitude, or a street address. This kind of location generally has some sort of reference system underlying it, such as the WGS 84 reference system for the United States GPS system.⁶

43. The second kind of location is relative: where a device (e.g. person) is relative to some other person, place or thing. While GPS can be used to determine relative location, there are other, more efficient ways, such as whether (or not) one device is within range of the Bluetooth signal for another device. Since there such

⁶ EX1047, “World Geodetic System,” available at

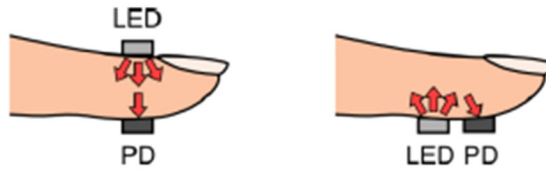
https://en.wikipedia.org/wiki/World_Geodetic_System#WGS84

signals have a very short range (e.g. 10 meters), such techniques are very good for determining if a device is “in proximity” to another device. Both absolute and relative location determination are useful in location services, depending on the application, use cases, and capabilities of the devices involved. These distinctions and key aspects are discussed more in the Grounds (particularly for claim 2).

C. Biometric Sensors and Associated Applications

44. Location was not the only capability that innovators looked to include in form factors such as smartwatches; numerous other ones soon followed, particularly biometric-related ones (particularly useful for fitness and other purposes, such as authentication, discussed shortly). All sorts of sensors were evaluated and incorporated into smartwatch design, including the “photoplethysmogram sensors,” near infrared sensors, light sensors, and optical sensors described in Agrafioti, prior art in this matter. Applications using these kinds of sensors were varied; for example Agrafioti (EX1011) states that its biometric wearable may include pulse detection ([0108], [0116]) or vein pattern recognition ([0028]).

45. These kinds of sensors are known as skin illumination measurement hardware, because they emit light (or other optical output) and measure a response to that light (or other optical output). Other art, such as Tamura (Exhibit 1030) uses the associated light reflection, seen below, for a variety of purposes:



(transmission) (reflectance)

46. These capabilities, and continued development of computer-type capabilities in smartwatches, such as the 2012 Sony SmartWatch below, had set the logical stage for using smartwatches for authenticating accessing electronic systems using smartwatches, next.

2012: Sony SmartWatch



D. User Authentication

47. Well before biometrics came on the scene, computer security experts recognized the utility of requiring multiple layers of authentication to access systems and applications. For example, a 1990 study, *When a Password is Not a Password*, looked at “How two-factor systems can be technically overlaid for implementation in existing environments.”⁷

48. Location-related two-factor authentication innovations also occurred, taking advantage of the location capabilities explosion that followed The 1996 Telecommunication Act. Various research investigated various aspects of using location—and biometrics—in such authentication and authorization. For example, a 2012 paper—*Location-based Authentication and Authorization Using Smart Phones*⁸—while focusing on using mobile location in user authentication and authorization, emphasized the utility of broader biometrics for such purposes:

⁷ EX1048, Weiss, “When a Password Is Not a Password,” IEEE Proceedings IEEE International Carnahan Conference on Security Technology, Crime Countermeasures, Abstract (1990).

⁸ EX1049, Zhang, “Location-based Authentication and Authorization Using Smart Phones,” IEEE Proceedings 11th International Conference on Trust, Security and Privacy in Computing and Communications (2012).

“Authentication and authorization are two of the most important security features for mobile transaction systems. Most commonly, these schemes depend on three factors: what you know (secret), what you have (token), **and what you are (biometrics).**” Abstract (emphasis added).

49. By the time of the '480 patent 2015 priority date, there had been numerous research studies and innovations in such biometric-based authentication and authorization, including for form factors such as smartwatches. Studies such as a 2010 article, *Biometric Identification Through Hand Vein Patterns*⁹, focused on aspects such as “statistical processing of the...vein patterns,” while Lee (2013, EX1009), describes a wrist wearable such as a watch with contact sensors “for authenticating a user based on a wrist vein pattern.” Lee, [0003]. Other art, such as Jun (EX1010) disclosed at length key applications for such capabilities, such as unlocking car doors:

⁹ EX1050, Yuksel, “Biometric Identification Through Hand Vein Patterns,” IEEE Proceedings 2010 International Workshop on Emerging Techniques and Challenges for Hand-Based Biometrics, Abstract (2010).

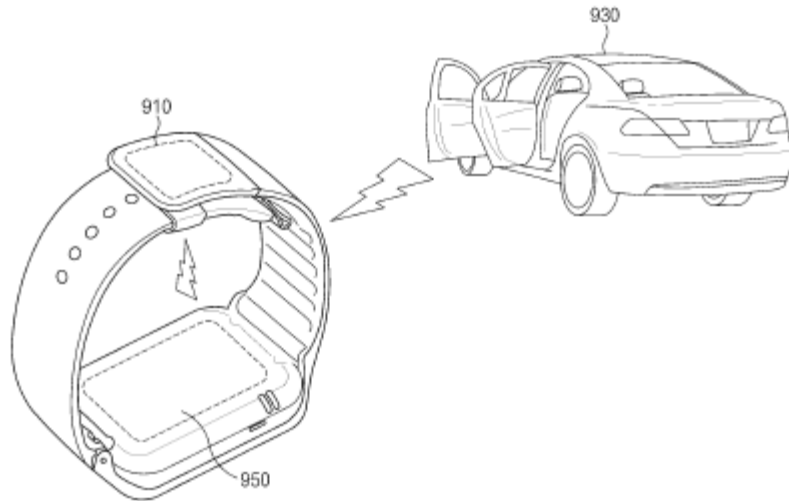


FIG. 9

50. Thus, in total, a POSA would recognize that by the time of the '480 priority date, all the component relevant and associated technology fields and disciplines were well known.

VI. THE '480 PATENT

A. Introduction to '480 Patent

51. The '480 patent relates to wearable devices (“wearables”), e.g., smartwatches, that allow a user to access secured electronic systems based on user authentication. EX1001, Abstract, 2:53-3:61. An SES is “broadly defined” as any “system requiring electronic initiation for its operation or to gain access to it.” EX1001, 4:57-59. Examples include secured entry barriers (safes, doors), laboratory equipment, ATMs, payment mechanisms (e.g., parking meters), point-of-sale, and other secured databases. EX1001, 2:60-3:3. Wearables, including smartwatches, with “wireless communication capability” and a subscriber

identification module (“SIM”) were already well-known and on the market by 2015. EX1001, 1:37-65, 4:51-52.

52. The claimed authentication techniques include biometric authentication (voice, heart rate pattern) and relative location authentication (user location in relation to the SES). EX1001, 3:4-:3; 5:62-7:22. The wearable includes appropriate hardware to enable such authentication, such as a microphone (for voice authentication) and “skin illumination hardware” (for “vital pattern” authentication). EX1001, 3:29-37, 7:11-12. The disclosed authentication methods can be used independently or together. EX1001, 5:50-53.

53. Claims 1-9 are method claims. The independent claims share common steps [PRE] through [D], which relate to wearable functionality and hardware that was well-known in 2015. The patent’s purported novelty appears in steps [E]-[F], which recite certain hardware (e.g., a microphone, skin illumination/measurement hardware, a GPS module) and related user authentication techniques to access a “secured electronic system” (“SES”). As demonstrated herein, these purportedly novel hardware components and user authentication techniques also were well-known and used in wearables by 2015. It was also well-established by 2015 that multifactor authentication (e.g., requiring user authentication to be verified via more than one authentication technique) enhanced security and was an important feature in environments involving highly

sensitive information or areas. It would have been obvious over one or more of the references relied on in the Petition and discussed herein to arrange well-known hardware components and authentication techniques in the claimed manner, and POSAs would have expected success in doing so.

B. Prosecution History of the '480 Patent

54. During prosecution, original claims 9-19 were elected in response to a restriction requirement. EX1002, 82, 76. The Examiner rejected original independent claims 9 and 16 as anticipated by O'Toole (EX1012) and Agrafioti (EX1011) but indicated (without explanation) that the pending dependent claims, including original claims 10-12 and 17, were allowable. EX1002, 61-62.

55. In response, applicants canceled the original independent claims and rewrote original claims 10-12 and 17 as independent claims, with the limitations that were originally recited as dependent claims now recited in steps [E]-[F] for each rewritten claim. EX1002, 47-50. This resulted in issued independent claims 1-3 and 7 having shared limitations from the canceled original independent claims, plus differing limitations [E]-[F] from the rewritten dependent claims.

C. The Challenged Claims

56. Independent claim 1 is reproduced below with labels for individual limitations added:

[1PRE]: A method for enabling a wearable device user to access secured electronic systems, said method comprising:

[1A] placing a wearable device in contact with a user, said wearable device including [1A-1] a telecommunications carrier access identification module, [1A-2] a cellular RF communications module, and [1A-3] a short-range RF communications module;
[1B] achieving secured, short-range RF communication between the wearable device and a secured electronic system;
[1C] authenticating the user with at least one of [1C-1] the wearable device, [1C-2] a remote server via cellular communications supported by the telecommunications carrier access identification module and the cellular RF communications module, and [1C-3] the secured electronic system via the secured, short-range RF communication; and
[1D] providing the user with access to or through the secured electronic system once authenticated;
[1E] wherein said wearable device comprises a smartwatch including a microphone and skin illumination and measurement hardware, and
[1F] wherein authentication of the user is based on biometric information obtained from the user via at least one of the microphone and the skin illumination and measurement hardware.

57. Independent claims 2, 3, and 7 include claim 1's steps [PRE] through [D] but recite different requirements for steps [E]-[F]. Steps [2E]-[2F] relate to user location determined by a "GPS module." Steps [3E]-[3F] recite a "registration module." Steps [7E]-[7F] relate to user authentication with a SIM and a cellular communications module.

58. Each dependent claim merely replicates elements from other independent claims. For example, claim 4 depends from claim 2 and adds the biometric authentication limitations of claim 1.

59. I have been asked to provide my opinion concerning whether claims 1-9 of the '480 patent are anticipated or would have been obvious to a POSA in

light of the prior-art references identified in the Petition. For the reasons explained below, it is my opinion that each of claims 1-9 is anticipated and/or would have been obvious to a POSA.

VII. CLAIM INTERPRETATION

60. I understand that determining whether a claimed invention is novel and non-obvious requires comparing the prior art to the claim. I discuss in this Section below the interpretations I have applied to certain claim terms, in accordance with the standards set forth in Section III above.

A. “at least one of”

61. Each challenged claim includes the phrase “at least one of” followed by a list of options joined by the word “and.”

62. I understand that, in the challenged claims, the term “at least one of” has a disjunctive meaning—i.e., the claim is met when one or more of the listed items is present. In other words, the phrase “at least one of” as used in the challenged claims does not require that all listed items be present.

63. Further, I have been informed that “at least one” may be presumed to have a conjunctive meaning *only when* it “precedes a series of categories” that contain multiple possible values. Here, the ’480 patent uses “at least one of” not before a series of categories that can each have multiple values, but rather either before a list of single-valued conditions or options (e.g., “authenticating the user

with at least one of” followed by various optional authentication methods) or to introduce two single-valued items, only one of which is required (e.g., “at least one of the microphone and the skin illumination and measurement hardware”).

Therefore, I understand that this presumption does not apply to the phrase “at least one of” in the challenged claims.

64. Additionally, I understand that such a presumption can be rebutted if the surrounding claim language or the patent’s specification support such a rebuttal. Here, even if there is a presumption that “at least one of” is used conjunctively in the challenged claims, my review of the surrounding claim language and specification rebuts that presumption. *See, e.g.*, EX1001, 6:55-57; 6:64-65; 7:14-16. For example, the ’480 patent expressly refers to these listed items as “conditions.” *See* EX1001, 6:64; 7:15-16.

65. I also understand that Patent Owner interprets “at least one of” in the challenged claims to have a disjunctive meaning parallel district-court litigation. *See* EX1006 at 7. This further supports interpreting “at least one” disjunctively.

66. Accordingly, in my analysis, I interpret and assess the unpatentability of the challenged claims using a disjunctive meaning for the phrase “at least one of”—*i.e.*, the claim is met when one or more of the listed items is present.

B. Other Matters of Claim Interpretation

67. I have been informed that in the parallel District Court litigation, Petitioner has asserted that the step of “authenticating the user” must be performed in the order recited, before the step of “providing the user with access to or through the secured electronic system once authenticated.” EX1023, 4. The opinions as set forth herein do not depend on whether or not it is ultimately determined that the steps must occur in this order, nor do my opinions change if no determination is made on this issue. This is because the prior art renders obvious the claims when the step of “authenticating the user” must be performed before the step of “providing the user with access to or through the secured electronic security system once authenticated.” Accordingly, the claims are obvious whether or not that order is required.

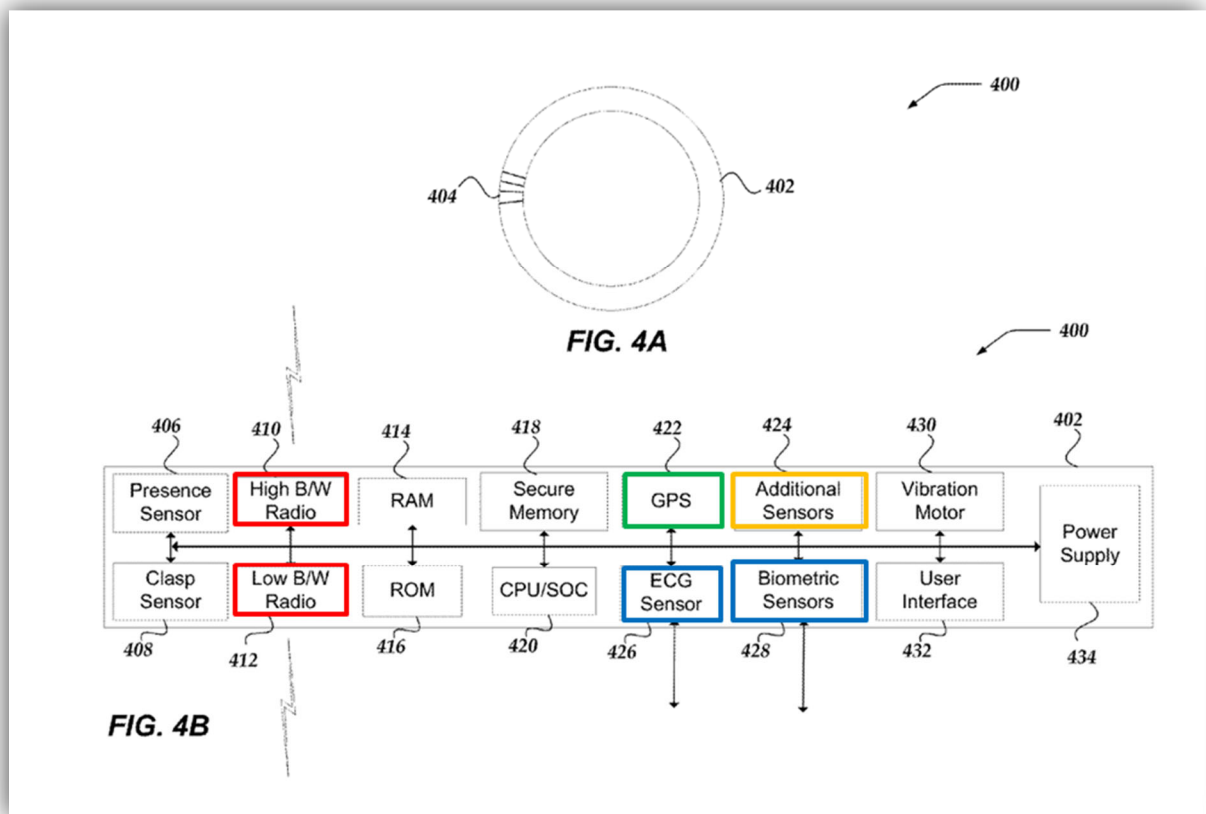
VIII. GROUND 1: CLAIMS 1-5 ARE OBVIOUS OVER AGRAFIOTI ALONE OR WITH BERNEY

A. Agrafioti (EX1011)

68. Agrafioti is directed to a user authentication system that is “centered around a wearable biometric device that authenticates the wearer based on one or more unique biometric characteristics.” [0055]-[0057]; *see id.*, Abstract, [0030]-[0033], [0045]-[0046], [0089]. Agrafioti’s system allows an authenticated user to gain “secure access to other systems and devices at one or more” access points. [0054]. Agrafioti defines an “access point” as “any logical or physical gateway,

device, or application that requires authorization, ...and is otherwise locked or inaccessible to the user.” [0029]-[0030], [0093]-[0096], [0104]-[0107], [0155]-[0171], [0196]-[0198]. Agrafioti’s biometric wearable is “any device that can be worn by a user and is capable of obtaining a biometric signal” such as “a wristband, wristwatch, bracelet, necklace,” etc. Agrafioti, [0044], [0089].

69. An exemplary wristband/bracelet biometric wearable 400 is illustrated in Figures 4A and 4B and includes, among other things, high and low bandwidth radio transceivers, a GPS module, an ECG sensor, other biometric sensors, and optional additional sensors. [0113]-[0123].



Figs. 4A-4B (annotated).

70. Other biometric sensors may include “microphones, near infrared sensors, light sensors, ... photoplethysmogram sensors,” and others, including “optical sensors.” [0122]. Additional sensors 424 include motion sensors, proximity sensors, and GPS sensors. [0109]; Figs. 4A-4B. “These additional sensors may provide one or more contextual signals such as the location of the wearable device and/or proximity to trusted environments.” *Id.*; [0096], [0112], [0121]. The wearable’s sensors may be used to identify a range of “biometric signals and/or data that represent biometric features that may be employed to uniquely identify the user.” [0091]; *id.*, [0028], [0124]. “Non-limiting examples of biometric data that may be employed to uniquely identify a user” include “heart rate, galvanic skin response, ...voice or voiceprint, body electrical characteristic, body thermal characteristic,” as well as “vein pattern” and “photoplethysmogram, electromyogram, [or] electroencephalogram.” [0091]; *id.* [0028]; [0124].

71. The wearable’s “additional sensors” may be used “to obtain additional biometric or environmental readings. Some non-limiting examples of an additional sensor are motion sensor, proximity sensor,” as well as “GPS sensor.” [0109]. “These additional sensors may provide one or more contextual signals such as the location of the wearable device and/or proximity to trusted environments.” *Id.*; *see*

[0096] (discussing use of proximity data); [0112] (discussing tacking or GPS detector activity); [0121] (discussing GPS transceiver).

72. POSAs would have understood that proximity refers to a relative location between two or more objects while “location” refers to absolute location (e.g., latitude and longitude). [0121]. *See* below, Section VIII.E.1.

73. Agrafioti describes multiple ways of user authentication, including by the wearable itself, by an authorized authentication device (“AAD”) that can communicate with the wearable, and/or by a biometric authentication server that can communicate with the wearable and the AAD. [0028], [0033]-[0037], [0057], [0091]-[0093], [0103]. For example, Agrafioti describes user authentication based on biometric data (e.g., pulse, vein pattern) captured by the wearable’s biometric sensors. [0033], [0091] (biometric sensors capture a range of “biometric signals and/or data” that may be used “to uniquely identify the user”), [0124]. Agrafioti also describes creating a “unique biometric profile” that can be stored on the wearable or on the AAD to authenticate a user or pre-authenticate the wearable. [0055], [0095], [0102]-[0103], [0140]-[0153], [0196], Fig. 7.

