

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

**PETITION FOR *INTER PARTES* REVIEW
UNDER 35 U.S.C. §§ 311-319 AND 37 C.F.R. § 42.1 *et seq.***

TABLE OF CONTENTS

I.	MANDATORY NOTICES	1
A.	Real Party-In-Interest – § 42.8(b)(1).....	1
B.	Related Matters – § 42.8(b)(2)	1
1.	United States Patent & Trademark Office	1
2.	District Court Matters	1
C.	Counsel and Service Information – § 42.8(b)(3) and (b)(4)	2
II.	INTRODUCTION	4
III.	CERTIFICATION OF STANDING	5
IV.	TABLE OF GROUNDS	5
V.	THE '480 PATENT	6
VI.	CHALLENGED CLAIMS	7
VII.	PERSON OF ORDINARY SKILL IN THE ART (“POSA”).....	8
VIII.	PROSECUTION HISTORY	8
IX.	CLAIM CONSTRUCTION	9
X.	GROUND 1: CLAIMS 1-6 ARE OBVIOUS OVER AGRAFIOTI ALONE OR WITH BERNEY	11
A.	Agrafioti (EX1011)	11
B.	Berney (EX1008)	14
C.	Agrafioti and Berney	16
D.	Claim 1	19
1.	[1PRE]: “A method for enabling a wearable device user to access secured electronic systems”	19
2.	[1A] “placing a wearable device in contact with a user”	19
a.	[1A-1] “telecommunications carrier access identification module”	20
b.	[1A-2] “a cellular RF communications module”	21
c.	[1A-3] “a short-range RF communications module”	23

3.	[1B] “achieving secured, short-range RF communication between the wearable device and a secured electronic system”	23
4.	[1C] “authenticating the user with at least one of [1C-1] the wearable device, [and] [1C-2] a remote server via cellular communications....”	25
a.	[1C-1].....	26
b.	[1C-2].....	27
5.	[1D] “providing the user with access to or through the secured electronic system once authenticated”	31
6.	[1E] “wherein said wearable device comprises a smartwatch including a microphone and skin illumination and measurement hardware”	31
7.	[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”	33
E.	Claim 2	34
1.	[2E]: “said wearable device includes a GPS module for determining location of the wearable device user with respect to the secured electronic system”	34
2.	[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”	36
F.	Claim 3	37
1.	[3PRE] – [3D]	37
2.	[3E]: “said wearable device further comprises a registration module”	37
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-3] the user biometrically authenticated for access by remote server, [3F-4] the user granted access based on	

	location, and [3F-5] the user granted access based on proximity to a secured electronic system”	38
G.	Claim 4	39
H.	Claim 5	39
I.	Claim 6	40
XI.	GROUND 2: CLAIMS 1-9 ARE OBVIOUS OVER AGRAFIOTI, BERNEY, AND LEE	40
A.	Lee (EX1009)	40
B.	Agrafioti, Berney, and Lee	41
C.	Claims 1-6	42
	1. [1E]/[4A]/[6A]	42
	2. [1F]/[4B]/[6B]	43
D.	Claim 7	43
	1. [7PRE]	43
	2. [7A]	44
	3. [7B]-[7D]	44
	4. [7E]	44
E.	Claim 8	45
F.	Claim 9	46
XII.	GROUND 3: CLAIMS 2, 5, 8 ARE OBVIOUS OVER AGRAFIOTI-JUN	46
A.	Jun (EX1010)	46
B.	Combining Agrafioti and Jun	47
C.	Claims 2, 5, 8	49
	1. [2E]/[5A]/[8A]	49
	2. [2F]/[5B]/[8B]	49
XIII.	GROUND 4: CLAIMS 1-9 ARE OBVIOUS OVER THARAPPEL-BERNEY	50
A.	Tharappel (EX1007)	50
B.	Combining Tharappel and Berney	52

C.	Claim 1	55
1.	[1PRE].....	55
2.	[1A]	56
a.	[1A-1]	56
b.	[1A-2]	56
c.	[1A-3]	57
3.	[1B]	57
a.	Locked Smartphone as SES.....	57
b.	Other Types of SES	58
c.	Achieving Secured, Short-Range RF Communication.....	59
4.	[1C]	60
a.	[1C-1].....	60
b.	[1C-2].....	62
c.	[1C-3].....	62
5.	[1D]	63
6.	[1E].....	64
7.	[1F].....	65
D.	Claim 2	66
1.	[2PRE]-[2D].....	66
2.	[2E].....	66
3.	[2F].....	66
E.	Claim 3	67
1.	[3PRE]-[3D].....	67
2.	[3E].....	67
3.	[3F].....	68
F.	Claim 4	69
G.	Claim 5	70
H.	Claim 6	70