74. Agrafioti also teaches that wearable biometric “devices may be arranged to employ additional non-biometric security factors,” such as “a password, a Personal Identification Number (PIN), a gesture, a voice command, a finger tap, a distance between the preauthorized biometric device and the at least

[one] access point, [or] one or more additional biometric features of the user.”

[0035]; [0153] (similar).

75. Agrafioti’s Figures 6-15 depict “generalized operations” of certain embodiments. [0131]. In the Figure 12 embodiment, a wearable is “sensed by an access point.” [0196]. At step 1204, if the user is authenticated, the user is granted access to the access point. [0196]-[0198]. In some embodiments, proximity data may be used to unlock an access point when the wearable “is within a specific range” or distance of an access point. Agrafioti, [0096], [0167].

76. Agrafioti’s user authentication techniques are described in greater detail in the limitation-by-limitation analysis below. As discussed below, Agrafioti discloses or renders obvious claims 1-4. Agrafioti Figures 6-12 depict “generalized operations” of its various embodiments. In the Figure 12 embodiment, a biometric wearable is “sensed by an access point.” [0196]. Access points include “any logical or physical gateway, device, or application that requires authorization, ...and is otherwise locked or inaccessible to the user.” [0029]. At step 1204, if the biometric wearable is authenticated, the user may be granted access to the access point. [0196]-[0198].

77. Agrafioti also allows the biometric wearable to be “pre-authenticated.” [0196]; *see* [0140]-[0153] (Fig. 7). In one such embodiment, the biometric wearable captures biometric signals to authenticate the user. [0143].

Then, the biometric data may be transmitted wirelessly to a paired “authorized authentication device” (AAD). [0144]; *see* [0055].

78. The AAD may authenticate the user and authorize the biometric wearable to wirelessly communicate the preauthenticated user identity to other devices and systems,” such as access points. [0055]; *see id.*, [0030], [0034], [0106], [00143]-[0153]. Once preauthorized, the biometric wearable “may stay in the preauthorized mode until it is separated from the user.” Agrafioti, [0140].

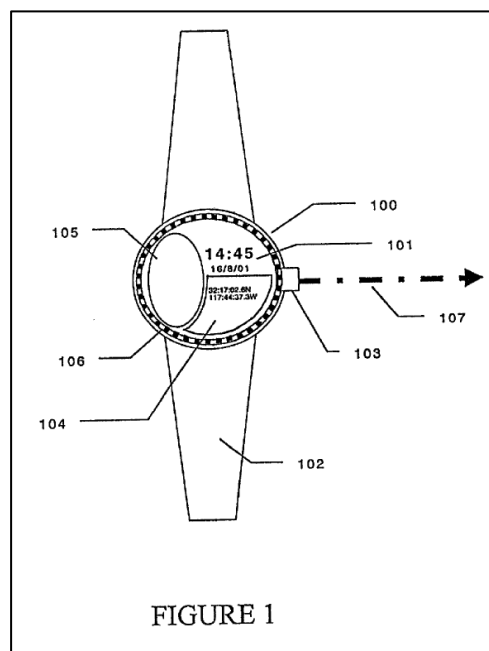
79. Agrafioti’s wearable biometric “devices may be arranged to employ additional non-biometric security factors for preauthorizing an enrolled device,” such as “a password, a Personal Identification Number (PIN), a gesture, a voice command, a finger tap, a distance between the preauthorized biometric device and the at least [one] access point, [or] one or more additional biometric features of the user.” Agrafioti, [0035]; [0153] (similar). In some embodiments, proximity data may be used to unlock an access point when the biometric wearable “is within a specific range,” for example, “a door lock is only unlocked when the authorized user is within a certain distance.” Agrafioti, [0096]; [0167] (“an access point ...grants access to the user when the preauthorized wearable biometric device is detected to be in close proximity”).

80. As discussed below, Agrafioti discloses or renders obvious claims 1-4. To the extent that Agrafioti alone does not render obvious using GPS location

information for authentication purposes, it would have been obvious to do so based on Berney, discussed below in Section VII.C.

B. Berney (EX1008)

81. Like Agrafioti, Berney teaches using a wearable to authenticate user identity and authorize the authenticated user for transactions such as “car parking at a public parking meter” ([0036]), gaining authorized entry to a restrict area ([0037]), and other use cases with “no discernable limit” on the wireless transaction use cases that could be applicable ([0035]). *See* Berney, [0001] Berney’s exemplary wearable is a watch that “provides a biometric data reader” ([0028]-[0029]) and includes “other functional circuitry” such as a GPS receiver ([0039]-[0040]). *See* Berney, [0012]; [0032]. Berney’s Fig. 1 is reproduced below:



82. Like Agrafioti, Berney describes user authentication via the wearable. [0032]. Berney teaches that requiring multiple layers of authentication enhances security, including requiring biometric-based authentication in conjunction with authentication based on location, proximity, or both. Berney, [0034] (noting that “requiring multiple levels” of security provides “virtually ironclad” security for “a single specific user”), [0035]-[0040].

83. For example, Berney describes “a proximity check” enabled by “RF communications such as Bluetooth” ([0038]), where the user is authenticated by the wearable using “the user’s biometric data” *and* by whether the wearable is “worn by the authorized user” and “in suitable proximity to [the] transaction device” ([0041]). Berney further teaches that “very accurate location information” from a GPS receiver can be used as an additional “backup to a proximity indication,” by requiring a wearable’s GPS location to “agree with proximity communications devices in order to authenticate a transaction.” Berney, [0040] (explaining that such a configuration makes “forgery” of the wearable “much more difficult”). POSAs would have understood these disclosures as teaching using a GPS module to obtain the absolute location information of two or more devices and comparing those locations to determine the relative location of the devices, in order to provide “backup” proximity information. Further, POSAs would have known that one way of determining a wearable user’s location with respect to a

device or system (e.g., SES) is by comparing GPS location information of each respective device/system. Berney, [0040]; EX1026, 5:4-14, 6:65-7:2, 10:8-45; 12:31-66; Fig. 5.

C. Combining Agrafioti and Berney

84. Well before the '480 patent's priority date, POSAs would been familiar with multiple authentication methods, including passcodes, passwords, biometric data readings, and location and proximity metrics. Agrafioti, [0003]; Berney, [0002]-[0010], [0028]. Also in this timeframe, POSAs would have understood that using multiple authentication techniques together enhanced security. *See* EX1010, 13:49-14:5; EX1033, 3:4-14, 16:3-14; EX1034.

85. It would have been obvious to POSAs to combine Berney's teachings about using GPS location information with Agrafioti's systems and method. Each reference describes wearables with sensors (including biometric sensors), short-range communication capability, and GPS capabilities. Further, each reference describes user authentication with biometric features and contemplates that location and/or proximity data may be used as an additional security measure before providing the user access to secured (e.g., locked) data or areas. Agrafioti, [0055]-[0057], [0096], [0167]; Berney, [0028]-[0029], [0038]-[0041].

86. Based on Agrafioti's teachings that its wearable biometric devices may "employ *additional non-biometric security factors* for preauthorizing an

enrolled device” (Agrafioti, [0153])¹⁰ coupled with Agrafioti’s description of using proximity data and GPS location ([0096], [0167]), POSAs would have been motivated to require that GPS location information “agree with proximity communications” as taught by Berney ([0040], [0029]). Further, POSAs would have understood that Berney’s location and proximity authentication techniques are alternative options for authentication that are consistent with Agrafioti’s teachings. Berney, [0037]-[0038], [0040]; Agrafioti, [0003]; below Section X.B (discussing corroborating references for multifactor authentication).

87. Additionally, in view of Berney, POSAs would have been motivated to apply Agrafioti’s methods and systems to both Agrafioti’s uses (e.g., unlocking access points) and the types of “wireless transactions” described in Berney (e.g., authorizing “car parking at a public parking meter” ([0036]), “an authorized person seeking entry into a restricted entry area” ([0037])).

88. POSAs would have reasonably expected success in combining Agrafioti and Berney. Both Agrafioti and Berney describe a wearable device with a GPS receiver having similar form factors (e.g., watches) and describe similar platforms (including processors, memory, biometric readers, and antennas).

¹⁰ ***Bold and italics*** emphases herein are added unless otherwise indicated. *Italics* emphases herein are added to indicate challenged claim language.

Agrafioti, Fig. 4B, [089], [0104], [0112]-[0115], [0121]; Berney, Fig. 6, [0029], [0039], [0040]. By the critical date, POSAs would have known how to configure and program Agrafioti's hardware to implement programs using GPS in a wrist-wearable device because implementation of GPS location technology in a wrist-wearable form factor was well understood by POSAs. *See* EX1027, U.S. Patent No. 6,185,157, ("Farine"), Abstract; EX1028, U.S. Patent No. 7,391,677 ("Urano"), 4:61-67; EX1029, 7,889,085 ("Downey"), 1:25-35, 3:61-63. Farine incorporates a GPS receiver into a traditional analog watch to "indicat[e] the direction of a 'target' destination or location from a 'source' location where the GPS receiver is situated" as an aid to navigation. EX1027, 1:7-11. Urano describes improvements to transmission of data needed by a GPS receiver to optimize for use in "small devices such as a wristwatch." EX1028, 10:59-62. Downey describes a watch that couples GPS-based location with location based on motion so that location can be tracked underwater where GPS is unavailable. EX1029, 5:27-6:3. These examples demonstrate that incorporating GPS into wearable devices, and specifically wristwatch-style devices, was well-known by the critical date. Accordingly, a POSA would understand how to implement applications of GPS in a wrist wearable form factor.

D. Claim 1

89. Agrafioti alone or in combination with Berney renders obvious claim 1.

1. [1PRE]: “A method for enabling a wearable device user to access secured electronic systems”

90. Agrafioti discloses methods for authenticating a user of a wearable device before allowing the user to access an “access point.” Agrafioti, [Abstract], [0029]-[0030], [0044], [0054], [0093]-[0096], [0104]-[0107], [0155]-[0171], [0196]-[0198]. Agrafioti’s “access points” are examples of “secured electronic systems” as demonstrated below §VIII.D.3 ([1B]). Thus, to the extent [1PRE] is limiting, Agrafioti satisfies “*a method for enabling a wearable device user to access secured electronic systems.*”

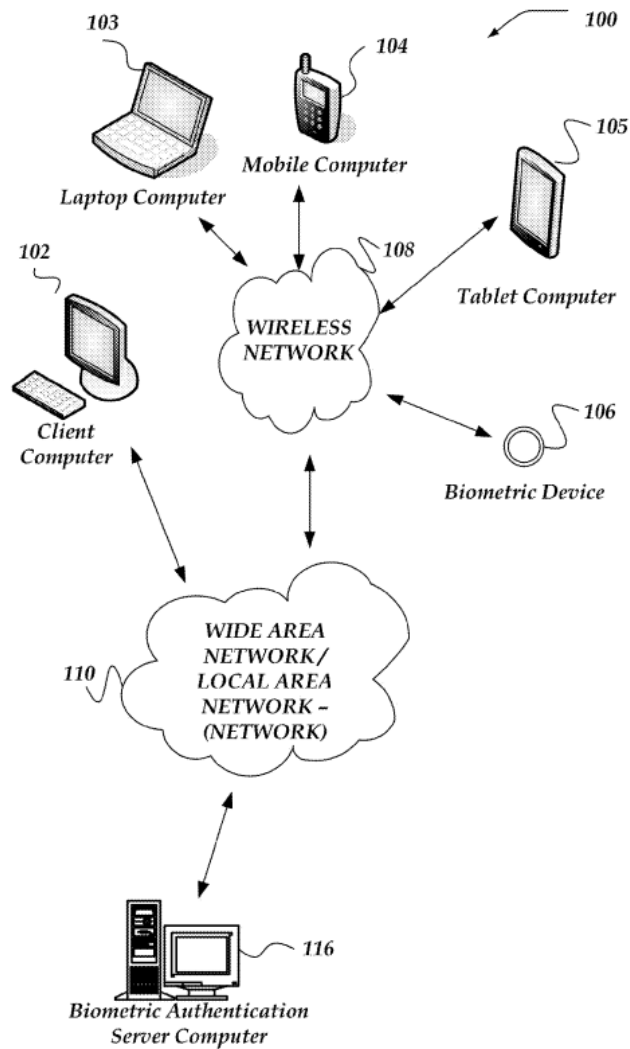
2. [1A] “placing a wearable device in contact with a user”

91. Agrafioti uses biometric wearable devices including is “any device that can be worn by a user and is capable of obtaining a biometric signal,” such as wristbands, wristwatches, bracelets, necklaces, or rings. Agrafioti, [0044], *also* [0089], [0114]-[0115], Fig. 4A-4B. Agrafioti further teaches that that the wearable includes sensors that are in physical contact with the user. *See* Agrafioti, [0124] (“biometric sensor [] may be arranged to include a variety of components for interacting with the wearer”); [0091] (biometric data collected from user); [0099] (wearable’s “electrodes make[] contact with the wrist”), [0107]. Berney also

teaches POSAs that wrist-worn wearables like Agrafioti's are worn in contact with the user. Berney, [0032] (watch sensor). As stated in the '480 Patent, contact includes "placement" on wrist. EX1001, 6:33-36. Thus, Agrafioti's method places the wearable "*in contact with a user*" as claimed.

a. [1A-1] "said wearable device including a telecommunications carrier access identification module"

92. Agrafioti's wearable communicates with client computers 102-105 over a network such as wireless network 108. Agrafioti, [0044]-[0049], [0117]. Agrafioti's Fig. 1 is reproduced below.



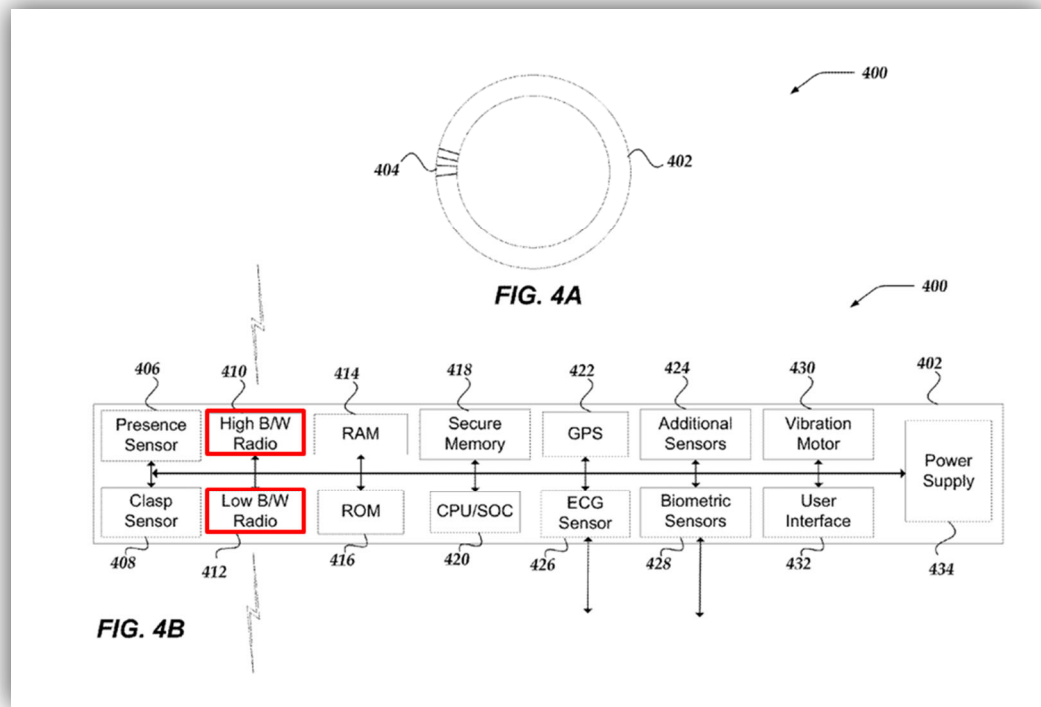
93. “Wireless network 108 may include virtually any wireless communication mechanism by which information may travel between client computers 103-105, *biometric device 106*, and another computer network.” Agraftoti, [0049] (also discussing “cellular” communication such as 2G/3G/4G/5G for network 108).

94. Agraftoti ([0042]) describes using mechanisms implemented by modules within client computers 103-105 (e.g., mobile identification number,

electronic serial number) to “uniquely identify themselves” on network 108. POSAs would have understood that the same mechanisms could beneficially be included in biometric device 106 to uniquely identify itself on the same network. These “uniquely” identifying mechanisms within Agrafioti’s wearable are types of “*telecommunications carrier access identification modules*” as claimed. EX1001, Abstract (“A wearable device can include a telecommunications carrier identification module (e.g., SIM).”), 2:21-34, 4:4-14.

b. [1A-2] “a cellular RF communications module”

95. [1A-2] recites “*a cellular RF communications module*.” “RF communications” means “radio frequency communications.” EX1001, 5:5:33; *see also* EX1041, Merriam-Webster’s Collegiate Dictionary, 1068 (2006) (defining “RF” as “radio frequency”). Agrafioti’s wearable device has “one or more radios or transceivers ...to communicate with other computers or devices.” Agrafioti, [0095], [0105], [0113]-[0115], Figs. 4A-4B.



96. For example, wearable 400 includes high bandwidth radio transceivers 410 that can include “high bandwidth mechanisms such as Wi-Fi, or the like” for “communication with various devices,” including “biometric servers and cloud services.” Agrafioti, [0117]. The transceiver may be coupled to a dipole or other antenna “to facilitate the transmission and reception of wireless signals.” Agrafioti, [0104]. The wearable communicates with biometric servers and cloud services (e.g., server 116) via networks 108 and 110 (see FIG. 1), where network 108 may employ 2G/3G/4G/5G “radio access for cellular systems.” Agrafioti, [0049]. POSAs would thus have understood that the wearable’s high bandwidth radio transceivers 410 alone or coupled with antenna(e) include cellular

communications and, therefore, comprise a “*cellular RF communications module*” as claimed. EX1001, 5:31-37; Agrafioti, [0047]-[0050]; EX1022, 1:9-2:28.

c. [1A-3] “said wearable device including...a short-range RF communications module”

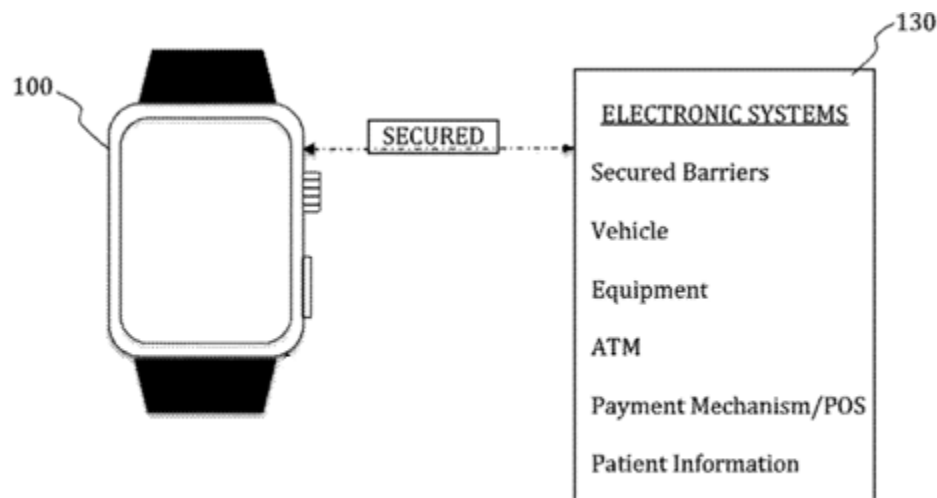
97. Bluetooth communications and near field communication (NFC) are examples of “*short-range RF communications*” as claimed. EX1001, 2:6-10 (“short range radio frequency” communications include “Bluetooth” and “NFC”), 5:22-25, 6:23-24 (similar) 6:41-45 (similar); EX1014, (US 2010/0178866), [0002]-[0003] (“[N]ear field communication covers various *short-range* techniques and technologies which enable wireless communication.”) EX1018, US Patent No. 8,208,867, 1:24-28 (“Electronic devices may use short-range wireless communications links,” such as “the WiFi® (IEEE 802.11) bands at 2.4 GHz and 5 GHz and the Bluetooth® band at 2.4 GHz.”); EX1024, U.S. Patent Publication No. 2010/0178866, [0002]-[0003] (“[N]ear field communication covers various *short-range* techniques and technologies which enable wireless communication.”), [0013] (Bluetooth is a short-range communication technology)).

98. Agrafioti’s biometric wearable includes a low bandwidth radio transceiver 412, which “may represent components for communicating using low-power, shorter range radio systems such as, Blue Tooth, ...NFC, ...the like, or combination[s] thereof.” Agrafioti, [0117], [0002]-[0003], [0030], [0094]-[0096],

[0165]-[0166]. Thus, Agrafioti's wearable includes "*a short-range RF communications module*" (e.g., low bandwidth radio transceiver 412) as claimed.

3. [1B] "achieving secured, short-range RF communication between the wearable device and a secured electronic system"

99. The '480 patent's Figure 2 (excerpt below) illustrates a "secured" connection between wearable device 100 and SESes 130, such as "secured barriers, vehicle, equipment, ATM" and others. *See* EX1001, 5:62-64.



100. Agrafioti discloses the same type of secured, short-range RF communication between a wearable biometric device and "access points." Agrafioti, [0030], [0166] (explaining that explains that the "transmission of entry authorization signals from the preauthorized wearable biometric device to the desired access point ... is preferably accomplished wirelessly," for example, by "Bluetooth, WIFI, NFC, or the like"). For example, the wearable may send a

“control signal...to a physical or logical access point that may enable the user to unlock or access the access point.” “The control signal may be a binary encoded sequence transmitted wired or wirelessly using but not limited to bluetooth, near field communication or Wifi.” Agrafioti, [0030], [0049], [0166], [0196]-[0199]. Agrafioti also describes biometric authentication using the cloud. [0102]-[0103], [0131], [0211-0215].¹¹

101. The ’480 patent “broadly define[s]” an SES “as a system requiring electronic initiation for its operation or to gain access to it.” EX1001, 4:57-59. Agrafioti similarly defines an access point as “any logical or physical gateway, device, or application that requires authorization, such as for security or personalization purposes, and is otherwise locked or inaccessible to the user.” Agrafioti, [0029]. Agrafioti describes non-limiting physical examples of access points including “electronically locked doors” and “parking transceivers” and non-limiting logical examples of access points including “passcode protected electronic devices or accounts” and “proof of payment systems.” *Id.* Agrafioti’s “access points” are thus “*secured electronic systems*” as claimed. EX1001, 2:63-3:3

¹¹ Agrafioti also describes biometric authentication using the cloud. Agrafioti, [0102]-[0103], [0131], [0211-0215].

(examples of SES include secured doors, parking meters, point-of-sale systems and secured databases); Section VIII.D.1 (discussing SES).

102. Additionally or alternatively, POSAs would have been motivated to extend Agrafioti's wearable to apply to the "wireless transactions" described in Berney (e.g., "car parking at a public parking meter" ([0036]), "an authorized person seeking entry to a restricted entry area" ([0037]); and "paying for a store-bought purchase by the use of" a wearable device ([0035])). *See* Section VIII.C (discussing Agrafioti-Berney). All such applications encompass "achieving secured, short-range RF communication between the wearable device" and the types of "secured electronic systems" expressly discussed in the '480 patent. EX1001, 2:60-3:3 ("Examples of secured electronic systems include: ***secured entry barriers*** (e.g., doors, gates, safes),...***payment mechanisms*** (e.g., vending machines, ***parking meters***), ***point-of-sale (POS)***...."). As discussed *supra* in Section VIII.C, POSAs would have been motivated to ensure that Agrafioti's wearable extended to these wireless transactions described in Berney and would have reasonably expected success in doing so. Agrafioti as modified in view of Berney satisfies [1B] for this additional reason.

4. [1C] “authenticating the user with at least one of [1C-1] the wearable device, [and] [1C-2] a remote server via cellular communications”

103. For the same reasons I previously mentioned in Section VII.A, the phrase “at least one of” in [1C] is disjunctive and does not require that all the listed possibilities be satisfied. Therefore, Agrafioti satisfies [1C] because it satisfies both two of the three alternatives—specifically, [1C-1] and [1C-2].

a. [1C-1] “the wearable device”

104. Agrafioti describes “authenticating users *using biometric devices*.” [0032], [0057], [0089]-[0091]. For example, Agrafioti describes using the wearable to acquire biometric data (e.g., fingerprint, voice, pulse, ECG, or vein pattern data captured via sensors) and establish a “unique biometric profile” associated with a user and wearable. Agrafioti, [0028], [0089]-[0091], [0095], [0124]. Agrafioti’s user’s biometric profile may be created “by the wearable itself” ([0103]) and stored on the wearable “to authenticate the user” ([0102], [0124]).

105. For example, Agrafioti teaches that a user “may be authenticated” by the wearable device using the wearable’s biometric sensors. [0091] (biometric sensors capture a range of “biometric signals and/or data” that may be used “to uniquely identify the user”), [0033], [0097], [0124]. “Non-limiting examples” of uniquely identifying biometric data captured by biometric sensors include “heart rate, galvanic skin response,” voice/voiceprint, pulse, and “vein pattern.” Agrafioti,

[0091], [0028], [0124]. Alternatively or additionally, Agrafioti also teaches that authentication can be achieved by the wearable by entering a password or PIN, which is the same type of user authentication by the wearable described in the '480 patent. *Compare* Agrafioti, [0035] *with* EX1001, 3:11-15, 6:58-61.

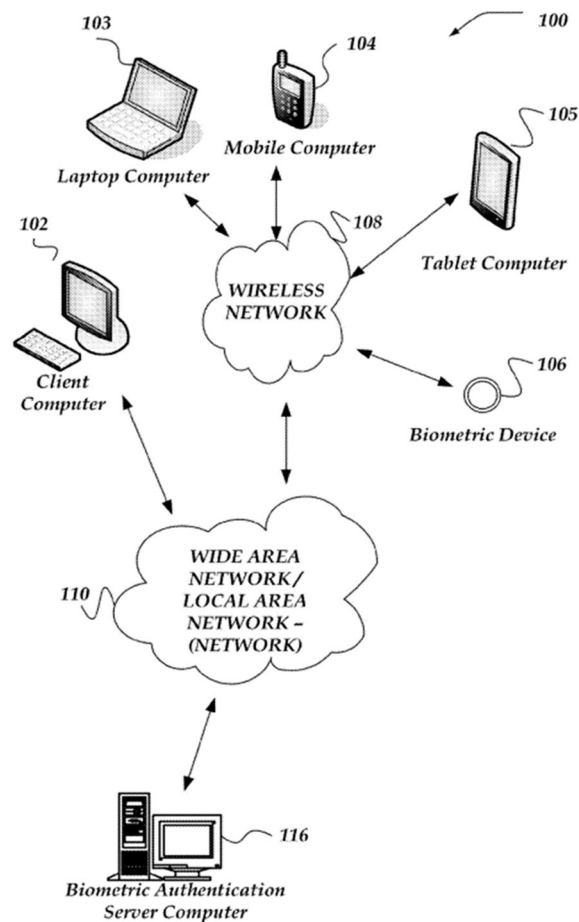
106. Thus, Agrafioti teaches multiple ways of authenticating the user “*with the wearable*” as claimed. Indeed, the '480 patent has the same examples of how to authenticate with the wearable as Agrafioti. *See* EX1001, 3:11-15 (“a user can be authenticated by biometric hardware (e.g., voice, skin illumination) integrated on the smartwatch worn by the user”), 6:58-61 (“Authentication can be accomplished by password entry on the user interface (e.g., touch screen) of the smartwatch or by using the smartwatch to obtain biometric information from the user.”).

b. [1C-2] “a remote server via cellular communications supported by the telecommunications carrier access identification module and the cellular RF communications module”

107. Agrafioti teaches authenticating the user by a remote server in at least two ways: (1) authentication through the “biometric authentication server” (*id.*, [0045]) and (2) authentication through the AAD (Agrafioti, [0033]; [0144]).

i. User Authentication Through Biometric Authentication Server.

108. Agrafioti describes a “remote server,” e.g., biometric authentication server 116, which “may be implemented using one or more cloud instances in one or more cloud networks.” Agrafioti, [0053], [0180], Fig. 1 (excerpt below).



109. The user’s biometric profile may be stored alternatively or additionally in this biometric authentication server. Agrafioti, [0211]. Agrafioti thus describes some embodiments in which the wearable transmits biometric data

acquired by the wearable's sensors to a biometric authentication server 116 for user authentication. Agrafioti, [0044]-[0045], [0052]-[0053].

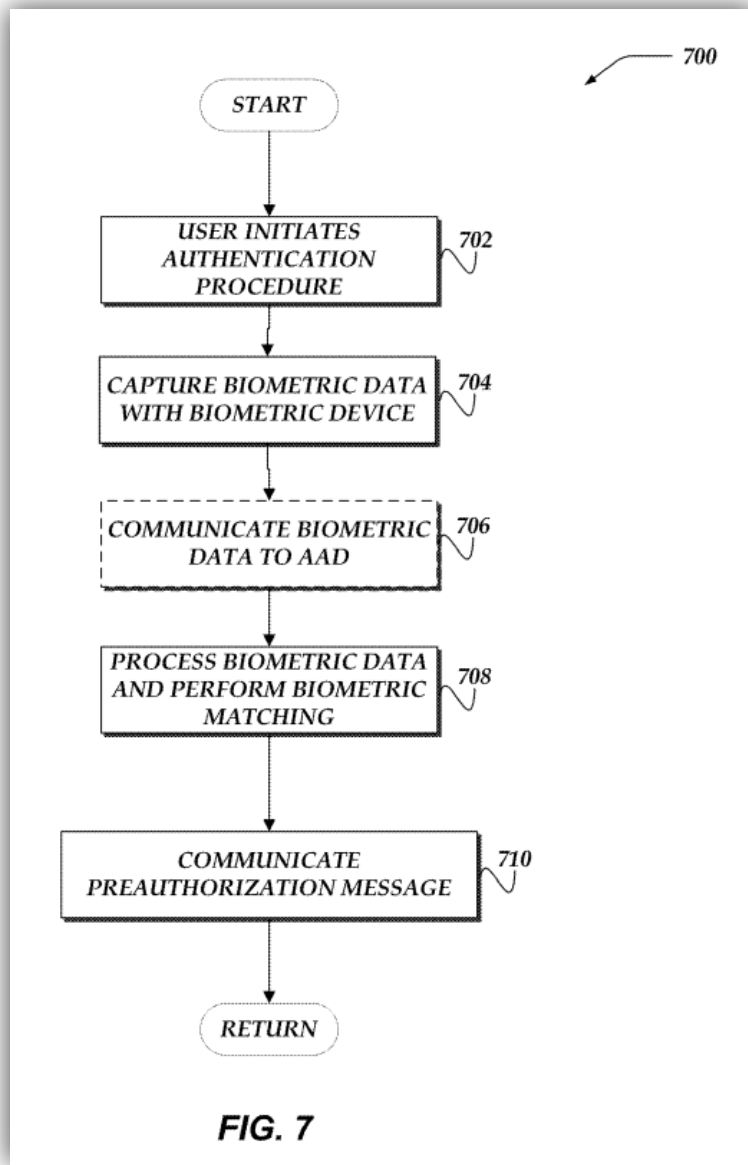
110. Configured user profiles may be stored in the biometric authentication server computer 116, including when it is implemented virtually in a cloud environment. Agrafioti, [0211]. “[E]nabling access for [a] user to access points [may be] based at least on the user profile information for the authenticated users.” Agrafioti, [0037]; [00138].

111. The wearable communicates with biometric authentication server 116 via wireless network 108 and network 110. Agrafioti, [0047]-[0050], Fig. 1. Wireless network 108 includes 2G/3G/4G/5G “radio access for cellular systems” (Agrafioti, [0049]) which is supported by the wearable's modules that meet [1A-1]-[1A-2] as discussed §§VIII.D.2.a-VIII.D.2.b. Thus, authentication by Agrafioti's biometric authentication server computer constitutes authentication by a “*remote server via cellular communications supported by the telecommunications carrier access identification module and the cellular RF communications module*” as claimed.

ii. User Authentication Through the AAD.

112. In another embodiment (e.g., Figure 7), the user's biometric profile is stored on an AAD that “may be separate from the biometric” wearable. Agrafioti, [0033], [0100]-[0103], [0132]-[0135], [0137]-[0138]. In this embodiment, the

wearable transmits biometric feature(s) captured by the wearable to an AAD that performs the user authentication. Agrafioti, [0142]-[0150]. Agrafioti's Figure 7 is reproduced below:



113. Specifically, the AAD compares the received biometric features to the stored biometric profile “that corresponds to the user.” Agrafioti, [0033], [0037], [0138], [0142]-[0150], [0219]; Fig. 7.

114. If the features received by the AAD correspond to a stored biometric profile for the user, then the wearable biometric “may be preauthorized for the user.” Agrafioti, [0033], [0037], [0138], [0142]-[0150], [0219]. This process “authenticates the identity of the user and authorizes the wearable biometric device to wirelessly communicate the preauthenticated user identity to other devices and systems,” including access points. Agrafioti, [0055], [0146]-[0149], [0152], [0160]-[0162].

115. The wearable communicates with the AAD via “radios/transducers,” and the AAD may be one of client computers 103-105 with which the wearable communications over network 108 (including cellular communications supported by the wearables modules that meet [1A-1] to [1A-2] as discussed *supra*, Sections VIII.D.2.a-VIII.D.2.b. Agrafioti, [0093], [0039]. POSAs would this have understood that the corresponding authentication occurs by “*a remote server via cellular communications supported by the telecommunications carrier access identification module and the cellular RF communications module*” as claimed. See VIII.D.2 ([1A]). POSAs would therefore have understood that the corresponding authentication satisfies [1C-2].

5. [1D] “providing the user with access to or through the secured electronic system once authenticated”

116. Agrafioti describes granting the user access to an “access point” (i.e., the SES as claimed) after authenticating the user. Agrafioti, [0107], [0148], [0154]-[0163], Fig. 8 (showing authorization followed by enabling user access to one or more access points). Thus, Agrafioti’s method provides the user with access to the SES “*once authenticated*,” as claimed. Indeed, Agrafioti’s descriptions of granting access to an “access point” is highly similar to the sequence described in the ’480 patent in which “a smartwatch is placed in contact with a user’s wrist,” “[t]he smartwatch then authenticates the user,” “[t]he smartwatch then establishes communication with a secured electronic system,” and, finally, “the user can be granted access to [the] secured electronic system.” ’480 patent, 6:46-7:2. Agrafioti performs the same sequence. For example, Agrafioti’s Fig. 8 shows a “process [] for authenticating a user” in which, at block 802, the process asks whether the “biometric device [is] preauthorized?” Fig. 8. If the biometric device is preauthorized (and in range), the process asks “if one or more additional conditions (if any) are met. Agrafioti, [0155]. If these conditions are met, “*access* to one or more access points *may be enabled* for the user that has the biometric device.” Agrafioti, [0160] (emphasis added).

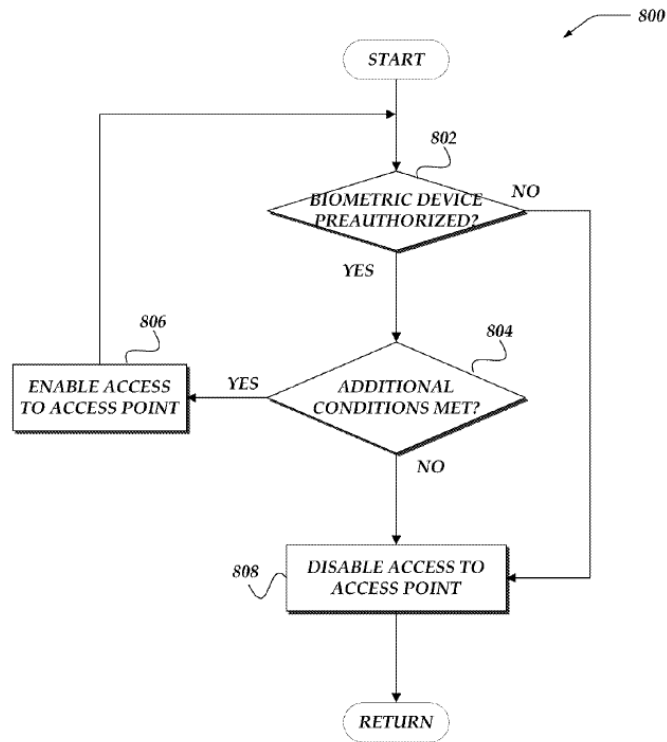


FIG. 8

117. Similarly, Agrafioti explains that “one method of gaining entry at an access point” includes determining “whether a wearable biometric device has been preauthorized and if that wearable biometric device is within an allowable range of the access point.” If the answer is yes for both, then the biometric wearable “may be arranged to transmit a control signal to the access point that affirmatively confirms that the biometric device is preauthorized. Accordingly, the user may *obtain access* to the access point.” Agrafioti, [0161] (emphasis added).

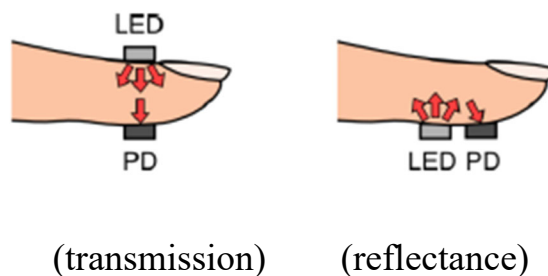
6. [1E] “wherein said wearable device comprises a smartwatch including a microphone and skin illumination and measurement hardware”

118. Agrafioti describes a “wristwatch” wearable ([0044]) and teaches that the wearable includes a microphone and can recognize voice commands ([0035], [0105]-[0109], [0122]), may include high and low frequency radio transceivers, GPS and other sensors, and can send and receive signals including cellular signals (e.g., via network 108) ([0038], [0044]-[0050], [0092]-[0097]). *See* section VIII.A. POSAs would have understood that a wristwatch wearable as described in Agrafioti is a “smartwatch” including a microphone as claimed. Indeed, Agrafioti’s biometric wearable can recognize “voice command[s]” ([0035]) and use “voice of voiceprint” as a biometric signal” ([0028]). Agrafioti biometric wearable may also include “near infrared sensors [or] light sensors.” [0122], [0109].