I.	Claim 7	70
1.	[7PRE].....	70
2.	[7A]	71
3.	[7B]-[7D]	71
4.	[7E].....	71
J.	Claim 8	72
K.	Claim 9	72
XIV.	GROUND 5: CLAIMS 1-9 ARE OBVIOUS OVER THARAPPEL- BERNEY-LEE.....	72
A.	Tharappel-Berney-Lee	72
B.	Claims 1-9	74
1.	[1E]/[4A]/[6A]/[7A]	74
2.	[1F]/[4B]/[6B]/[7C]	74
XV.	GROUND 6: CLAIMS 2 AND 4 ARE OBVIOUS OVER THARAPPEL AND JUN	75
A.	Combining Tharappel and Jun	75
B.	Claim 2	76
1.	[2PRE].....	76
2.	[2A]	76
3.	[2B]	77
4.	[2C]	78
5.	[2D]	79
6.	[2E].....	79
7.	[2F].....	80
C.	Claim 4	80
1.	[4A]	80
2.	[4B]	80
XVI.	NO BASIS FOR DISCRETIONARY DENIAL	81
A.	Section 314(a).....	81
1.	Potential for Stay.....	81

2.	Timing of Trial.....	81
3.	Litigation Investment.....	82
4.	Overlap of Issues.....	82
5.	Litigation Defendants.....	83
6.	Other Circumstances.....	83
B.	Section 325(d)	83
1.	Step One: The Petition Advances Art and Arguments Not Previously Considered.	83
2.	Step Two: The Office Erred Materially.....	84
XVII.	CONCLUSION.....	85
XVIII.	CLAIM LISTING.....	88

TABLE OF AUTHORITIES

Cases

<i>10X Genomics, Inc. v. Bio-Rad Labs., Inc.</i> , IPR2020-00087, Paper 9, 16-17 (PTAB Apr. 27, 2020)	58
<i>Advanced Bionics, LLC v. Med-El Elektromedizinische Geraete GmbH</i> , IPR2019-01469, Paper 6, 7-8 (Feb. 13, 2020).....	83, 84
<i>Altiris, Inc. v. Symantec Corp.</i> , 318 F.3d 1363 (Fed. Cir. 2003)	60
<i>Apple Inc. v. Fintiv, Inc.</i> , IPR2020-00019, Paper 11 (Mar. 20, 2020)	81, 82
<i>Apple, Inc. v. Evolved Wireless LLC</i> , No. IPR2016-01177, 2017 WL 6543970 (P.T.A.B. Dec. 20, 2017)	10
<i>BMW of North America v. Michigan Motor Techs.</i> , IPR2023-01224, Paper 15, 11 (Feb. 15, 2024).....	81, 82
<i>Brown v. 3M</i> , 265 F.3d 1349 (Fed. Cir. 2001)	25, 60
<i>Dish Network LLC v. Broadband iTV, Inc.</i> , IPR2020-01332, Paper 14 (Jan. 27, 2021).....	82
<i>Interactive Gift Exp., Inc. v. Compuserve Inc.</i> , 256 F.3d 1323 (Fed. Cir. 2001)	60
<i>IPXL Holdings, L.L.C. v. Amazon.com, Inc.</i> , 430 F.3d 1377 (Fed. Cir. 2005)	44
<i>Markforged Inc. v. Continuous Composites, Inc.</i> , IPR2022-00679, Paper 7 (Oct. 25, 2022)	82
<i>Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.</i> , 868 F.3d 1013 (Fed. Cir. 2017)	9
<i>Nokia of Am. Corp. v. TQ Delta, LLC</i> , IPR2022-00471, Paper 11, 19-21 (Aug. 18, 2022).....	81