119. Agrafioti teaches that the wristwatch wearable may include “photoplethysmogram sensors” and discusses near infrared sensors, light sensors, and optical sensors. Agrafioti, [0122]. Agrafioti also states that its biometric wearable may include pulse detection ([0108], [0116]) or vein pattern recognition ([0028]). POSAs would have understood that photoplethysmogram (“PPG”) sensors, infrared sensors, light sensors, and optical sensors are types of “skin illumination measurement” sensors—i.e., skin illumination measurement

hardware—because they emit light (or other optical output) and measure a response to that light (or other optical output).

120. Agraftoti also teaches that the biometric wearable device (e.g., smart wristwatch) may perform biometric authentication via pulse detection ([0108], [0116]). POSAs would have understood that PPG was a common and conventional implementation of pulse detection at that time typically involved emitting infrared, red, or green-light from a light source and measuring the light’s reflection, transmission, or variation with a sensor (e.g., a photodetector). *See* EX1030, 283-84 (describing PPG pulse sensing using “reflection from or transmission through the tissue” of the user from red, infrared, or green light sources). For example, Tamura compares reflection to transmission in Fig. 2, reproduced below:



121. EX1030, 285 (annotated); *also* EX1031, (PPG pulse monitoring using “a light source to illuminate the skin tissue, and a photodetector to measure small variations in light intensity”); EX1009, [0026]-[0030]; EX1021, US Patent No. 6,178,343, 1:8-56 (pulse oximeters used two light sources passed through user’s

skin to determine pulse rate); EX1019, US Publication No. 20020188210, [0005] (pulse rate detector including LED (light emitting diode) and photodetector...to measure heart rate from frequency of pulse waves from reflected or transmitted light); EX1020, US Patent No. 8,781,569, 7:13-28 (light-based pulse sensor), EX1021, U.S. Patent No. 6,178,343, 1:8-56.

122. Thus, POSAs would have understood that a conventional and obvious implementation of Agrafioti's described pulse detection would include a light source and a measurement sensor (such as the optical or infrared sensors disclosed by Agrafioti). Further, POSAs would have understood that a biometric wearable device (e.g., smart wristwatch) that includes a pulse detection light source and measurement sensor has "*skin illumination and measurement hardware*" as claimed.

7. [1F] "and wherein authentication of the user is based on biometric information obtained from the user via at least one of the microphone and the skin illumination and measurement hardware"

123. As discussed above in sections VIII.D.4 (1[C]), and VIII.A, Agrafioti describes biometric user authentication which may be performed by the wearable device, by a remote authentication server, or by an AAD. In any implementation, the biometric user authentication may be based on voice/voiceprint or pulse detection. Agrafioti, [0028], [0091], [0124], [0140], [0153]. POSAs would have understood from Agrafioti and their knowledge and experience that

voice/voiceprint biometric authentication includes acquiring biometric information (the user's voice) from a microphone, which Agrafioti discloses on the wearable (*see* §VIII.A). Additionally, for the reasons discussed Section VIII.D.6 (1[E]), POSAs would have understood from Agrafioti and their knowledge and experience that pulse detection biometric authentication includes acquiring biometric information (the user's pulse patterns) from the skin illumination and measurement hardware (e.g., PPG-related sensors). Thus, Agrafioti satisfies [1F].

E. Claim 2

124. [2PRE]-[2D] are identical to [1PRE]-[1D]. Agrafioti alone or in combination with Berney satisfies [2PRE]-[2D] for the discussed Section VIII.D.1-VIII.D.5.

1. Location

125. [2E] recites “*said wearable device includes a GPS module for determining location of the wearable device user with respect to the secured electronic system*” and [2F] recites “*the step of providing a user access to or through the secured electronic systems is also dependent on the location of the wearable device user.*”

126. Before addressing these limitations, I will briefly address how a POSA would have understood the concept of location, with respect to absolute location and relative location (or proximity). POSAs would have understood that

proximity refers to a relative location between two or more objects while “location” refers to absolute location (e.g., latitude and longitude). Agrafioti, [0121]. For example, an absolute location could be a set of coordinates made up of a latitude and longitude, or a street address, typically associated with a standardized reference system. In the case of latitude and longitude this reference system typically is the World Geodetic System 1984 (WGS 84) system. For a street address in the United States, it typically uses a grid system, assigned by city or county planning departments or municipal governments, and/or in coordination with state reference systems and/or the U.S. Postal Address system (particularly for rural addresses).

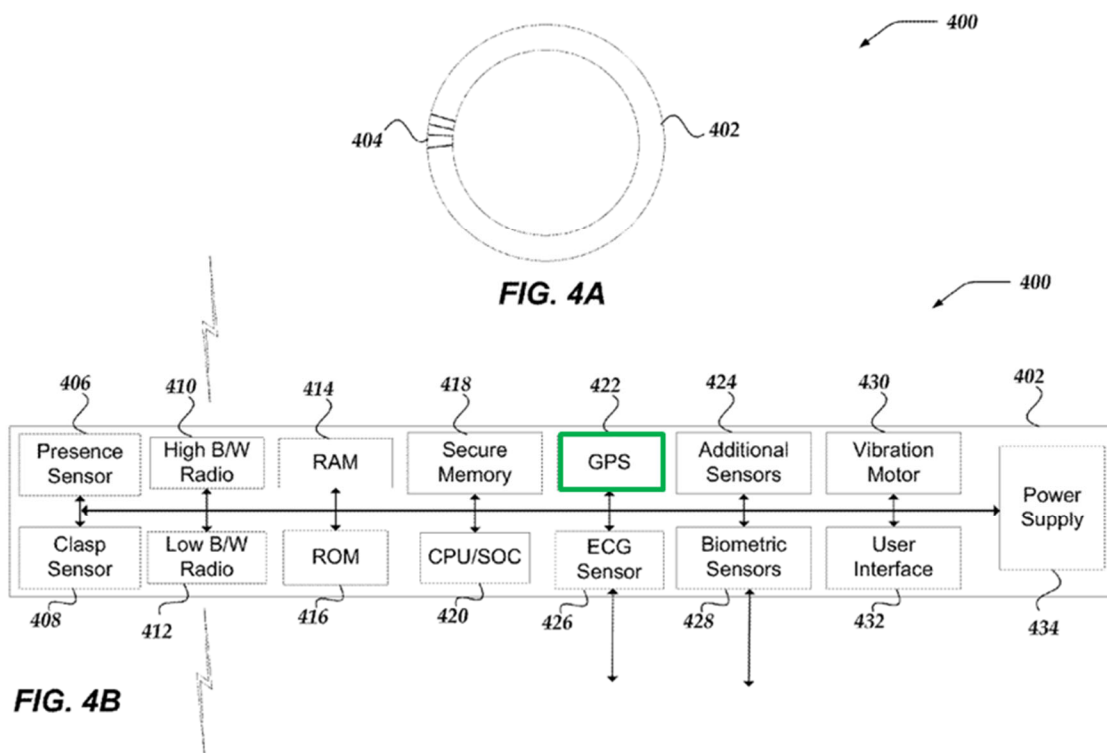
127. In contrast, a proximity location is defined by its “nearness” to (e.g. in reference to) another person, place or thing. It does not require linkages to an underlying reference system; rather, its “reference system” is on a case-by-case basis, e.g. where (or, how close to) one person’s device is to another person’s device. In relative location, an absolute location is not necessary. Indeed, a person can determine if they are in proximity to another without having any idea where they are in absolute location terms (I’m standing by the big tree to your left. I am 10 meters straight ahead of you).

128. Finally, while proximity can be determined without absolute locations (such as via GPS), proximity can be determined using two sets of absolute location

coordinates, e.g. determining the coordinates of two devices, calculating the distance between the devices, and comparing that distance to a value that defines proximity (e.g. less than or equal to X = proximity, greater than X = not in proximity). This kind of technique could serve as a backup to more “direct” forms of proximity determination (e.g. are the two devices within range of each other or not). It can also enable use cases where “proximity” is a large distance, e.g. within the same city – use cases not possible using short-range communications.

2. [2E]: “said wearable device includes a GPS module for determining location of the wearable device user with respect to the secured electronic system”

129. Agrafioti’s biometric wearable includes a GPS transceiver 422, which “may represent the radios, hardware, and instructions (e.g., software) for receiving geo-location.” Agrafioti, [0121],[0109], [0112]-[0115].



130. “GPS transceiver 422 may determine the physical coordinates of biometric device 402 on the surface of the Earth” and “typically outputs a location as latitude and longitude values.” [0121]. Under some conditions, “GPS transceiver 422 may determine a physical location within millimeters for biometric device 402.” *Id.* Agrafioti thus discloses “a GPS module for determining the location of the wearable device” as claimed.

131. To the extent Agrafioti does not expressly teach “*determining location of the wearable device user with respect to the [SES],*” it would have been obvious to configure Agrafioti’s biometric wearable to do so in view of Agrafioti alone or in combination with Berney in the manner discussed Section VIII.C.

132. Determining the location of the wearable device user with respect to the SES is a relative location determination—i.e., a type of proximity information. Both Agrafioti and Berney describe using proximity information for accessing an SES or as part of authenticating a user. Agrafioti teaches that “access control may be further conditioned by requiring ...*determination of proximity/range of the wearable biometric device to the access point.*” [0167], [0095]-[0096] (“only unlocking a device when the proximity is within a specified range”), [0106], [0112], [0169], [0187], [0194]. Similarly, Berney teaches that proximity information may be considered together with a GPS receiver’s very accurate location information and may be required to agree with each other in order to authenticate the user.

133. Thus, it would have been obvious to POSAs in view of Agrafioti alone and/or Berney’s teachings to use Agrafioti’s GPS transceiver 422 to “determin[e] location of the wearable device user *with respect to the [SES]*” as claimed. Agrafioti, [0112].

3. [2F] “the step of providing a user access to or through the secured electronic systems is also dependent on the location of the wearable device user”

134. Agrafioti teaches that the wearable provides “access control” based on “*determination of proximity/range of the wearable biometric device to the access point.*” Agrafioti, [0167], [0095]-[0096], [0106], [0112], [0169], [0187], [0194].

For example, “to access a smartphone, the wearable biometric device may transmit a control signal to the smartphone indicating that the wearable biometric device is preauthorized, and is also *within proximity to the device or system to be unlocked or accessed.*” Agrafioti, [0169][0095]-[0096] (“only unlocking a device when the proximity is within a specified range”), [0106], [0112]. Agrafioti thus discloses “*providing a user access to or through the [SES] dependent on the location of the wearable device user,*” because the user wearing the wearable must be located close to the access point in order to gain access.

135. To the extent that [2F] requires that “the location of the wearable device” be an absolute location (e.g., determined by the GPS module), this step would have been obvious to POSAs for the reasons discussed in Sections VIII.C and VIII.E.3 ([2E]), and Agrafioti’s teachings that access control is based on the proximity of the wearable to an access point. For example, it would have been obvious to POSAs to configure Agrafioti in view of Berney such that access to the SES granted only when the wearable’s GPS location indicates that the wearable is in a particular location (and additionally close to the access point).

F. Claim 3

1. [3PRE] – [3D]

136. [3PRE]-[3D] are identical to [1PRE]-[1D]. Agrafioti alone or in combination with Berney satisfies [3PRE]-[3D] for the reasons discussed Sections VIII.D.1-VIII.D.5.

2. [3E] “said wearable device further comprises a registration module”

137. The ’480 patents states that the registration module (a.k.a “electronic system registration module”) is “for registering secured electronic devices.”

EX1001, 4:12-13, Abstract (“A registration module can register secure electronic systems, authenticate a wearable device user, and grant the wearable device user with access to secured electronic systems.”); 6:1-6 (similar). Using a registration module, an SES may be registered with the wearable. “[R]egistration of [an SES] is different from merely setting up a Bluetooth connection.” EX1001, 6:2-28.

138. Agrafioti explains that access point (i.e., SES) “permission information may be communicated to the biometric device “in the form of a list of” restricted or accessible (or both) access points. Agrafioti, [0174], [0034], [0179]. Agrafioti’s list of accessible/r inaccessible) access points is the type of “*registration module*” claimed at least because the wearable receives the information and “registers” the access points by listing them with accessible/inaccessible status. Agrafioti, [0174].

3. [3F]: “providing a user access to or through the secured electronic system is determined by at least one of the wearable device and the registration module based on at least one of: [3F-1] the user authenticated for access to secured electronic system by the wearable device, ... [3F-4] the user granted access based on location, and [3F-5] the user granted access based on proximity to a secured electronic system”

139. [3F] recites that “*providing a user access to or through the secured electronic system is determined by at least one of the **wearable device** and the registration module based on at least one of*” five authentication options. In the first place, the alternative language of limitation 3F means that the access may be provided by the wearable device, the registration module, or both. *See* Section VII.A (discussing disjunctive interpretation of “at least one of”). Agrafioti satisfies “providing a user access to or through the secured electronic system” at least by the wearable for the reasons discussed in Section VIII.D.5.

140. Agrafioti satisfies [3F-1] (“the user authenticated for access to secured electronic system by the wearable device”) for substantially the same reasons as [1C-1] (“authenticating the user with ...the wearable device”). *See* Section VIII.D.4.a. Agrafioti also renders obvious at least “[3F-3] the user biometrically authenticated for access by remote server” (Section VIII.D.4.b); “[3F-4] the user granted access based on location” (Sections VIII.E.2-VIII.E.3); and “[3F-5] the user granted access based on proximity to a secured electronic system” (Sections VIII.E.2-VIII.E.3).

- G. Claim 4 [PRE] The method of claim 2, [A] wherein said wearable device further comprises a smartwatch including a microphone and skin illumination and measurement hardware, [B] wherein authentication of the user is based on biometric information obtained from the user via at least one of the microphone and the skin illumination and measurement hardware.**

141. Claim 4 depends from claim 2 and recites the identical requirements of [1E]-[1F]. Thus, Agrafioti alone or in combination with Berney satisfies claim 4 for the reasons discussed §§ VIII.D.6-VIII.D.7.

- H. Claim 5 [PRE] The method of claim 1, [A] wherein said wearable device further comprises a GPS module for determining location of the wearable device user with respect to secured electronic systems, and [B] wherein access to the secured electronic systems is dependent on the location of the wearable device user in relationship to the secured electronic systems.**

142. Claim 5 depends from claim 1 and recites the identical requirements of [2E] and nearly-identical requirements of [2F]. Thus, Agrafioti alone or combined with Berney satisfies claim 5 for substantially the same reasons discussed Sections VIII.E.2-VIII.E.3. Claim 5 differs from [2F] by further reciting the clause “in relationship to the secured electronic systems.” Agrafioti combined with Berney satisfies this requirement at least because the combination discussed §§VIII.B-VIII.C requires that “accurate location information” from a GPS receiver “agree with proximity communications devices to order to authenticate a

transaction” (Berney, [0040]), which is “*location ... in relationship to the [SEses]*” as claimed.

- I. Claim 6 [PRE] The method of claim 3, [A] wherein said wearable device further comprises a smartwatch including a microphone and skin illumination and measurement hardware, [B] wherein authentication of the user is based on biometric information obtained from the user via at least one of the microphone and the skin illumination and measurement hardware.**

143. Claim 6 depends from claim 3 and recites the identical requirements of [1E] and [1F]. Agrafioti alone or combined with Berney satisfies claim 6 for substantially the same reasons discussed supra §§VIII.D.6-VIII.D.7.

IX. GROUND 2: CLAIMS 1-9 ARE OBVIOUS OVER AGRAFIOTI, BERNEY, AND LEE

A. Lee (EX1009)

144. Lee describes a wrist wearable such as a watch with contact sensors “for authenticating a user based on a wrist vein pattern.” Lee, [0003]. Wrist contact sensor have an array of illuminators and sensors on a surface of the wrist device that is opposite the user’s wrist when the device is worn by the user. Lee, [0031]. “The illuminators [] produce illumination in the infrared spectrum which directed into the skin of the palmar side of the wrist.” Lee, [0031]; [0036]. The wrist contact sensor obtains “digital data representing the wrist vein pattern for the user.” Lee, [0003]. The user’s wrist vein pattern is compared to stored wrist vein pattern information to authenticate the user. Lee, [0005], [0070] (“The

authentication software ...compares the digital data presenting the wrist vein pattern with digital data representing one or more reference wrist vein patterns.”). The digital data may be encrypted and transferred for authentication of the user. Lee, [0055]. The authentication may be used for “security of computer access and data stored by a computer system” and may also be used for continuous authentication “in military or other environments requiring high securing or monitoring of activity over time.” Lee, [0026].

B. It Would Have Been Obvious to Combine Agrafioti, Berney, and Lee

145. Agrafioti explains that “a user of [its] wearable biometric device may be authenticated with one or more biometric technologies or sensors that may capture biometric signals” ([0091]) such as vein patterns ([0028]). Agrafioti, [0124]. Agrafioti explains that vein patterns are one of the “examples of biometric signals” that “can be obtained from a user that can uniquely identify the user.” Agrafioti, [0028]; *also* [0091]; [0124] (user may provide vein pattern data). To the extent that Agrafioti does not expressly disclose how to obtain such “vein patterns,” POSAs would have been motivated to use an array of illuminators and sensors on a surface opposite a section of a user’s wrist as taught by Lee (Lee, [0031], [0036]) to obtain “digital data representing the wrist vein pattern for the user” (Lee, [0003], [0005], [0070]).

146. POSAs would have had such motivation to implement Agrafioti's wearable itself and/or as modified in view of Berney (as discussed Section VIII.C) to obtain vein patterns based on Lee's teachings. Both options are collectively discussed herein as "Agrafioti-Berney-Lee." POSAs would have reasonably expected success in incorporating Lee's array of illuminators into Agrafioti-Berney-Lee at least because Agrafioti, Berney, and Lee all describe a wearable device having similar form factors (e.g., watches) and describe similar platforms (processors, memory, biometric readers, and antennas). Agrafioti, Fig. 4B, [089], [0104], [0112]-[0115], [0121]; Berney, [0028]-[0029], [0032], claim 2; Lee, [0005], [0070].

C. Claims 1-6

147. To the extent that Agrafioti alone or combined with Berney does not satisfy the "skin illumination" claim requirements of claim 1-6 (i.e., elements [1E]-[1F], [4A]-[4B], [6A]-[6B]), Agrafioti-Berney-Lee satisfies those limitations as set forth below. Agrafioti-Berney-Lee satisfies the other limitations of claims 1- 6 for the same reasons set forth Section VIII.

1. [1E] (“wherein said wearable device comprises a smartwatch including a microphone and skin illumination and measurement hardware” / [4A] (“wherein said wearable device further comprises a smartwatch including a microphone and skin illumination and measurement hardware”) / [6A] (“wherein said wearable device further comprises a smartwatch including a microphone and skin illumination and measurement hardware”))

148. Agrafioti-Berney-Lee renders obvious a “wearable device compris[ing] a smartwatch including a microphone and skin illumination and measurement hardware.” Agrafioti-Berney-Lee includes Agrafioti’s watch wearable biometric device, which is a smartwatch that includes a microphone as discussed Sections VIII.A and VIII.D.6. Agrafioti, [0044], [0089], [0099].

149. Agrafioti-Berney-Lee’s biometric authentication may include measuring vein pattern data as taught by Agrafioti and described in detail in Lee. EX1011, [0028], [0091], [0124]; EX1009, [0003]-[0008], [0054]-[0064], [0070]-[0072]; §IX.A-IX.B. Agrafioti-Berney-Lee’s array of illuminators and sensors comprise “*skin illumination and measurement hardware*,” as claimed. Lee, [0030]-[0031], [0058].

2. **[1F] (“wherein authentication of the user is based on biometric information obtained from the user via at least one of the microphone and the skin illumination and measurement hardware”) / [4B] (“wherein authentication of the user is based on biometric information obtained from the user via at least one of the microphone and the skin illumination and measurement hardware”) / [6B] (“wherein authentication of the user is based on biometric information obtained from the user via at least one of the microphone and the skin illumination and measurement hardware”)**

150. Agrafioti-Berney-Lee satisfies [1F]/[4B]/[6B] for the reasons discussed Section VIII.

151. Agrafioti-Berney-Lee additionally implements Lee’s teaching that its array of illuminators is illuminated (e.g., one at a time) to illuminate skin of the wrist proximate the illuminators. Lee, [0036]-[0037]. Lee’s wearable uses data from its sensors to generate reference user wrist vein pattern data and then authenticates users by matching the sensed wrist vein data to the reference data using pattern recognition signal processing software. Lee, [0038], [0058]. When the user’s wrist matches the reference wrist vein pattern, a user identity is “communicated to ... applications [] requesting user authentication.” Lee, [0059]. Thus, Agrafioti-Berney-Lee satisfies [1F]. Thus, based on Lee, POSAs would have configured the Agrafioti-Berney-Lee wearable to generate a user’s biometric profile based on wrist vein pattern data. Agrafioti, [0028], [0091], [0124]; Lee, [0038], [0058]. Agrafioti-Berney-Lee would be configured to authenticate users by matching the sensed wrist vein pattern data to the biometric profile wrist vein

pattern data. Lee, [0038], [0058]-[0059]; Agrafioti, [0124] (biometric data include vein pattern). Agrafioti-Berney-Lee thus satisfies authenticating the user “*based on biometric information obtained from the user via ...the skin illumination and measurement hardware*” for these additional reasons. Thus, Agrafioti-Berney-Lee satisfies [1F], [4B], and [6B].

D. Claim 7

1. [7PRE] “A method for enabling a smartwatch user to access secured electronic systems”

152. Claim 7’s preamble differs from claim 1’s preamble only in that claim 7 refers to “a smartwatch user.” To the extent [7PRE] is limiting, Agrafioti-Berney-Lee renders obvious [7PRE] for the same reasons Agrafioti satisfies [1PRE] (*see* Section VIII.D.1) and because POSAs would understand that Agrafioti discloses a smartwatch (*see* Section VIII.D.6 ([1E])).

2. [7A] “placing a smartwatch in contact with a user, the smartwatch including a registration module, a short-range RF communications module, a microphone, and skin illumination and measurement hardware”

153. Agrafioti-Berney-Lee discloses placing a wearable device in contact with a user (*see* Section VIII.D.2 ([1A])) and the wearable device may be a smartwatch (*see* previous section). Agrafioti discloses that its wearable device may include: [1] a registration module and [2] a short-range RF communications module and [3] a microphone (Agrafioti, [0109]). §§VIII.F.2 ([3E]), VIII.D.2.c

([1A-3]). Finally, including [4] skin illumination and measurement hardware was obvious as discussed in Section VIII.D.6 ([1E]).

3. **[7B]-[7D] “achieving secured, short-range RF communication between the smartwatch and a secured electronic system”; [7C] “authenticating the user with at least one of the smartwatch and the secured electronic system using at least one biometric obtained from at least one of the microphone and the skin illumination and measurement hardware”; [7D] “providing the user with access to or through the secured electronic system once authenticated”**

154. Agrafioti-Berney-Lee renders obvious [7B], [7C], and [7D] for the reasons discussed in Sections VIII.D.3, VIII.D.4, VIII.D.5, and VIII.D.7, respectively.

4. **[7E] “a subscriber identification module (SIM) and a cellular communications module, wherein authentication of the user is also achievable by accessing a remote server via cellular communications supported by the SIM and the cellular communications module and matching the at least one biometric”**

155. Limitation [7E] recites “a subscriber identification module (SIM) and a cellular communications module...” The limitation is indefinite because [7E] recites an apparatus when claim 7 is a method claim. It is also obvious over Agrafioti-Berney-Lee.

156. Agrafioti discloses that its biometric device may communicate via cellular communication. See §§VIII.D.2.a-VIII.D.2.b ([1A-1]-[1A-2]); Agrafioti, [0047], [0049]. A POSA would understand that including a SIM was well-known

means for identifying the device to permit a cellular wireless connection. Indeed, the '480 patent admits that smartwatches incorporating SIMs were known in the prior art. '480 patent, 1:43-47. Other prior art confirms this. *See, e.g.*, EX1032, U.S. Patent No. 8,851,372 (describing wearable personal digital device which may be a watch (10:32-33) and may include a SIM (8:16-17)).

157. The biometric data may be transferred via a secure wireless connection. Agrafioti, [0047]-[0049]. Thus, Agrafioti-Berney-Lee satisfies matching the biometric data sensed by the wearable device by accessing a remote server via the cellular communications.

E. Claim 8

1. **[8A] “wherein the smartwatch wearable device includes a GPS module for determining location of the smartwatch user with respect to the secured electronic system”;
[8B] “wherein the step of providing a user access to or through the secured electronic systems is also dependent on a location of the smartwatch user with respect to a location of the secured electronic system”**

158. Claim 8 depends from claim 7 and recites substantively the same requirements of claim 5 except that claim 8 specifically recites a smartwatch. As discussed in section VIII.A, Agrafioti's wearable may be a smartwatch. Agrafioti-Berney-Lee satisfies claim 8 for the same reasons that Agrafioti-Berney satisfies claim 5. *See* section VIII.H.

- F. Claim 9 “The method of claim 8, wherein providing a user access to or through the secured electronic system is determined by the registration module based on at least one of: [1] user authentication for access to secured electronic system by smartwatch, [2] user biometric authentication by a wireless carrier, [3] user biometric authentication by remote server, [4] user location, and [5] user proximity to a secured electronic system.”**

159. Agrafioti-Berney-Lee renders obvious at least “*providing a user access to or through the secured electronic system [] determined by the registration module based on ...[1] user authentication for access to secured electronic system by smartwatch,*” for the reasons discussed in Sections VIII.D.4, VIII.F.3.

X. GROUND 3: CLAIMS 2, 5, 8 ARE OBVIOUS OVER AGRAFIOTI-

A. Jun (EX1010)

160. I understand that Jun qualifies as prior art pursuant to §102(a)(2) because it (1) meets the “ministerial requirements for claiming priority to” an earlier application (EX1039, Korean Patent Application 10-2015-0068739 (“Jun-739”), filed May 18, 2015); and (2) the earlier application describes the same subject matter from Jun that Petitioner relies upon.

161. Jun describes a wearable (*e.g.*, smartwatch) that can transmit short-range RF signals to unlock a target object (*e.g.*, vehicle) as shown in Figure 9, reproduced below. Jun, Abstract, 4:65-5:5; 6:65-7:9; 8:20-56; 11:53-57; 13:49-57.

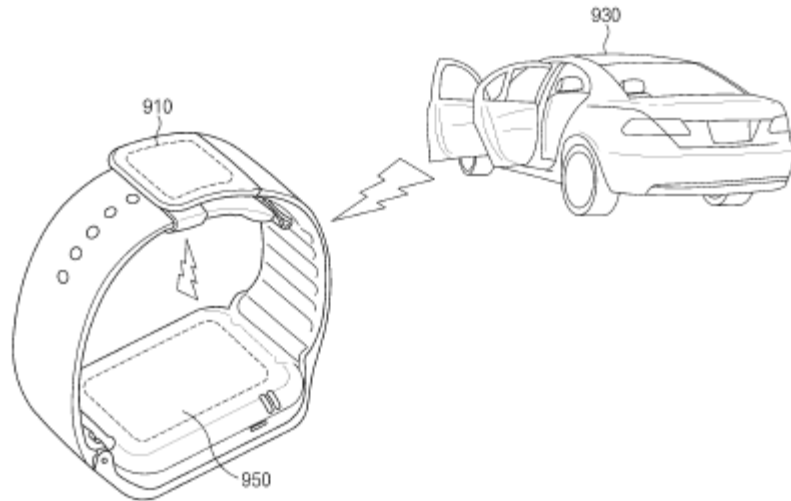


FIG. 9

162. Jun describes using the wearable to extract authentication information from the target object and then determine “whether the target object [] is an authenticated object.” Jun, 13:57-14:5. The wearable can also “transmit[] a control signal for controlling the authenticated object,” such as “*opening and closing of a lock* of a target object.” Jun, 14:10-15, 8:6-7, 14:32-61 (discussing biometric and location authentication). Jun teaches using its wearable’s GPS sensor to “detect[] an approach of the smart key [] to the target object” and unlock the target. Jun, 15:10-16.

B. Combining Agrafioti and Jun

163. POSAs would have had reasons to combine Agrafioti’s wearable and Jun’s GPS-based proximity-detection access control (e.g., door unlocking) technique (“Agrafioti-Jun”). Agrafioti and Jun each describe a wearable device having a GPS receiver and that performs user authentication before granting access

to a locked or secured system; thus POSAs would have recognized Jun's techniques as applicable and beneficial to Agrafioti. Agrafioti, [0109], [0112], [0121], [0163]-[0164]; Jun, 4:65-5:10, 14:32-61, 15:10-16.

164. POSAs would have had reasons to implement within Agrafioti's system and wearable Jun's methods using GPS information acquired by a wearable device to manage control signals. Jun, 15:10-16; Agrafioti, [0210] ("[A] user may be restricted or enabled access to access points based on geolocation"); Section X.A. For example, POSAs would have been motivated to apply Jun's teachings to Agrafioti to provide additional security. *See* Jun, 13:49-14:5 (explaining that its techniques provide ways to authenticate a user before permitting access to secured system); *see* EX1033, US Patent No. 5,708,422, 3:4-14 (describing two-factor authentication using a pager) and 16:3-14 (controlling "entry door to a secure room" using claimed two-factor authentication); EX1034, Lieber, "A Two-Step Plan to Stop Hackers," The New York Times (2014) (multifactor authentication "add[s] to the consumer's security").

165. POSAs would have reasonably expected success in modifying Agrafioti's system and method to include Jun's GPS-based techniques, at least because GPS location technology and authentication methods were well understood by POSAs and used in wearables long before the '480's priority date. Further, Jun explains a GPS-based, proximity authentication technique is

successfully implementable in a wearable device, such as a wrist-wearable device of the same form as Agrafioti's wearable device. Jun, 11:53-57, 13:49-53.

C. Claims 2, 5, 8

166. Agrafioti-Jun renders obvious claims 2, 5, and 8, reciting a GPS module providing user access, because Agrafioti-Jun includes Agrafioti's teachings for limitations of claims 2, 5, and 8, discussed in Sections VIII.E, VIII.H, IX.D, IX.E and Jun's teachings discussed below respecting limitations [2E]-[2F], [5A]-[5B], and [8A]-[8B].

1. **[2E] (“wherein said wearable device includes a GPS module for determining location of the wearable device user with respect to the secured electronic system”)/ [5A] (“wherein said wearable device further comprises a GPS module for determining location of the wearable device user with respect to secured electronic systems”)/ [8A] (wherein the smartwatch wearable device includes a GPS module for determining location of the smartwatch user with respect to the secured electronic system”)**

167. Jun's wearable, like Agrafioti's, includes a GPS module for determining location of the wearable user. Jun, 7:47-49, 8:55-56, 13:49-57, 14:32-35; 15:10-16. Applying Jun's teachings to Agrafioti's wearable results in the location being determined relative to the SES (i.e., relative to Agrafioti's access point). Jun, 15:10-16 (wearable detects “approach ...to the target object”); *see* Section XV.B.[2E].

2. [2F] (“wherein the step of providing a user access to or through the secured electronic systems is also dependent on the location of the wearable device user”)/ [5B] (“wherein access to the secured electronic systems is dependent on the location of the wearable device user in relationship to the secured electronic systems”) / [8B] (“wherein the step of providing a user access to or through the secured electronic systems is also dependent on a location of the smartwatch user with respect to a location of the secured electronic system”)

168. Applying Jun’s teachings to Agrafioti results in the wearable using GPS-determined location in part to “provid[e] a user access” to the SES. Jun, 15:10-23 (“lock releasing function”; “opening of a door”); *see* Section XV.B.[2F].

XI. GROUND 4: CLAIMS 1-9 ARE OBVIOUS OVER THARAPPEL-BERNEY

A. Tharappel (EX1007)

169. Tharappel provides a wearable that extends “authentication across a trust group of smart devices” (1:6-10) and provides “secure convenient access to multiple smart electronic devices” (3:55-58). Tharappel, 1:14-29; 2:16-4:15 (discussing challenges associated with the “proliferat[ion]” of wearables).

170. Figure 1 depicts an example trust group with two smart devices: wearable 40 and smart device 20. Tharappel, 2:24-26.

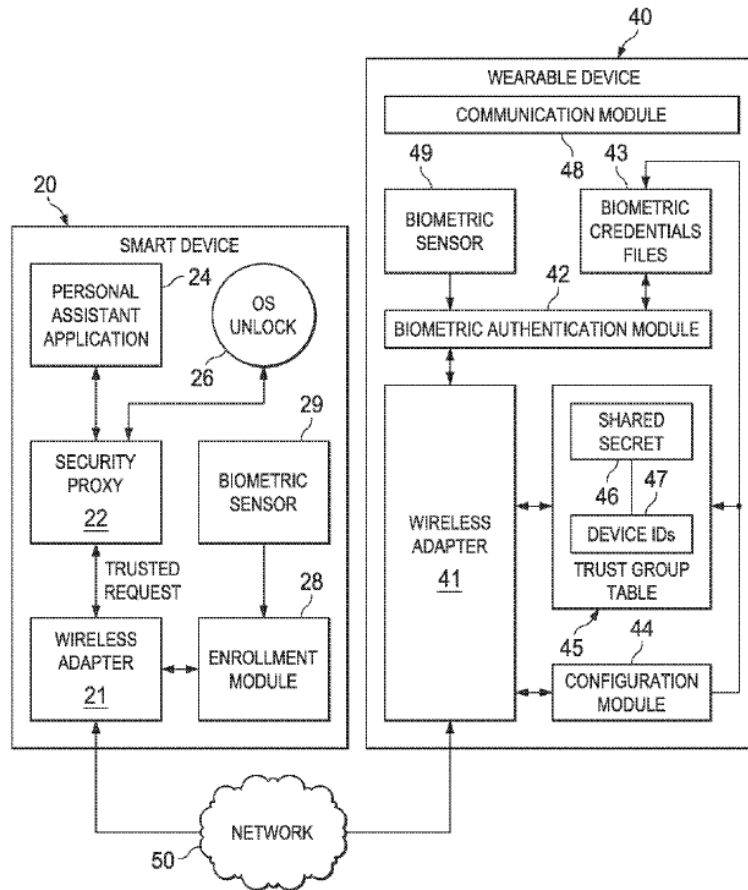


FIG. 1

171. Wearable 40 is “any smart device capable of voice audio, media, or data exchanges” (3:14-20), including an “electronic watch or bracelet” (3:58-61). Wearable 40 has biometric authentication capabilities. Tharappel, 2:28-29; 3:58-61.

172. Wearable 40 and smartphone 20 communicate “via a secure network 50.” Tharappel, 2:26-27; Fig. 1. Smart device 20 and wearable 40 include “respective wireless adapters 21 and 41” that include “wireless communication

circuitry” such as Wi-Fi, Bluetooth, NFC, satellite, and/or any cellular technologies (“including ‘3G/4G/5G/nG’”). Tharappel, 4:50-5:30.

173. Both smart device 20 and wearable 40 “include respective biometric sensors 29 and 49 for sensing” user “biological characteristics,” including but not limited to “voice patterns, speech, fingerprints ... hand features, palm prints, and pulse features.” Tharappel, 6:31-41. Biometric sensors 29 and 49 can include any suitable biometric sensor for sensing the desired biological characteristic, such as “a pulse sensor ... to sense pulse features.” Tharappel, 6:41-49. Wearable 40 includes “a biometric authentication module 42” (2:28-29), which allows the user to “authenticate[] to the wearable based on the user specific biometric credentials” (4:16-20). *See* Tharappel, 2:24-45. Wearable 40 “may be configured to allow a user to authenticate based on a single biometric credential or multiple biometric credentials.” Tharappel, 4:22-25.

174. Smart device 20 includes enrollment module 28, which allows the user to enroll his/her biometric characteristic “to enable biometric authentication.” Tharappel, 3:61-4:15; 2:46-55. In some embodiments, after authenticating the user using biometric credentials, “a determination may be made as to whether smart device 20 is in the trust group” by searching a trust group table “to find a device identifier corresponding to” smart device 20. Tharappel, 18:3-10; Fig. 8. “If smart

device [20] is in the trust group,” the user’s biometric authentication is extended to the smart device [20].” Tharappel, 18:14-18.

175. As discussed below, Tharappel discloses or renders obvious claims 1 and 3 and most limitations of all other challenged claims. Tharappel does not expressly disclose limitations (e.g., [2E]-[2F]) that require using GPS location for authentication or for allowing SES access. However, these limitations are rendered obvious by Tharappel-Berney. *See* Sections XI.D.2-XI.D.3.

B. Combining Tharappel and Berney

176. It would have been obvious to POSAs to combine Berney’s teachings about using GPS location and proximity information with Tharappel’s system and method. Tharappel and Berney both describe wearables that perform biometric-data-based authentication before providing user access to secured (e.g., locked) systems, data, and/or areas. Further, both Tharappel and Berney confirm that POSAs understood that implementing multi-factor authentication beneficially enhanced security. Tharappel, 1:14-31, 3:21-43, 4:20-28; Berney, [0002]-[0010], [0026]-[0027], [0038]; EX1013, 1:15-33, 1:54-2:50.

177. Berney specifically describes benefits of using GPS location data and proximity information to enhance wearable-based user authentication. For example, Berney teaches that requiring the wearable’s GPS receiver’s “very accurate location information” to “agree with proximity communications devices”

provides heightened security. Berney, [0040]. Berney discloses that using location and/or proximity information *in addition* to biometric-based authentication beneficially makes “forgery...much more difficult.” Berney, [0029], [0040].