<i>Penumbra, Inc. v. Rapidpulse, Inc.</i> , No. IPR2021-01466, 2023 WL 2605070 (P.T.A.B. Mar. 10, 2023).....	46
<i>Prisua Eng’g Corp. v. Samsung Elecs. Am., Inc.</i> , No. 2021-1960, 2023 WL 4287194 (Fed. Cir. June 30, 2023).....	45
<i>Samsung Elecs. Am., Inc. v. Prisua Eng’g Corp.</i> , 948 F.3d 1342 (Fed. Cir. 2020)	44
<i>Samsung Elecs. Co. v. Netlist, Inc.</i> , IPR2022-00063, Paper 13 (May 5, 2022).....	83
<i>Sand Revolution II v. Continental Intermodal Group–Trucking</i> , IPR2019-01393, Paper 24, 7 (June 16, 2020).....	81
<i>SuperGuide Corp. v. DirecTV Enterprises Inc.</i> , 358 F.3d 870 (Fed. Cir. 2004)	10
<i>Thorne Research v. Trs. of Dartmouth Coll.</i> , IPR2021-00491, Paper 18, 8-9 (Aug. 12, 2021).....	84
<i>Uber Techs. v. LBT IP II</i> , IPR2020-00880, Paper 8, 13 (Dec. 7, 2022)	83
Statutes	
35 U.S.C. § 102	6, 46
35 U.S.C. § 103	5
35 U.S.C. § 119(a)	46
35 U.S.C. § 314(a)	81
35 U.S.C. § 325(d)	83
Regulations	
37 C.F.R. § 42.100(b)	9
37 C.F.R. § 42.104(a).....	5

Other Authorities

83 Fed. Reg. 51,340 (Nov. 13, 2018)	9
---	---

APPENDIX LISTING OF EXHIBITS

Exhibit	Description
1001	U.S. Patent No. 10,362,480 (“the ’480 patent”)
1002	Prosecution History of U.S. Patent No. 10,362,480
1003	Declaration of David Williams (“Williams”)
1004	CV of David Williams
1005	Plaintiff’s Preliminary Infringement Contentions, <i>SmartWatch Mobileconcepts, LLC v. Google LLC</i> , Ex. 26-1, Case No. 6:23-cv-00398 (W.D. Tex.) (now Case No. 3:24-cv-00937-TSH (N.D. Cal.) due to transfer) (as filed 11/9/2023)
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)
1017	Docket Sheet, No. 3:24-cv-00937-RFL (N.D. Cal.)
1018	U.S. Patent No. 8,208,867

Exhibit	Description
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,” <i>Electronics</i> , 3:282-302 (2014)
1031	Yuka Maeda, “The Advantages of Wearable Green Reflected Photophethysmography,” <i>J. Medical Sys.</i> 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,” <i>The New York Times</i> (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
1038	U.S. District Courts–Combined Civil and Criminal Federal Court Management Statistics (December 31, 2023), https://www.uscourts.gov/statistics-reports/analysis-reports/federal-court-management-statistics

Exhibit	Description
1039	Certified Translation of Korean Patent Application 10-2015-0068739 (“Jun-739”)
1040	Redline Comparison of Jun and 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)

I. MANDATORY NOTICES

A. Real Party-In-Interest – § 42.8(b)(1)

Google LLC is the real party-in-interest.¹

B. Related Matters – § 42.8(b)(2)

1. United States Patent & Trademark Office

U.S. Patent No. 10,362,480 (“the ’480 patent”) was filed on August 11, 2016 as Application No. 15/234,565. The ’480 patent claims priority to U.S. Provisional Patent Application No. 62/204,050 filed August 12, 2015. U.S. Patent Application No. 16/512,607 claims the benefit of priority to Application No. 15/234,565.

The ’480 patent has never been challenged in an *inter partes* review proceeding.

2. District Court Matters

The ’480 patent is asserted against Petitioner in the following case: *SmartWatch Mobileconcepts, LLC v. Google LLC*, 3:24-cv-00937-RFL (N.D. Cal.). The case was filed May 24, 2023 as 6:23-cv-00398 (W.D. Tex.) and transferred to the Northern District of California on February 16, 2024 as 3:24-cv-00937.

¹ Google LLC is a subsidiary of XXVI Holdings Inc., which is a subsidiary of Alphabet Inc. XXVI Holdings Inc. and Alphabet Inc. are not real parties-in-interest to this proceeding.

The '480 patent has also been asserted by Patent Owner against:

- Philips North America LLC (6-22-cv-00572 (W.D. Tex) and 6-23-cv-00775 (W.D. Tex));
- Cellco Partnership d/b/a Verizon Wireless (6-23-cv-00731 (W.D. Tex.));
- Epson America, Inc. (6-23-cv-00397 (W.D. Tex.));
- Timex Group USA, Inc. (6-23-cv-00399 (W.D. Tex.));
- T-Mobile USA, Inc. (6-23-cv-00400 (W.D. Tex.));
- Casio America, Inc. (1-22-cv-04658 (S.D.N.Y.));
- Qualcomm Incorporated (6-22-cv-00569 (W.D. Tex.));
- Apple Inc. (6-22-cv-00570 (W.D. Tex.)); and
- Samsung Electronics America, Inc. (6-22-cv-00571 (W.D. Tex.)).