178. Tharappel teaches that a wearable device configured for biometric authentication may also be “configured to accept other types of authentication credentials.” Tharappel, 4:16-28. POSAs would have recognized that Berney’s authentication using device proximity with GPS backup are “other types” of authentication credentials expressly permitted by Tharappel. Berney, [0037]-[0038], [0040].

179. POSAs also would have understood that including Berney’s proximity authentication with GPS backup in Tharappel would have furthered Tharappel’s goal of providing “secure, convenient access to” multiple smart devices (e.g., by providing another layer of security or backup authentication). Berney, [0038]; EX1013, U.S. Patent No. 8,943,580, Fadell, 6:54-67.

180. Additionally, in view of Berney, POSAs would have been motivated to apply Tharappel’s methods and systems (with or without Berney’s method of using location information) to both Tharappel’s use cases (e.g., unlocking smartphones) *and* the types of “wireless transactions” described in Berney (e.g.,

authorizing “car parking at a public parking meter” ([0036]), “an authorized person seeking entry to a restricted entry area” ([0037])).

181. POSAs would have reasonably expected success in implementing the above-described Tharappel-Berney combination, e.g., with the system described in Tharappel, (e.g., device 20, wearable 40, and accompanying circuitry), including because Tharappel and Berney disclose similar form factors (*e.g.*, watches) and describe similar platforms (including processors, memory, biometric readers, and antennas) for a wearable. Berney, Fig. 6, [0039]; Tharappel; Figs. 10-11, 19:13-14.

182. Both Berney and Tharappel describe wearable devices that include a GPS component and perform user authentication. Tharappel, 19:18-44; Berney, [0029], [0040]. Thus, POSAs would have expected success in implementing proximity authentication with GPS backup in Tharappel’s wearable based on Berney’s teachings. Such a modification could be implemented with software modifications to use GPS location data for authentication. Further, both GPS location technology generally and location-based authentication methods were well understood by POSAs at that time. EX1027, Abstract; EX1028, 4:61-67; EX1029, 1:25-35, 3:61-63.

183. Similarly, POSAs would have expected success in extending Tharappel (with and without Berney’s location-based authentication) to Berney’s

“transactions” (parking meters, locked doors, and POS systems (Berney, [0035]-[0037])), at least because Tharappel already discloses a flexible understanding of smart devices including e.g., “embedded controllers, car infotainment systems, navigation systems” (Tharappel, 3:4-13) and uses proximity of the wearable device to the smart device as part of the process for forming a secure connection.

Tharappel, 4:16-20; 18:3-6.

C. Claim 1

1. [1PRE] “A method for enabling a wearable device user to access secured electronic systems”

184. To the extent [1PRE] is limiting, Tharappel-Berney satisfies it via Tharappel’s methods (augmented by Berney’s techniques discussed §§VIII.B, VIII.D.1) for using “[a] *wearable* electronic *device*” to provide “*users*” with “*secure*, convenient *access* to multiple smart *electronic* devices,” including smartphones. Tharappel, 3:55-58, 2:16-19, 2:64-3:20, Abstract; Fig. 1. Thus, Tharappel-Berney allows an authenticated wearable device user to “interact with” and “control” a secured (e.g., locked) smartphone. Tharappel, 4:28-41, 6:62-7:15. As explained in §VIII.D.3 ([1B]), Patent Owner argues that locked smartphones are SES. Further, even under a narrower interpretation of SES, Tharappel-Berney satisfies [1PRE]. *See* Sections VIII.D.1 ([1PRE]), VIII.D.3 ([1B]).

2. [1A] “placing a wearable device in contact with a user”

185. Tharappel-Berney satisfies [1A] because the “[w]earable device...can be worn by a user” in contact with (“by attachment to”) a user’s “body part.” Tharappel, 3:14-20, 14:15-19, 14:49-50, Fig. 3B. Tharappel’s wearable can be a bracelet or a watch (Tharappel, 3:14-20), which POSAs understood (and Berney corroborates) to be worn in contact with the user. Berney, [0032] (“a sensor...on the back of watch 100...could read body temperature” or vein patterns “on the wearer’s wrist”).

a. [1A-1] “said wearable device including a telecommunications carrier access identification module”

186. Tharappel-Berney satisfies [1A-1] via the wearable’s “subscriber identity module (SIM) I/F 1030” (Tharappel, 19:27), which is part of “processor 1000” within Tharappel’s wearable 40 (Tharappel, 15:28-32, 16:51-55, 17:35-39, 19:12-45). According to the ’480 patent, a “SIM” is an example of the claimed “telecommunications carrier access identification module.” EX1001, Abstract (“A wearable device can include a telecommunications carrier identification module (e.g., SIM).”), 2:21-34, 4:4-14.

b. [1A-2] “a cellular RF communications module”

187. In [1A-2], “RF communications” means “radio frequency communications.” *See* Section VIII.D.2.b.

188. Tharappel's wearable includes Tharappel's "wireless adapter[]" including circuitry for communications via "*cellular* technologies (e.g., 3G/4G/5G/nG, etc.), other *radio frequencies*...and/or any other networking protocols that facilitate wireless *communications*." Tharappel, 4:50-5:8, Fig. 1, 5:9-30 ("the wireless connection may also include any *cellular* wireless"), 19:27-45 (wearable device processor 1000 includes "3G/4G modem 1075"). Tharappel-Berney's "wireless adapter" with at least "3G" "cellular technologies" is a "*cellular RF communications module*," as claimed. *See, e.g.*, EX1001, 5:31-37 (discussing cellular RF communications module using GSM or CDMA); EX1024, U.S. Patent No. 8,825,011, 7:48-50 (corroborating that 3G cellular used CDMA); EX1025, U.S. Patent No. 8,781,475, 6:36 (corroborating that 3G wireless used "CDMA/GSM").

c. [1A-3] "said wearable device including...a short-range RF communications module"

189. In addition to the "*cellular communications module*" (e.g., wireless adapter configured for 3G/4G/5G/nG cellular communication), Tharappel-Berney's wireless adapter's wireless communication circuitry also includes Bluetooth and NFC modules, which are types of claimed "*short-range RF communications modules*." Tharappel, 4:50-59, 19:27-45 (wearable device processor may include "Bluetooth™"), 5:9-15 (discussing connection via "Bluetooth™"), Fig. 1, 5:28-30 ("[N]etwork 50 represents a Bluetooth™ secure

wireless connection between wearable device 40 and smart device 20.”); EX1001, 2:6-10 (“short range radio frequency, and/or line of sight communications standards” include “Bluetooth” and “NFC”), 5:22-25, 6:23-24 (similar) 6:41-45 (similar); EX1024, U.S. Patent Publication No. 2010/0178866, [0002]-[0003] (“[N]ear field communication covers various short-*range* techniques and technologies which enable wireless communication.”), [0013] (Bluetooth a short-range communication technology)).

190. The wearable can include these modules alongside (i.e., in addition to) the circuitry for “cellular technologies” discussed §VIII.D.2.b ([1A-2]).

Tharappel, 4:50-5:5 (“The wireless communications may be inclusive of wireless technologies..., cellular technologies..., other radio frequencies (e.g., near field communications (NFC),...and/or any other networking protocols that facilitate wireless communications.”), 5:9-30 (“the wireless connection” may include “BluetoothTM” and “may also include any cellular wireless...connection”).

It also would have been obvious to implement Tharappel-Berney’s wearable to include both near field and cellular wireless communication, to support different use cases and enhance flexibility. EX1029, U.S. Patent No. 7,889,085, 4:1-5, 5:10-14; EX1035, U.S. Patent No. 8,111,589, 24:63-25:20 33:5-22; EX1036, U.S. Patent No. 8,467,272, 8:11-21; 26:34-37.

3. [1B] “achieving secured, short-range RF communication between the wearable device and a secured electronic system”

191. Tharappel-Berney satisfies [1B] in two alternative ways.

a. Locked Smartphone as SES:

192. The ’480 patent “broadly define[s]” an SES “as a system requiring electronic initiation for its operation or to gain access to it.” EX1001, 4:57-59. I understand that, in district court, Patent Owner has asserted that the recited SES can be a locked mobile phone. *See* EX1016, 5 (“a secured electronic system includes a mobile phone that uses a password”); EX1015, 6-7 (“[T]he mobile phone is a secured electronic system accessible by the accused watch.”); *id.* (“[T]he secured electronic system is the mobile phone[.]”); *id.* (“Access to or through the secured electronic system occurs during pairing of the accused watch to the mobile phone.”).

193. Under Patent Owner’s interpretation of SES, Tharappel-Berney’s locked smartphone (e.g., smart device 20) is an SES. Tharappel, 3:4-10, 3:64-65, 4:28-37, 6:62-7:15, 8:4-7 (“[S]ecurity proxy 22 may be configured to unlock the operating system of smart device 20 after verifying a received request was sent by wearable device 40.”). For example, Tharappel teaches that smart device 20 or its operating system may be “locked” (i.e., “capabilities of the smart device cannot be

accessed by a user”) until a “security proxy 22” electronically unlocks it.

Tharappel, 2:49-51, 6:64-67, 7:38-53, 8:4-7.

b. Other Types of SES.

194. Tharappel-Berney extends Tharappel’s system and method to Berney’s “wireless transactions,” including “car parking at a public parking meter” ([0036]), “an authorized person seeking entry to a restricted entry area” ([0037]), and “paying for a store-bought purchase by the use of” a wearable device ([0035]). Section XI.B. Tharappel-Berney’s “wireless transactions” are the *same types* of SESes expressly discussed in the ’480 patent. EX1001, 2:60-3:3 (“Examples of secured electronic systems include: *secured entry barriers* (e.g., doors, gates, safes),...*payment mechanisms* (e.g., vending machines, *parking meters*), *point-of-sale (POS)*....”); *see* §XI.B (discussing Tharappel-Berney).

c. Achieving Secured, Short-Range RF Communication:

195. Tharappel-Berney’s “wearable device 40 communicates with a smart device 20 via a *secure* network 50.” Tharappel, 2:24-45, 4:16-49 (“Where the user authenticates to the wearable device ... the wearable device establishes a *secure* wireless connection.”), Fig. 5 (Step 502), Fig. 7 (similar). In one embodiment, “network 50 represents a Bluetooth™ *secure* wireless connection between wearable device 40 and smart device 20.” Tharappel, 5:28-30, 5:9-30; *see* §VII.D.2.c (Bluetooth is short-range RF communication). Tharappel-Berney’s

wearable would connect with Berney’s “wireless transaction” devices (parking meter, point-of-sale, secure entry device/system) in the same manner. Berney, [0026]. Thus, Tharappel-Berney satisfies [1B].

4. [1C] “authenticating the user with at least one of [1C-1] the wearable device, [1C-2] a remote server..., and [1C-3] the secured electronic system via the secured, short-range RF communication”

196. Tharappel-Berney satisfies [1C] because if it satisfies any one or more of the three alternatives—[1C-1] through [1C-3]. *See* §VII.A

a. Authenticating with Wearable ([1C-1])

197. Tharappel-Berney authenticates the user with the wearable as recited by [1C-1]. A user may enroll biometric credentials “to enable authentication of the user by” Tharappel-Berney’s wearable. Tharappel, 6:9-29. The wearable’s biometric sensors can detect “voice patterns, speech, fingerprints, ...hand features, palm prints, and pulse features.” Tharappel, 6:30-49, 13:52-14:2, Fig. 8, 17:29-18:18. If the “biometric input data” acquired by the sensors matches the user’s previously- enrolled biometric credentials, then “authentication is successful.” Tharappel, 17:43-18:18. Tharappel-Berney’s wearable authentication with biometric input data (e.g., voice patterns, speech, pulse features) is the same type of wearable authentication that the ’480 patent describes. EX1001, 3:11-15 (“a user can be authenticated by biometric hardware (e.g., voice, skin illumination)

integrated on the smartwatch worn by the user”), 6:58-61; *see* Section XI.A (Tharappel-Berney implements Tharappel’s pulse sensing via skin illumination).

198. Tharappel-Berney additionally meets [1C-1] by incorporating any of Berney’s authentication techniques in Tharappel’s wearable, including “read[ing] body temperature,” “vein patterns on the wearer’s wrist,” “fingerprint,” and “speech pattern recognition,” both to secure access to the wearable itself and to transmit authentication to a separate transaction device. Berney, [0032]-[0033], [0037]-[0038], [0041]; *see* §XI.B (Tharappel-Berney combination).

199. Claim 1 does not require that the user authentication in [1C-1] be performed *after* the “secured communication” of [1B]. Nothing in the claim language’s “logic or grammar” requires that [1B] occur before [1C-1]. The ’480 specification also explicitly teaches that the “communication” step ([1B]) and the user authentication ([1C]) with a wearable step may occur in either order. *Compare* EX1001, 6:29-45; 7:3-11 (communication before authentication) *with* 6:46-53 (authentication before communication). For example, Figure 4’s “arrow labeled 325” illustrates that secured communication ([1B]) and user authentication (e.g., [1C-1]) can occur in either sequence. EX1001, 6:46-7:2; *see id.*, 7:3-22.

200. Nevertheless, Tharappel-Berney satisfies authenticating the user with the wearable ([1C-1]) even if it must be performed after [1B], because Tharappel-Berney’s wearable can receive the user’s enrolled biometric credentials from smart

device 20 via “secure wireless connection” and store the credentials for later biometric user authentication.¹² Tharappel, 14:57-15:47, 9:46-10:15, 12:12-15, Figs. 4-5. Communication of the biometric credentials to the wearable via secure wireless connection is a “*secured, short-range RF communication between the wearable*” and the smartphone (SES) as required by [1B] and occurs *before* the wearable uses those credentials to biometrically authenticate the user.

Specifically, Tharappel states that, “[a]t [step] 804, a determination is made as to whether a biometric authentication has been successful. Generally, a comparison may be made between the biometric input data and biometric credentials *previously enrolled* on wearable device.” Tharappel, 17:46-53 (“Thus, the implementation of Tharappel-Berney performs step [1B] (Tharappel’s step 406/502) before Tharappel-Berney performs step [1C-1] (Tharappel’s steps 802-804).

b. Authenticating with a Remote Server via Cellular Communications ([1C-2])

201. Tharappel-Berney authenticates the user with a remote server via cellular communications as recited by [1C-2] for the reasons discussed below Section XI.I.4.

¹² In other embodiments, the wearable receives the credentials via the cloud rather than directly from the smart device. Tharappel, 9:61-64.

c. Authenticating with SES via Secured, Short-Range RF Communication ([1C-3])

202. Tharappel-Berney additionally satisfies authenticating the user with the SES via the secured short-range RF communication ([1C-3]).

203. Tharappel teaches the security proxy in the SES (e.g., smartphone) determines “whether to unlock the operating system,” and what “level of security” to use to control the user’s “access to services and applications” on the SES, “based on an authentication result that the security proxy receives from the wearable device,” thus establishing an “authenticated session.” Tharappel, 19:3-11. This is authenticating the user with the SES. *See* Tharappel, 2:46-55 (describing “extending user authentication across a trust group of smart devices”); *id.*, 7:47-49. Tharappel also teaches that the Bluetooth connection (secured, short-range RF communication) may be used as a part of the authentication process. *See* Tharappel, 8:13-24. Thus, Tharappel’s techniques in Tharappel-Berney meet [1C-3].

204. Additionally, Berney discloses Berney’s “authorized entry” use case in which the SES is part of the authentication process. Berney, [0037]-[0038]. In this implementation, a “biometric data reader” on the wearable transmits identity data to “a counterpart device” via the Bluetooth RF communication. *Id.* A “security system associated with the secured area” determines “whether the validly identified user is or is not an authorized person.” *Id.* Applying Tharappel’s

wearable in this use case in Tharappel-Berney additionally meets [1C-3]. *See* §XI.A (Tharappel-Berney incorporates Berney’s described use cases).

5. [1D] “providing the user with access to or through the secured electronic system once authenticated”

205. Tharappel teaches that “[w]hen appropriate biometric credentials have been provided, the accessed smart device [*i.e.*, the SES] can unlock its operating system to allow the user to interact with the smart device.” Tharappel, 4:29-31, 2:49-51 (“An operating system (OS) unlock 26 is enabled by security proxy 22 when authentication of a user is extended from wearable device 40 to smart device 20.”), 4:16-49, 7:6-15.

206. Unlocking constitutes providing access to/through the SES as claimed. EX1001, 6:38-45. “[U]nlocking” allows users to access “applications data, and/or other capabilities of the smart device.” Tharappel, 6:67-7:6 (“A smart device” is “‘locked’ when any applications, data, and/or other capabilities of the smart device cannot be accessed by a user unless appropriate authentication credentials...are provided.”). Unlocking constitutes providing access *to* the SES. Additionally, because a smartphone includes applications that communicate *through* the smartphone to other devices, a POSA would appreciate that unlocking also constitutes providing access *through* the SES.

207. Tharappel teaches that a user may be granted access to the SES only after authentication. Tharappel, 7:4-43 (“In at least one embodiment, wearable

device 40 sends trusted requests from the user to smart device 20 *only after the user has been successfully authenticated.*”), 8:4-7; 18:3-18. POSAs would have maintained this functionality in Tharappel-Berney. Additionally, based on Berney’s teachings, it would have been obvious to POSAs to “provide the user with access to or through” Berney’s wireless transaction SESes “*once authenticated*” as claimed. *See* Berney, [0035]-[0036] (enabling transactions at checkout counter, parking meter); §VIII.B. Thus, Tharappel-Berney satisfies [1D].

6. [1E] “wherein said wearable device comprises a smartwatch including a microphone and skin illumination and measurement hardware”

208. Tharappel-Berney includes Tharappel’s “biometric authentication capability” for any type of suitable biometric authentication, such as by voice, fingerprint, hand features, or pulse. *See* Tharappel, 3:58-64, 2:28-29 (wearable device with biometric authentication module), 4:16-41, 6:11-27, 6:30-49 (biometric sensor 49 may be “a fingerprint sensor” or “a microphone”), 9:65-10:32 (biometric input includes “voice input, fingerprint input, ...hand input, pulse input”), 13:27-64, 15:4-8, Fig. 1 (biometric sensor 49). Tharappel-Berney’s wearable thus includes a microphone and voice authentication capabilities as taught by Tharappel. *See* Tharappel, 6:44-45 (“microphone can be used to sense a voice” for “voice identification”), 13:30-35, 13:52-56.

209. Tharappel-Berney's biometric authentication may include fingerprint or pulse authentication (Tharappel, 3:58-64) with appropriate sensors (Tharappel, 6:43-48). For example, "a pulse sensor can be used to sense pulse features." Tharappel, 6:43-48. POSA' would have understood that a typical, conventional, and obvious implementation of "a pulse sensor" was a reflection-type pulse sensor, including hardware that operated by emitting infrared, red, or green-light, and then measuring reflection, transmission, or variation as discussed in Section VIII.D.6; Thus, Tharappel-Berney satisfies "*skin illumination and measurement hardware*" for substantially the same reasons that Agrafioti-Berney satisfies "*skin illumination and measurement hardware*."

210. Additionally, from Berney, POSAs understood that biometric authentication can be based on "vein patterns" on a user's wrist. Berney, [0032]. And long before the '480 patent, POSAs knew that vein patterns were commonly detected and measured with sensors considered "*skin illumination and measurement hardware*," as claimed. For example, POSAs understood that illuminators and sensors were commonly used to collect wrist vein pattern data, and such data were commonly used for authentication purposes.

211. For example, the use of skin illumination and sensors to collect wrist vein pattern data was demonstrated by Lee and Fadell. *See* Lee, [0030]-[0031],

[0058]; EX1037, US Publication No. 2015/0304322, [0040], [0053]; EX1013, Fadell, 9:48-53.

212. POSAs would have been motivated and reasonably expected success in including Berney's vein-pattern sensors as part of Tharappel's biometric authentication methods and sensors including hand feature biometrics. *See* Tharappel, 3:61-66, 6:37-41; §IX.B.

213. In view of Berney's and Tharappel's teachings, Tharappel-Berney would include at least the types of skin illuminators and sensors used for pulse and vein reading. Thus, Tharappel-Berney satisfies [1E].

7. [1F] “and wherein authentication of the user is based on biometric information obtained from the user via at least one of the microphone and the skin illumination and measurement hardware”

214. In Tharappel-Berney, the authentication described above in connection with [1C] is “based on biometric information obtained from the user via at least one of the microphone and the skin illumination and measurement hardware” as discussed in connection with [1E]. *See* §XI.C.6. Thus, Tharappel-Berney satisfies [1F].

D. Claim 2

1. [2PRE]-[2D]

215. [2PRE]-[2D] are identical to [1PRE]-[1D]. Tharappel-Berney satisfies [2PRE]-[2D] for the reasons discussed above. *See* §XI.C.

2. [2E] “said wearable device includes a GPS module for determining location of the wearable device user with respect to the secured electronic system”

216. Tharappel-Berney’s wearable includes a GPS module. Tharappel, 19:20-21, 19:44; Berney, [0029], [0040]. As discussed in §XI.B, Tharappel-Berney incorporates Berney’s teaching to use the GPS receiver to acquire absolute location information from at least two devices and then compare those locations as a back-up for proximity information. Berney, [0040] (discuss use of GPS’s “very accurate location information” that may provide “a backup to a proximity location”).

217. Further, POSAs would have known generally that one way of determining a wearable user’s location with respect to a device or system (e.g., SES) is by comparing GPS location information of each respective device/system. Berney, [0040]; EX1026, 5:4-14, 10:33-45 (U.S. Patent No. 9,743,279) (corroborating POSA’s background knowledge “to authenticate one or more mobile devices of a user using a wearable device of the user” using “sensor data” from a “GPS”); *see also id.*, 6:65-7:2; 10:8-30; 12:31-36; 12:65-66 (describing capturing GPS data, and determining a “threshold value represents the maximum distance between any two similar sensor signatures.”); Fig. 5 (where “comparison value < threshold value” proceeding to “[l]ogin to the mobile device”).

218. Thus, and as discussed above in section XI.A, Tharappel-Berney's wearable device includes the ability to determine the location of the wearable device user with respect to Tharappel-Berney's SESes (including Tharappel's smartphone and Berney's wireless transactions). Berney, [0040]; Sections VIII.B (Berney), VIII.E.3 ([2F]), XI.B (Tharappel-Berney); *see also* EX1010, 15:10-18 (describing "detect[ing] an approach of the smart key [] to the target object [] ***based on a GPS sensor*** included in the smart key" and sending a unlock instruction in response), 14:32-35.

3. [2F] "the step of providing a user access to or through the secured electronic systems is also dependent on the location of the wearable device user"

219. As discussed above (§XI.B-XI.C), Tharappel-Berney implements a comparison of the "very accurate location information" obtained from the wearable's GPS receiver against the desired SES's location. Further, Tharappel-Berney's method determines whether the wearable's GPS location data "agree[s]" with other proximity information (e.g., a short-range RF connection) to confirm validity of the wearable device and to make "forgery" more difficult. Berney, [0041]. Tharappel-Berney also authenticates the wearable user's identity. *See id.*, [0031] (explaining that "proper [biometric] authentication ***coupled with proximity*** and communication would result in a valid user identification"). Thus, Tharappel-

Berney performs the step of providing user access to a desired SES dependent on the location of the wearable user.

220. To the extent that [2F] requires that “the location of the wearable device” be the location determined by the GPS module, this step would have been obvious to POSAs for the same reasons discussed in Sections XI.B, VIII.E.2, Berney’s teachings that GPS location is “very accurate,” and a POSA’s familiarity with the many possible uses of GPS location information. For example, it would have been obvious to POSAs to configure Tharappel-Berney such that access to the SES granted only when the wearable’s GPS location indicates that the wearable is in a particular location. *See* Section VIII.C (Agrafioti-Berney).

221. In the parallel litigation, Patent Owner asserts that providing access is “dependent on the location of the wearable device user” when the wearable device user is required to be within range of a short-range signal, e.g., Bluetooth, to access the SES. *See* EX1016, No. 3:24-cv-00937-TSH (N.D. Cal.), No. 21 at 5-6 (arguing that access to or through the secured electronic system is dependent on the location of the wearable device user because “the phone must be within 0.5 m.”). Under Patent Owner’s interpretation of [2F], Tharappel-Berney additionally satisfies [2F] because Tharappel-Berney provides access to the SES when authentication is successful and the wearable and smartphone are within wireless range of each other, as taught by Tharappel. Tharappel, 18:3-6 (“If the authentication is

successful,...the wearable device may establish a secure wireless connection to a smart device *within a wireless range* of the wearable device.”); Fig. 8.

E. Claim 3

1. [3PRE]-[3D]

222. [3PRE]-[3D] are identical to [1PRE][1D]. Tharappel-Berney satisfies [3PRE]-[3D] for the reasons discussed §§XI.C.1-XI.C.5.

2. [3E] “said wearable device further comprises a registration module”

223. Tharappel-Berney’s wearable includes Tharappel’s trust group table, which is a “registration module” as recited by [3E]. Tharappel, 2:36-45, 10:33-65. As discussed (*supra* §XI.A), Tharappel describes “extending user authentication across a trust group of smart devices.” Tharappel, 2:16-19. Tharappel, 2:16-19. The devices in the trust group are identified within a “trust group table” stored on the wearable device. The trust group table includes a “device ID” of each smart device in the trust group. Tharappel, 10:33-37. The device ID in Tharappel’s trust group table “can be an index” providing “uniquely identifying information for each smart device.” Tharappel, 10:42-44. For example, “each device ID can be mapped to a different shared secret.” Tharappel, 10:45-46. The shared secret “may be used to secure a wireless connection between [a] wearable device [] and [a] smart device.” Tharappel, 10:50-52. Additionally, Tharappel’s “device IDs can be mapped to wireless connection security information.” Tharappel, 10:66-11:8.

224. The presence of a device in the trust group table may be used at least in part to determine whether the device is a member of the trust group. *See, e.g.*, Tharappel, 18:10-12 (“In at least one embodiment, the smart device is determined to be in the trust group if its device identifier is mapped to a shared secret in trust group table 45.”); 32:19-29 (similar). When “the smart device is included in [the] trust group,” an authenticated user *e* can “send a communication to unlock the smart device.” Tharappel, Abstract. Tharappel-Berney thus registers the smart device (SES) for access via the wearable’s user authentication, and therefore the wearable includes “*a registration module*,” as claimed.

3. **[3F] “providing a user access to or through the secured electronic system is determined by at least one of the wearable device and the registration module based on at least one of: [3F-1] the user authenticated for access to secured electronic system by the wearable device, ... [3F-4] the user granted access based on location, and [3F-5] the user granted access based on proximity to a secured electronic system”**

225. [3F] first recites “*providing a user access to or through the secure electronic system is determined by at least one of the wearable device and registration module.*”

226. Tharappel-Berney can authenticate the user using the wearable device as discussed *supra* § XI.C[1C]). Tharappel-Berney can also authenticate the user using the trust group table, *i.e.*, a registration module. *Compare* Tharappel, 18:6-16 (when a determination is made that the smart device is in the trust group, then

“*biometric authentication is extended to the smart device*”) with *id.* 17:63-18:2, 18:12-14 (user is not authenticated to access smart device “[i]f the smart device is *not* in the trust group”).

227. [3F] next recites that the providing access step is “based on at least one of” five disjunctive options. *See supra* claim construction §VII.A. Tharappel-Berney satisfies at least three of those options, thus rendering limitation [3F] obvious (*supra* Section VII.A): [3F-1] for the reasons discussed above §XI.C.4.a; [3F-4] for the reasons discussed *supra* §XI.D.3; and [3F-5] for the reasons discussed *supra* §XI.D.3. In each case, “*providing a user access*” is based on the respective authentication, as explained *supra* § XI.C.5 ([1D]).

F. Claim 4 “[PRE] The method of claim 2, [A] wherein said wearable device further comprises a smartwatch including a microphone and skin illumination and measurement hardware, [B] wherein authentication of the user is based on biometric information obtained from the user via at least one of the microphone and the skin illumination and measurement hardware.”

228. Claim 4 depends from claim 2 and recites the identical requirements of [1E]-[1F]. Tharappel-Berney satisfies claim 4 for the reasons discussed *supra* §§XI.C.6-XI.C.7.

- G. Claim 5 “[PRE] The method of claim 1, [A] wherein said wearable device further comprises a GPS module for determining location of the wearable device user with respect to secured electronic systems, and [B] wherein access to the secured electronic systems is dependent on the location of the wearable device user in relationship to the secured electronic systems.”**

229. Claim 5 depends from claim 1 and recites the identical requirements of [2E] and a similar requirement to [2F] with the additional requirement that access to the SES “*is dependent on the location of the wearable device user in relationship to the*” SES. Tharappel-Berney satisfies claim 5 for the reasons discussed above in sections XI.D.2-XI.D.3.

- H. Claim 6 “[PRE] The method of claim 3, [A] wherein said wearable device further comprises a smartwatch including a microphone and skin illumination and measurement hardware, [B] wherein authentication of the user is based on biometric information obtained from the user via at least one of the microphone and the skin illumination and measurement hardware.”**

230. Claim 6 depends from claim 3 and recites the identical requirements of [1E]-[1F]. Tharappel-Berney satisfies claim 6 for the reasons discussed *supra* §§XI.C.6-XI.C.6.

I. Claim 7

- 1. [7PRE] “A method for enabling a smartwatch user to access secured electronic systems”**

231. [7PRE] is nearly identical [1PRE] except that [7PRE] refers to “*a smartwatch user*” rather than a “*wearable device user*.” Tharappel-Berney’s

wearable includes a smartwatch, and its user may be a smartwatch user. *See* Tharappel, 3:14-20; 6:25-26; 8:64-9:3; 13:30-14:2. Tharappel-Berney satisfies [7PRE] for the same reasons it satisfies [1PRE] and because the user may be a smartwatch user. *See supra* §XI.C.1.

2. **[7A] “placing a smartwatch in contact with a user, the smartwatch including a registration module, a short-range RF communications module, a microphone, and skin illumination and measurement hardware”**

232. [7A] is similar to [1A] but specific to a smartwatch. Tharappel-Berney’s wearable can be a smartwatch. Thus, Tharappel-Berney satisfies [7A] for the same reasons explained above Section XI.C.2.

3. **[7B] achieving secured, short-range RF communication between the smartwatch and a secured electronic system; [7C] authenticating the user with at least one of the smartwatch and the secured electronic system using at least one biometric obtained from at least one of the microphone and the skin illumination and measurement hardware; [7D] providing the user with access to or through the secured electronic system once authenticated; and**

233. [7B]-[7D] [7B]-[7D] are substantially the same as [1B]-[1D] but specific to a smartwatch. Tharappel-Berney’s method includes a smartwatch and satisfies [7B]-[7D] for the reasons discussed *supra* §§ XI.C.3-XI.C.5.

4. [7E]¹³ “a subscriber identification module (SIM) and a cellular communications module, wherein authentication of the user is also achievable by accessing a remote server via cellular communications supported by the SIM and the cellular communications module and matching the at least one biometric”

234. As discussed *supra* §XI.A and §XI.c.2, Tharappel-Berney includes a SIM and a cellular communications module that support cellular communications.

235. Tharappel-Berney’s biometric data may be transferred via a secure wireless connection. Tharappel, 12:12-29. For example, “the biometric credentials” may be “transferred to the cloud and then transferred to a primary wearable device 60.” Tharappel, 12:22-25. POSAs would have understood that such data transfer involves the wearable accessing a remote server (in the cloud) to obtain the biometric credentials and match the user’s current biometric input to those past credentials. POSAs would recognize that the smartwatch can access the cloud in multiple ways, including using the internet (*e.g.*, via WiFi) and cellular data, both of which Tharappel discloses. Tharappel, 4:59-5:2 (“WiFi” and “cellular technologies”), 5:24-27 (same), 19:35-45.

236. Accordingly, cellular data is a disclosed option, as well as one of a finite number of known, conventional options for accessing the cloud. *Id.*; *see also*

¹³ [7E] renders claim 7 indefinite because it recites an apparatus when claim 7 is a method claim.

Tharappel, 4:59-5:2;12:22-25. Thus, Tharappel-Berney satisfies matching the biometric data sensed by the wearable device by accessing a remote server via the cellular communications.

- J. Claim 8 “[PRE] The method of claim 7, [A] wherein the smartwatch wearable device includes a GPS module for determining location of the smartwatch user with respect to the secured electronic system, and [B] wherein the step of providing a user access to or through the secured electronic systems is also dependent on a location of the smartwatch user with respect to a location of the secured electronic system.”**

237. Claim 8 depends from claim 7 and recites substantially the same requirements as [2F] and claim 5, and Tharappel-Berney satisfies [8B] for substantially the same reasons as [2F]. *See* Section XI.D.3.

- K. Claim 9 “The method of claim 8, wherein providing a user access to or through the secured electronic system is determined by the registration module based on at least one of: [1] user authentication for access to secured electronic system by smartwatch, [2] user biometric authentication by a wireless carrier, [3] user biometric authentication by remote server, [4] user location, and [5] user proximity to a secured electronic system.”**

238. Claim 9 depends from claim 8 and recites substantially the same requirements as [3F]. Tharappel-Berney satisfies claim 9 for the reasons discussed *supra* §XI.E.3.

XII. GROUND 5: CLAIMS 1-9 ARE OBVIOUS OVER THARAPPEL-BERNEY-LEE

A. Tharappel-Berney-Lee

239. Based on Lee, POSAs would have had reasons to modify Tharappel-Berney to incorporate Lee's wrist-vein-pattern biometric authentication techniques discussed above in section IX.A (resulting in "Tharappel-Berney-Lee"). For example, POSAs would have understood that Lee's biometric authentication techniques based on wrist-vein-pattern identification provide "other types" of authentication credentials contemplated by Tharappel and that Lee describes in detail the type of wrist-contact authentication techniques mentioned in Berney. Lee, [0005], [0070]; Tharappel, 8:53, Berney, [0032]; *see* §§ IX.A- IX.B. POSAs also would have understood that including Lee's biometric authentication methods would further Tharappel's goal of providing "secure, convenient access to" multiple smart devices. Tharappel, 3:55-58.

240. Incorporating Lee's biometric authentication teachings in Tharappel-Berney-Lee would have been nothing more than using a known biometric authentication method using the techniques described in Lee. POSAs would have had a reasonable expectation of success in implementing Lee's wrist-vein-pattern biometric-sensor-based authentication in Tharappel-Berney-Lee's wearable.

241. Tharappel, Berney, and Lee each have similar form factors (*e.g.*, watches) and describe similar platforms (including processors, memory, biometric

readers, and antennas). Lee, Fig. 4A, [0045]-[0046]; Tharappel; Figs. 10-11, 19:13-14; Berney, Fig. 6, ¶[0026], [0028]-[0029], [0038]-[0039]. For example, Tharappel, Berney, and Lee each describe a wearable that authenticates a user with biometric data before providing the user access to secured (e.g., locked) data or areas. Further, both biometric sensors generally and biometric-based authentication methods were well understood by POSAs by the '480 patent's claimed priority date.

B. Claims 1-9

242. Tharappel-Berney-Lee satisfies claims 1-9 for the same reasons that Tharappel-Berney satisfies claims 1-9. *See* §§XI.C-XI.K. However, to the extent that Tharappel-Berney does not satisfy limitations that include “skin illumination and measurement hardware,” Tharappel-Berney-Lee satisfies those limitations as set forth below.

1. [1E] (“wherein said wearable device comprises a smartwatch including a microphone and skin illumination and measurement hardware”) / [4A] (wherein said wearable device further comprises a smartwatch including a microphone and skin illumination and measurement hardware”) / [6A] (“wherein said wearable device further comprises a smartwatch including a microphone and skin illumination and measurement hardware”) / [7A] (“placing a smartwatch in contact with a user, the smartwatch including a registration module, a short-range RF communications module, a microphone, and skin illumination and measurement hardware”)

243. Tharappel-Berney-Lee satisfies [1E]/[4A]/[6A]/[7A] at least because it includes Lee’s array of illuminators and sensors which are “skin illumination and measurement hardware,” as claimed. *See* §§IX.A, IX.C.1

2. [1F] (“wherein authentication of the user is based on biometric information obtained from the user via at least one of the microphone and the skin illumination and measurement hardware”) / [4B] (“wherein authentication of the user is based on biometric information obtained from the user via at least one of the microphone and the skin illumination and measurement hardware”) / [6B] (“wherein authentication of the user is based on biometric information obtained from the user via at least one of the microphone and the skin illumination and measurement hardware”) / [7C] (“authenticating the user with at least one of the smartwatch and the secured electronic system using at least one biometric obtained from at least one of the microphone and the skin illumination and measurement hardware”)

244. Tharappel-Berney-Lee satisfies [1F]/[4B]/[6B]/[7C] for the reasons that Tharappel-Berney does as set forth in Section IX.C.2. Additionally, when Tharappel-Berney-Lee uses Lee’s wrist vein data for authentication, that wrist vein

data is obtained from the Tharappel-Berney-Lee wearable's array of illuminators and other sensors that illuminate the wrist skin. Lee, [0036]-[0038]. Tharappel-Berney-Lee uses the gathered vein pattern data to authenticate by using Lee's "authentication software" to correlate the gathered vein pattern data with "reference wrist vein patterns." Lee, [0058]-[0059].

XIII. GROUND 6: CLAIMS 2 AND 4 ARE OBVIOUS OVER THARAPPEL AND JUN

A. Combining Tharappel and Jun

245. POSAs would have had reasons to implement (in Tharappel's system) Jun's GPS-location proximity-detection access control (e.g., door unlocking) technique discussed above in section X.A (resulting in "Tharappel-Jun"). Tharappel and Jun each describe a wearable device having a GPS receiver that performs user authentication before granting access to a locked or secured system. Tharappel, 2:16-23, 4:37-41, 19:18-44; Jun, 4:65-5:10, 14:32-61, 15:10-16. POSAs would have recognized Jun's techniques as applicable and beneficial to Tharappel.

246. For example, POSAs would have been motivated to apply Jun's methods using GPS and proximity of the wearable device to manage control signals from the smart device to Tharappel to provide additional security. *See* Jun, 13:49-14:5 (explaining that its techniques provide ways to authenticate a user before permitting access to secured system), 15:10-16; Tharappel, 4:16-28; *supra*

Section VIII.C (describing recognized benefits of user authentication and security enhancement by using multiple authentication mechanisms).