C. Counsel and Service Information – § 42.8(b)(3) and (b)(4)

Lead Counsel	Elisabeth Hunt (Reg. No. 67,336)	
Backup Counsel	Elizabeth A. DiMarco (<i>pro hac vice</i> application forthcoming) Thomas F. Foley (Reg. No. 76,384)	
Service Information	<u>E-Mail:</u>	EHUNT-PTAB@wolfgreenfield.com Elizabeth.DiMarco@wolfgreenfield.com TFOLEY-PTAB@wolfgreenfield.com
	<u>Post & Hand-Delivery:</u>	Wolf, Greenfield & Sacks, P.C. 600 Atlantic Avenue Boston, MA 02210-2206

	<u>Telephone:</u>	617-646-8000
	<u>Facsimile:</u>	617-646-8646

A power of attorney is submitted with this petition. Counsel for Petitioner consents to service of all documents via electronic mail.

II. INTRODUCTION

Petitioner requests *inter partes* review of claims 1-9 of the '480 patent. 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. 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; EX1003 (“Williams”), ¶¶51-52, 34-50.

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. Williams, ¶53. 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. Williams, ¶¶53, 34-50.

As this Petition demonstrates, it would have been obvious over one or more of the references relied on herein to arrange well-known hardware components and authentication techniques in the claimed manner, and POSAs would have expected success in doing so. All challenged claims should be found unpatentable.

III. CERTIFICATION OF STANDING

The '480 patent is available for IPR and Petitioner is not barred or estopped from requesting IPR of its claims. 37 C.F.R. §42.104(a).

IV. TABLE OF GROUNDS

The challenged claims are unpatentable under 35 U.S.C. §103 over the following grounds.

Ground	Reference(s)	Claim(s)
1	Agrafioti (EX1011), Berney (EX1008)	1-6
2	Agrafioti, Berney, Lee (EX1009)	1-9
3	Agrafioti, Jun (EX1010)	2, 5, 8
4	Tharappel (EX1007), Berney (EX1008)	1-9
5	Tharappel, Berney, Lee	1-9
6	Tharappel, Jun	2, 4

The above-identified references are prior art as follows:

Reference	Priority	Publication	Prior-Art Basis
Tharappel	12/28/2013	6/20/2017	§102(a)(2)
Berney	8/28/2001	3/6/2003	§§102(a)(1)-(2)
Lee	1/7/2013	7/10/2014	§§102(a)(1)-(2)
Jun	5/18/2015	12/5/2017	§102(a)(2)
Agrafioti	7/25/2013	1/29/2015	§§102(a)(1)-(2)

V. THE '480 PATENT

The '480 patent enables “a wearable device user to access” SESes (EX1001, 2:47-63) based on user authentication performed by one or more of several disclosed authentication techniques (EX1001, Abstract, 3:4-4:3). 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.

The claimed authentication techniques include biometric authentication (voice, heart rate pattern) and relative location authentication (user location in relation to the SES). EX1001, 3:4-4:3, 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.

VI. CHALLENGED CLAIMS

Claims 1-9 are reproduced in the Claim Listing (*infra* §XVIII). 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.

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.

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.

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

A POSA would have 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. References to POSAs herein are as of August 12, 2015, the claimed priority date.

VIII. PROSECUTION HISTORY

During prosecution, original claims 9-19 were elected in response to a restriction requirement. EX1002, 76, 82. 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 would be allowable if rewritten in independent form. EX1002, 61-62.

Applicants then canceled then-pending independent claims and rewrote then-pending dependent claims 10-12, 17 as independent claims, with the dependent

claim limitations now recited in steps [E]-[F] for each rewritten claim. EX1002, 47-50. Thus, independent claims 1-3, 7 share limitations from the original independent claims and differing limitations [E]-[F] from the rewritten dependent claims. EX1002, 24-25.

IX. CLAIM CONSTRUCTION

Claim terms are construed herein according to their ordinary meaning in light of the specification and prosecution history. 37 C.F.R. §42.100(b). The Board need only construe terms to the extent necessary to resolve parties' disputes.² *Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017); 83 Fed. Reg. 51,340, 51,353 (Nov. 13, 2018).