247. POSAs would have reasonably expected success in modifying Tharappel’s wearable to include Jun’s GPS-based authentication, at least because GPS location technology and authentication methods were well understood by POSAs long before the ’480’s invention date. Further, Jun explains a GPS-based, proximity authentication technique is successfully implementable in a wearable device, such as a wrist-wearable device of the same form as Tharappel’s wearable device. Jun, 11:53-57; 13:49-53.

B. Claim 2

1. [2PRE] “A method for enabling a wearable device user to access secured electronic systems”

248. Tharappel-Jun includes Tharappel’s system and methods for providing “secure, convenient access to multiple smart electronic devices,” including smartphones. Tharappel, 3:55-58; *see also* Section XI.C.1. In view of Jun’s teachings, POSAs would have extended Tharappel’s system for providing “secure, convenient access” to allow the user to access the types of SESes described in Jun—e.g., unlocking and locking a target object. Jun, 4:4-9, 7:52-53, 8:3-10, 8:53-56, 11:53-59, 14:13-17 (“[T]he smart key [] transmits a control signal regarding opening and closing of a lock of a target object ...”), 15:10-16 (“when

the smart key [] approaches the target object [] ... a lock releasing function” occurs).

2. **[2A] “placing a wearable device in contact with a user, said wearable device including [1] a telecommunications carrier access identification module, [2] a cellular RF communications module, and [3] a short-range RF communications module”**

249. Tharappel-Jun includes Tharappel’s method modified in view of Jun, which includes using a wearable for biometric and other types (e.g., location-based) of user authentication. *See* Sections XI.A, XI.B, XIII.A. As discussed in Sections XI.A, XI.C.2, Tharappel-Jun’s method “*places a wearable device in contact with a user*” as claimed. Additionally, Tharappel-Jun’s method of using a wearable includes the circuitry disclosed in Tharappel and discussed in Sections XI.A, XI.C.2. Thus, Tharappel-Jun satisfies [2A1]-[2A2].

3. **[2B] “achieving secured, short-range RF communication between the wearable device and a secured electronic system”**

250. Tharappel-Jun’s method includes Tharappel’s method for biometric authentication and secured short-range RF communication between the wearable and a locked smartphone as described in Tharappel. *See* §XI.A. Under Patent Owner’s interpretation of SES, Tharappel-Jun’s locked smartphone (e.g., smartphone 20) is an SES. Tharappel, 3:4-10, 3:64-65, 4:28-37, 6:62-7:15, 8:4-7.

Additionally, Tharappel-Jun extends Tharappel's system to applications described in Jun, such as unlocking and controlling a target object. For example, Jun describes using its wearable to "control[] transmission of a control signal regarding opening and closing of a locker for a target object (for example, opening and closing of a door of a vehicle or opening and closing of an entrance gate)." Jun, 8:2-10; *see also* 14:9-16. Jun also uses the wearable device to "turn[] on a starter of a vehicle." 14:22-24. The '480 patent expressly identifies "***secured entry barriers*** (e.g., doors, ***gates***, safes)" and "***vehicle[s]*** (e.g., to compartment access and start ignition)" as examples of SESes. EX,1001, 2:60-3:3. Thus, Tharappel-Jun satisfies [2B] for this additional reason.

4. [2C] **"authenticating the user with at least one of [1] the wearable device, [2] a remote server via cellular communications supported by the telecommunications carrier access identification module and the cellular RF communications module, and [3] the secured electronic system via the secured, short-range RF communication"**

251. Tharappel-Jun includes Tharappel's systems and methods and satisfies [2C] at least for the same reasons that Tharappel-Lee does. *See* Section XI.C.4 ([1C]).

252. Specifically, Tharappel-Jun includes Tharappel's method for biometric user authentication and thus authenticates the user with the wearable (e.g., by matching voice, fingerprint, voice data to previously-enrolled biometric credentials) as recited by [2C-1]. Tharappel, 6:9-49, 13:52-14:2, 7:29-18:18;

EX1001, 3:11-15, 6:58-61; §XI.C.4 ([1C]). To the extent [2C] must be performed after [2B], Tharappel-Jun satisfies [2C] because the wearable can receive the user's enrolled biometric credentials from smart device 20 via "secure wireless connection" and store the credentials for later biometric user authentication.

Tharappel, 14:57-15:47; *id.*, 9:46-10:15, 12:12-15, Figs. 4-5. Communication of the biometric credentials from the smart device to the wearable via secure wireless connection is a "*secured, short-range RF communication between the wearable*" and the smartphone (SES) as required by [2B] and occurs *before* the wearable uses those credentials to biometrically authenticate the user. Tharappel, 17:46-53 ("At 804, a determination is made as to whether a biometric authentication has been successful. Generally, a comparison may be made between the biometric input data and biometric credentials previously enrolled on wearable device.").

253. Tharappel-Jun additionally satisfies authenticating the user with the SES via the secured short-range RF communication as recited by [2C-3], including because Tharappel-Jun encompasses Tharappel's "security proxy" that establishes an "authenticated session." Tharappel, 19:3-11; Section [1C] (discussing Tharappel's "security proxy").

5. [2D] "providing the user with access to or through the secured electronic system once authenticated"

254. Tharappel-Jun includes Tharappel's functionality for unlocking the smart phone only after "appropriate biometric credentials" have been provided and

verified. Tharappel, 4:29-31; id. 2:49-51, 7:6-15. “[U]nlocking” allows users to access “applications data, and/or other capabilities of the smart device” (Tharappel, 6:67-7:6) and constitutes providing access to/through the SES as claimed (EX1001, 6:38-45). Tharappel-Jun further applies Tharappel’s wearable to Jun’s disclosed use case, which also provides the user with access to or through a secured electronic system, such as to unlock or start a vehicle only after authentication has been performed. Jun, 14:9-61, 8:3-10. Thus, Tharappel-Jun satisfies [2D] in two alternative ways.

6. [2E] “wherein said wearable device includes a GPS module for determining location of the wearable device user with respect to the secured electronic system”

255. Tharappel-Jun’s wearable includes “a global position system (GPS).” Tharappel, 19:18-44 (discussing ARM architecture that includes “a global position system (GPS)”). Tharappel-Jun implements using a wearable’s GPS for determining location of the wearable device user with respect to the secured electronic system (e.g., Jun’s locked target object). Jun, 7:47-49, 8:55-56, 13:49-57, 14:32-35, 15:10-16; *supra* Section XIII.A. For example, Jun describes an embodiment in which “when the user approaches the target object [e.g., a car] while carrying (or wearing) the smart key [], the smart key [] detects an approach of the smart key [] to the target object [] based on a GPS sensor included in the smart key.” Jun, 15:10-16 (emphasis added).

256. Based on Jun (e.g., Jun, 15:10-16) Tharappel-Jun utilizes the wearable's GPS for determining location of the wearable device user with respect to the secured electronic system, as claimed.

7. [2F] **“wherein the step of providing a user access to or through the secured electronic systems is also dependent on the location of the wearable device user”**

257. Tharappel-Jun meets [2F] because it implements Jun's teaching that the wearable “performs a control function,” e.g., “a lock releasing function” (Jun, 15:10-16) or “opening of a door of a vehicle, turning on the vehicle light, opening of a trunk, or automatic startup of the vehicle” (Jun, 15:18-23).

258. Second, Tharappel-Jun also provides user access *dependent* on the location of the wearable device user as taught by Jun. For example, after the smart key “detects an approach of the smart key [] to the target object [] based on a GPS sensor included in the smart key []” as described above, the smart key “performs a control function designated to be performed when the smart *key [] approaches the target object []*” Jun, 15:10-16 (emphasis added); see also 15:18-23 (“the smart key ...*when recognizing location information of the* user, performs a designated control function regarding, for example opening of a door of a vehicle...”).

C. Claim 4

1. **[4A] “wherein said wearable device further comprises a smartwatch including a microphone and skin illumination and measurement hardware”**

259. Tharappel-Jun includes Tharappel’s biometric authentication using microphone and voice authentication and fingerprint/hand input, as discussed in Section XI.C.6 ([1E]), as well as Jun’s biometric data collection and authentication including fingerprint and iris scan (Jun, 14:37-61). Thus, Tharappel-Jun meets [4A].

2. **[4B] “wherein authentication of the user is based on biometric information obtained from the user via at least one of the microphone and the skin illumination and measurement hardware”**

260. Tharappel-Jun meets [4B] because Tharappel and Jun each perform biometric authentication using the microphone and/or skin measurement techniques, as described in the previous section.

XIV. CONCLUSION

261. As explained above, the Challenged Claims of the ’480 Patent are rendered obvious by the combinations discussed above and the Challenged Claims are unpatentable under 35 U.S.C. § 103.

262. In signing this declaration, I understand that the declaration will be filed as evidence in a review proceeding before the Patent Trial and Appeal Board of the U.S. Patent and Trademark Office. I acknowledge that I may be subject to

cross examination in the case and that cross examination will take place within the United States. If cross examination is required of me, I will appear for cross examination within the United States during the time allotted for cross examination.

I declare that all statements made herein of my own knowledge are true, that all statements made on information and belief are believed to be true, and that these statements were made with the knowledge that willful false statements and the like are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code.

I declare under penalty of perjury that the foregoing is true and correct.

A handwritten signature in black ink, appearing to read "David H. Williams", written in a cursive style.

Executed on: April 26, 2024

David H. Williams

CLAIM LISTING

The following claim listing assigns element labels (e.g., [1A], [1B], etc.) to certain claims for clarity.

Claim 1
[1PRE]: A method for enabling a wearable device user to access secured electronic systems, said method comprising:
[1A] placing a wearable device in contact with a user, said wearable device including [1] a telecommunications carrier access identification module, [2] a cellular RF communications module, and [3] a short-range RF communications module;
[1B] achieving secured, short-range RF communication between the wearable device and a secured electronic system;
[1C] authenticating the user with at least one of [1] the wearable device, [2] a remote server via cellular communications supported by the telecommunications carrier access identification module and the cellular RF communications module, and [3] the secured electronic system via the secured, short-range RF communication; and
[1D] providing the user with access to or through the secured electronic system once authenticated;
[1E] wherein said wearable device comprises a smartwatch including a microphone and skin illumination and measurement hardware, and
[1F] wherein authentication of the user is based on biometric information obtained from the user via at least one of the microphone and the skin illumination and measurement hardware.
Claim 2
[2PRE]: A method for enabling a wearable device user to access secured electronic systems, said method comprising:
[2A] placing a wearable device in contact with a user, said wearable device including [1] a telecommunications carrier access identification module, [2] a cellular RF communications module, and [3] a short-range RF communications module;
[2B] achieving secured, short-range RF communication between the wearable device and a secured electronic system;

[2C] authenticating the user with at least one of [1] the wearable device, [2] a remote server via cellular communications supported by the telecommunications carrier access identification module and the cellular RF communications module, and [3] the secured electronic system via the secured, short-range RF communication; and
[2D] providing the user with access to or through the secured electronic system once authenticated;
[2E] wherein said wearable device includes a GPS module for determining location of the wearable device user with respect to the secured electronic system, and
[2F] wherein the step of providing a user access to or through the secured electronic systems is also dependent on the location of the wearable device user.
Claim 3
[3PRE]: A method for enabling a wearable device user to access secured electronic systems, said method comprising:
[3A] placing a wearable device in contact with a user, said wearable device including [1] a telecommunications carrier access identification module, [2] a cellular RF communications module, and [3] a short-range RF communications module;
[3B] achieving secured, short-range RF communication between the wearable device and a secured electronic system;
[3C] authenticating the user with at least one of [1] the wearable device, [2] a remote server via cellular communications supported by the telecommunications carrier access identification module and the cellular RF communications module, and [3] the secured electronic system via the secured, short-range RF communication; and
[3D] providing the user with access to or through the secured electronic system once authenticated;
[3E] wherein said wearable device further comprises a registration module,

[3F] wherein providing a user access to or through the secured electronic system is determined by at least one of the wearable device and the registration module based on at least one of: [1] the user authenticated for access to secured electronic system by the wearable device, [2] the user biometrically authenticated for access by a wireless carrier, [3] the user biometrically authenticated for access by remote server, [4] the user granted access based on location, and [5] the user granted access based on proximity to a secured electronic system.

Claim 4

[4PRE] The method of claim 2,

[4A] wherein said wearable device further comprises a smartwatch including a microphone and skin illumination and measurement hardware,

[4B] wherein authentication of the user is based on biometric information obtained from the user via at least one of the microphone and the skin illumination and measurement hardware.

Claim 5

[5PRE] The method of claim 1,

[5A] wherein said wearable device further comprises a GPS module for determining location of the wearable device user with respect to secured electronic systems, and

[5B] wherein access to the secured electronic systems is dependent on the location of the wearable device user in relationship to the secured electronic systems.

Claim 6

[6PRE] The method of claim 3,

[6A] wherein said wearable device further comprises a smartwatch including a microphone and skin illumination and measurement hardware,

[6B] wherein authentication of the user is based on biometric information obtained from the user via at least one of the microphone and the skin illumination and measurement hardware.

Claim 7

[7PRE] A method for enabling a smartwatch user to access secured electronic systems, said method comprising:

[7A] placing a smartwatch in contact with a user, the smartwatch including a registration module, a short-range RF communications module, a microphone, and skin illumination and measurement hardware;

[7B] achieving secured, short-range RF communication between the smartwatch and a secured electronic system;
[7C] authenticating the user with at least one of the smartwatch and the secured electronic system using at least one biometric obtained from at least one of the microphone and the skin illumination and measurement hardware;
[7D] providing the user with access to or through the secured electronic system once authenticated; and
[7E] a subscriber identification module (SIM) and a cellular communications module, wherein authentication of the user is also achievable by accessing a remote server via cellular communications supported by the SIM and the cellular communications module and matching the at least one biometric.
Claim 8
[8PRE] The method of claim 7,
[8A] wherein the smartwatch wearable device includes a GPS module for determining location of the smartwatch user with respect to the secured electronic system, and
[8B] wherein the step of providing a user access to or through the secured electronic systems is also dependent on a location of the smartwatch user with respect to a location of the secured electronic system.
Claim 9
The method of claim 8, wherein providing a user access to or through the secured electronic system is determined by the registration module based on at least one of: [1] user authentication for access to secured electronic system by smartwatch, [2] user biometric authentication by a wireless carrier, [3] user biometric authentication by remote server, [4] user location, and [5] user proximity to a secured electronic system.

APPENDIX A MATERIALS CONSIDERED

Exhibit	Description
1001	U.S. Patent No. 10,362,480 (“the ’480 patent”)
1002	Prosecution History of U.S. Patent No. 10,362,480
1006	Exhibit to Plaintiff’s Preliminary Infringement Contentions, <i>SmartWatch Mobileconcepts, LLC v. Google LLC</i> , 6:23-cv-00398 (W.D. Tex.) (now Case No. 3:24-cv-00937-RFL (N.D. Cal.) due to transfer) (as filed 11/9/2023)
1007	U.S. Patent No. 9,684,778 (“Tharappel”)
1008	U.S. Patent Application Publication No. 2003/0046228 (“Berney”)
1009	U.S. Patent Application Publication No. 2014/0196131 (“Lee”)
1010	U.S. Patent No. 9,836,900 (“Jun”)
1011	U.S. Patent Application Publication No. 2015/0028996 (“Agrafioti”)
1012	U.S. Patent Application Publication No. 2016/0155281 (“O’Toole”)
1013	U.S. Patent No. 8,943,580 (“Fadell”)
1014	U.S. Patent Application Publication No. 2010/0178866 (“Jalkanen”)
1015	Plaintiff’s Response to Defendant’s Motion To Dismiss, <i>Smartwatch Mobileconcepts, LLC v. T-Mobile USA, Inc.</i> , No. 6:23-400, Doc. 16 (W.D. Tex.)
1016	Plaintiff’s Response to Defendant’s Motion To Dismiss, <i>SmartWatch Mobileconcepts, LLC v. Google LLC</i> , No. 6:23-00398, Doc. 21 (W.D. Tex.) (now Case No. 3:24-cv-00937-RFL (N.D. Cal.) due to transfer)
1018	U.S. Patent No. 8,208,867
1019	U.S. Patent Application Publication No. 2002/0188210
1020	U.S. Patent No. 8,781,569
1021	U.S. Patent No. 6,178,343
1022	U.S. Patent No. 6,192,253
1023	Defendant Google LLC’s Opening Claim Construction Brief, <i>SmartWatch Mobileconcepts, LLC v. Google LLC</i> , No. 6:23-00398,

	Doc. 34 (W.D. Tex.) (now Case No. 3:24-cv-00937-RFL (N.D. Cal.) due to transfer)
1024	U.S. Patent No. 8,825,011
1025	U.S. Patent No. 8,781,475
1026	U.S. Patent No. 9,743,279
1027	U.S. Patent No. 6,185,157
1028	U.S. Patent No. 7,391,677
1029	U.S. Patent No. 7,889,085
1030	Toshiyo Tamura, et al., “Wearable Photoplethysmographic Sensors—Past and Present,” Electronics, 3:282-302 (2014)
1031	Yuka Maeda, “The Advantages of Wearable Green Reflected Photoplethysmography,” J. Medical Sys. 35:829-834 (2010)
1032	U.S. Patent No. 8,851,372
1033	U.S. Patent No. 5,708,422
1034	Lieber, “A Two-Step Plan to Stop Hackers,” The New York Times (2014)
1035	U.S. Patent No. 8,111,589
1036	U.S. Patent No. 8,467,272
1037	U.S. Patent Application Publication No. 2015/0304322
1039	Certified Translation of Korean Patent Application 10-2015-0068739 (“Jun-739”)
1041	Merriam-Webster’s Collegiate Dictionary (2006)
1042	“The 25th Edition of the International Symposium on Wearable Computers,” IEEE Pervasive Computing (April-June 2022), available at https://ieeexplore.ieee.org/document/9817040 .
1043	Pascoe, “On the Use of Mobile Tools in Everyday Life,” OZCHI '07: Proceedings of the 19th Australasian conference on Computer-Human Interaction: Entertaining User Interfaces, 39-47 (November 2007).
1044	IT History Society, “Benefon ESC!,” available at https://www.ithistory.org/db/hardware/benefon/benefon-esc

1045	“(Sc)Rolling Down the Highway: Vintage 1927 Analog GPS,” available at https://gajitz.com/scrolling-down-the-highway-vintage-1927-analog-gps/
1046	“Garmin Forerunner,” available at https://trigearlab.com/garmin-forerunner/
1047	“World Geodetic System,” available at https://en.wikipedia.org/wiki/World_Geodetic_System#WGS84
1048	Weiss, “When a Password Is Not a Password,” IEEE Proceedings IEEE International Carnahan Conference on Security Technology, Crime Countermeasures (1990)
1049	Zhang, “Location-based Authentication and Authorization Using Smart Phones,” IEEE Proceedings 11th International Conference on Trust, Security and Privacy in Computing and Communications (2012).
1050	Yuksel, “Biometric Identification Through Hand Vein Patterns,” IEEE Proceedings 2010 International Workshop on Emerging Techniques and Challenges for Hand-Based Biometrics (2010)