One claim phrase ("at least one of ... and") warrants express interpretation in applying the prior art here. Each challenged claim includes the phrase "at least one of" followed by a list of options joined by "and." Under Federal Circuit precedent, "at least one" followed by "and" is presumed to have a conjunctive meaning *only*

² In the parallel District Court litigation, Petitioner asserted that "authenticating the user" must be performed before "providing the user with access to or through the [SES] once authenticated" as recited. EX1023, 4. The Board need not resolve that dispute, as the Petition's prior art discloses performing these two steps in the recited order.

when it “precedes a series of categories” with multiple possible values. *SuperGuide Corp. v. DirecTV Ent’s*, 358 F.3d 870, 886 (Fed. Cir. 2004).

The *SuperGuide* presumption does not apply here because the ’480 patent does *not* use “at least one of” before a series of categories that can each have multiple values. Instead, in the challenged claims, “at least one of” appears either before a list of single-valued conditions/options (e.g., “authenticating the user with at least one of” various optional authentication methods)³ 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”).⁴ *Apple v. Evolved Wireless*, IPR2016-01177, 2017 WL 6543970, *4 (P.T.A.B. Dec. 20, 2017) (*SuperGuide* inapplicable “when the listed items following ‘at least one of’ are not categories containing many possible values”). In the parallel district-court litigation, Patent Owner interprets “at least one of” to have a disjunctive meaning. *See* EX1006, 7.

³ The ’480 patent expressly refers to these listed items as “conditions.” *See* EX1001, 6:64, 7:15-16.

⁴ Even if the *SuperGuide* presumption did apply, the surrounding claim language and specification rebut it by describing the conditions/options as alternatives or requiring only “at least one.” *See, e.g.*, EX1001, 6:55-65, 7:14-16.

Every time “at least one of” is used in the challenged claims, the term has a disjunctive meaning—i.e., the claim is met when one or more of the listed items is present. Williams, ¶¶61-66.

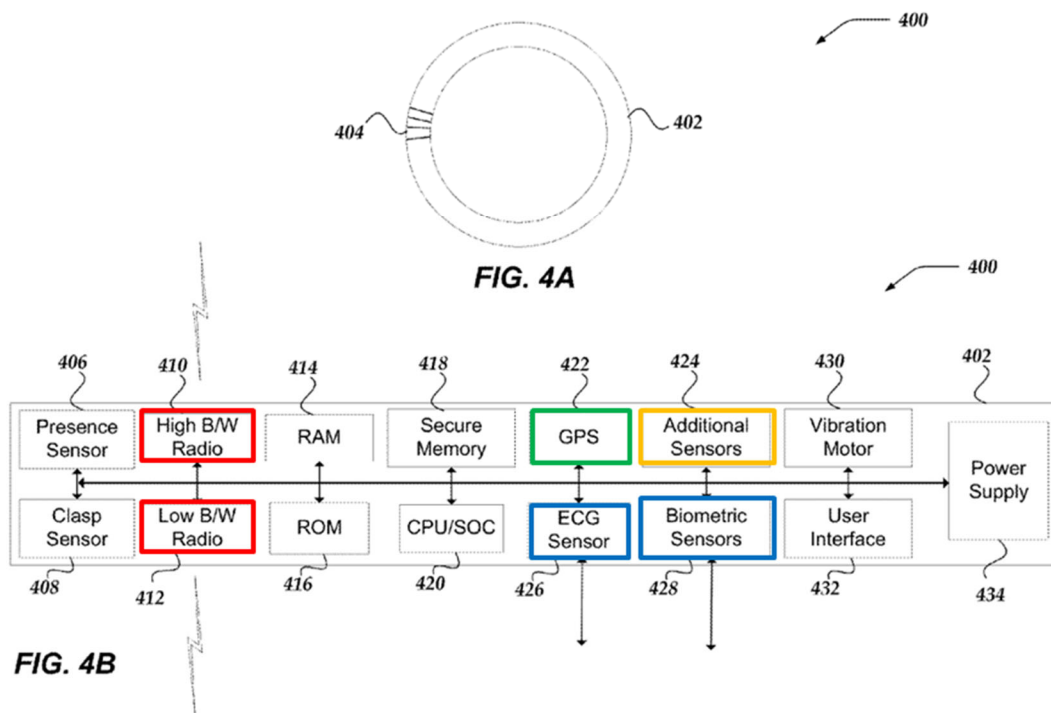
X. GROUND 1: CLAIMS 1-6 ARE OBVIOUS OVER AGRAFIOTI ALONE OR WITH BERNEY

A. Agrafioti (EX1011)⁵

Agrafioti is directed to a user authentication system “centered around a wearable biometric device that authenticates the wearer based on one or more unique biometric characteristics” ([0055]-[0057]). Abstract, [0032]-[0034], [0044]-[0045], [0089]. Agrafioti’s system allows authenticated users 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.” [0029]-[0030], [0093]-[0096], [0104]-[0107], [0155]-[0171], [0196]-[0198]; Williams, ¶68.

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

⁵ All unspecified citations in this section are to EX1011.



Figs. 4A-4B (annotated). Biometric sensors include “microphones, near infrared sensors, light sensors,” “photoplethysmogram sensors,” and others including “optical sensors.” [0122]. Additional sensors (424) include motion, proximity, and GPS sensors. [0109], Figs. 4A-4B. “These additional sensors may provide ... the location of the wearable device and/or proximity to trusted environments.”⁶ *Id.*, [0096], [0112], [0121]; Williams, ¶¶69-72.

⁶ 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]; Williams, ¶¶72, 126-128 (discussing corroborating evidence).

Agrafioti describes multiple ways of user authentication, including by the wearable itself, by an authorized authentication device (“AAD”) communicating with the wearable, and/or by a biometric authentication server communicating with the wearable and 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 “biometric signals and/or data” that may be used “to uniquely identify the user”), [0124]. Agrafioti also describes creating a “unique biometric profile” storable on the wearable or AAD to authenticate a user or pre-authenticate the wearable. [0055], [0095], [0102]-[0103], [0140]-[0153], [0196], Fig. 7; Williams, ¶73.

Agrafioti also teaches that wearable biometric “devices may be arranged to employ additional non-biometric security factors,” such as passwords, Personal Identification Numbers (PINs), gestures, voice commands, finger taps, “a distance between the preauthorized biometric device and the at least [one] access point, [or] one or more additional biometric features.” [0035], [0153]; Williams, ¶74.

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 specified range” or distance of an access point. [0096], [0167]; Williams, ¶75.

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. During prosecution of the ’480 patent, the examiner found that Agrafioti expressly discloses limitations [PRE]-[D] and anticipated the then pending independent claims. Applicants did not disagree. Although the examiner stated that dependent claims containing what matured into limitations [E]-[F] “would be allowable if rewritten in independent form” (EX1002, 62), the examiner erred as explained *infra* §XVI.B.2. Limitations [E]-[F] are at least obvious over Agrafioti, as demonstrated below.⁷ Williams, ¶¶76-80. To the extent Agrafioti alone does not render obvious limitations relating to using GPS-acquired location information, those steps would have been obvious based on Berney.

B. Berney (EX1008)⁸

Berney teaches using a wearable to authenticate user identity and authorize the authenticated user for “wireless transaction” uses such as “car parking at a public

⁷ Other grounds herein demonstrate these limitations are also obvious over Agrafioti in view of secondary references.

⁸ Unspecified cites in this section are to EX1008.

parking meter” ([0036]), gaining authorized entry to a restricted area ([0037]), and other use cases, with “no discernable limit” on its wireless-transaction uses ([0035]). *See* EX1008, [0001]. Berney describes a watch (Fig. 1) wearable that “provides a biometric data reader” ([0028]-[0029]) and includes “other functional circuitry” such as a GPS receiver ([0039]-[0040]). [0012], [0032]; Williams, ¶81.

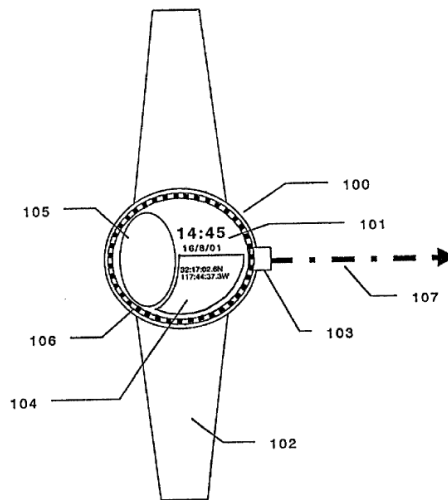


FIGURE 1

Like Agrafioti, Berney describes authenticating the user via the wearable. *E.g.*, [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. [0034] (noting that “requiring multiple levels” of security provides “virtually ironclad” security for “a single, specific user”), [0035]-[0040]; Williams, ¶82.

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.” EX1008, [0040] (such a configuration makes “forgery” of the wearable “much more difficult”); Williams, ¶83. POSAs would have understood that these disclosures teach 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 for the purpose of providing “backup” proximity information. Williams, ¶83. POSAs would have been familiar with determining a wearable user’s location with respect to a device or system (e.g., SES) by comparing their relative GPS coordinates. Williams ¶83; EX1008, [0040]; EX1026, 5:4-14, 6:65-7:2, 10:8-45, 12:31-66, Fig. 5.

C. Agraftoti and Berney

Long before 2015, many user authentication techniques in electronic devices including wearables were known to POSAs, including authentication with passcodes, passwords, biometric data, and location and proximity metrics.

Williams, ¶¶84-88; EX1011, [0003]; EX1008, [0002]-[0010]. POSAs also would have been familiar with using multiple authentication techniques together to enhance security. *See* EX1010, 13:49-14:5; EX1033, 3:4-14, 16:3-14; EX1034.

It would have been obvious to combine Berney’s teachings regarding GPS location and proximity information with Agrafioti’s system and method. Each reference describes wearables with sensors (including biometric sensors), short-range communication capabilities, and GPS capabilities. Further, each reference describes user authentication with biometric data and contemplates using location and/or proximity data as an additional security measure before providing users access to secured (e.g., locked) data or areas. EX1011, [0055]-[0057], [0096], [0167]; EX1008, [0028]-[0029], [0038]-[0041].

Based on Agrafioti’s teachings that its wearable biometric devices may “employ *additional non-biometric security factors* for preauthorizing an enrolled device” (EX1011, [0153]⁹) 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]). Williams, ¶86. Further, POSAs would have understood

⁹ ***Bold italics*** herein are added unless otherwise indicated. *Plain italics* indicate challenged claim language.

that Berney's location and proximity authentication techniques are alternative options for authentication consistent with Agrafioti's teachings. Williams, ¶86; EX1008, [0037]-[0038], [0040]; EX1011, [0003]; §X.E.1 (discussing multifactor authentication and implementation of Berney).

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," "an authorized person seeking entry into a restricted entry area" ([0036]-[0037])). Williams, ¶87.

POSAs would have reasonably expected success combining Agrafioti and Berney as described above. Williams, ¶88. Both Agrafioti and Berney describe wearable devices with a GPS receiver having similar form factors (e.g., watches) and similar platforms (including processors, memory, biometric readers, and antennas). EX1011, Fig. 4B, [0089], [0104], [0112]-[0115], [0121]; EX1008, Fig. 6, [0029], [0039]-[0040]. Further, implementation of GPS location technology, including how to configure and program a wearable using GPS location was then well-understood by POSAs. Williams, ¶88; EX1027, Abstract; EX1028, 4:61-67; EX1029, 1:25-35, 3:61-63.

D. Claim 1

Agrafioti alone or combined with Berney renders obvious claim 1. Williams, ¶¶89-123.

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

Agrafioti discloses methods for authenticating a wearable user before allowing the user to access an “access point.” EX1011, [Abstract], [0029]-[0030], [0054], [0093]-[0096], [0104]-[0107], [0155]-[0171], [0196]-[0198]; Williams, ¶91. Agrafioti’s “access points” are examples of “secured electronic systems,” as demonstrated *infra* §X.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.*” Williams, ¶91.

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

Agrafioti uses biometric wearable devices including “any device that can be worn by a user and is capable of obtaining a biometric signal,” such as wristwatches or bracelets. EX1011, [0044], [0089], [0114]-[0115], Fig. 4A-4B. Agrafioti further teaches, and POSAs would have understood, that the wearable includes sensors in physical contact with the user. EX1011, [0099] (wearable’s “electrodes make[] contact with the wrist”); *id.*, [0091], [0107], [0124]; EX1008, [0032] (corroborating POSAs’ background knowledge regarding wrist-worn wearables like Agrafioti’s); Williams, ¶91. Thus, Agrafioti’s method places the wearable “*in contact with a*

user” as claimed. Williams, ¶91; EX1001, 6:33-36 (contact includes “placement” on wrist).

a. [1A-1] “telecommunications carrier access identification module”

Agrafioti’s wearable communicates with client computers 102-105 over a wireless network 108. EX1011, [0044]-[0049], [0117], Fig. 1 (below).

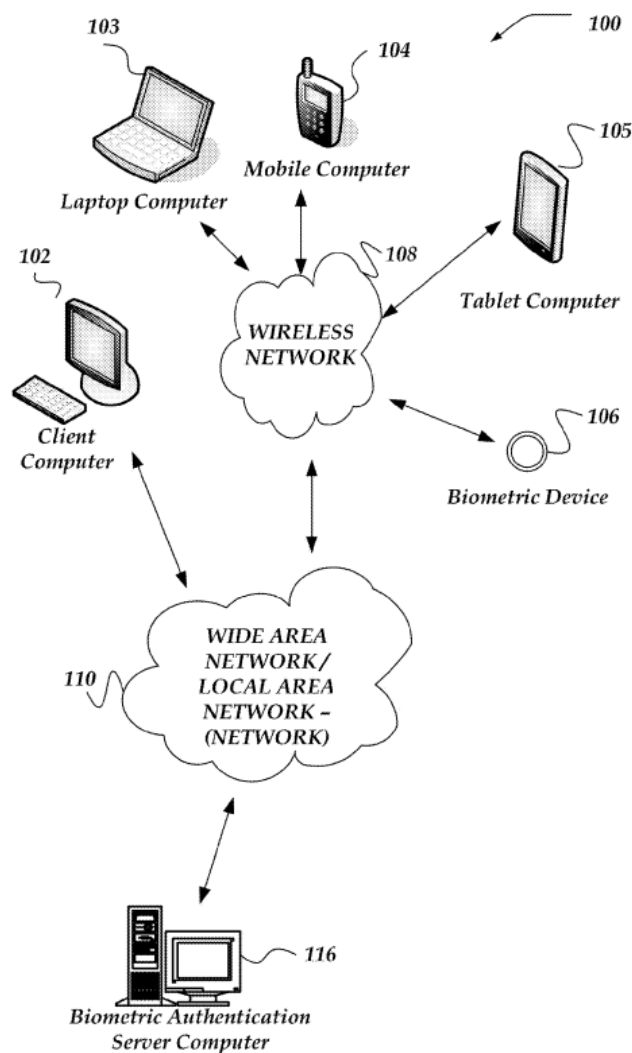


Fig. 1. “[W]ireless network 108 may include virtually any wireless communication mechanism by which information may travel between client computers 103-105,

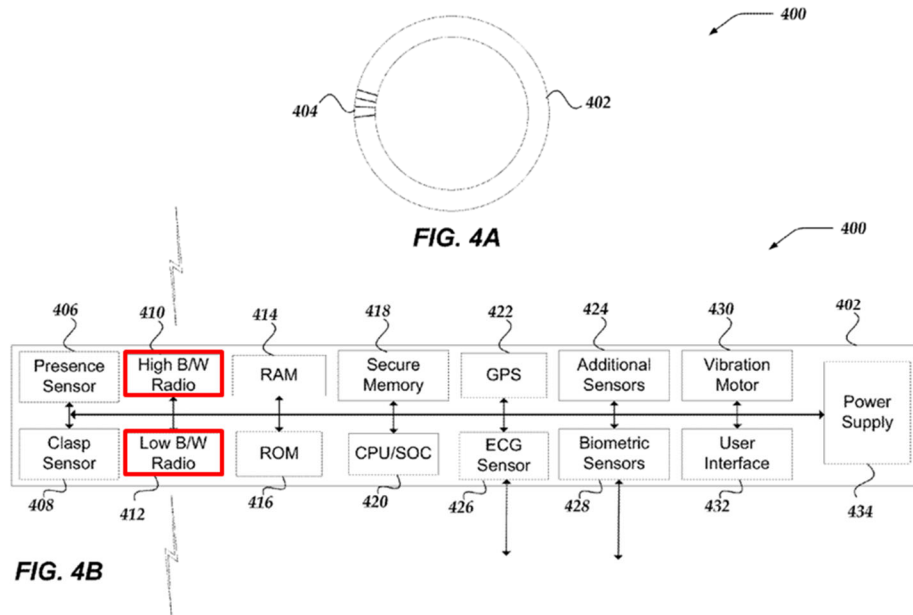
biometric device 106, and another computer network.” EX1011, [0049] (also discussing “cellular” communication such as 2G/3G/4G/5G for network 108).

Agrafioti ([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 “*telecommunications carrier access identification module[s]*” as claimed. EX1001, Abstract, 2:21-34, 4:4-15; Williams, ¶¶92-94.

b. [1A-2] “a cellular RF communications module”¹⁰

Agrafioti’s wearable device has radios, transceivers, and/or antennae enabling communication with other devices. EX1011, [0095], [0105], [0113]-[0115], Figs. 4A-4B (annotated below); Williams, ¶¶95-96.

¹⁰ “RF communications” means “radio frequency communications.” EX1001, 5:33; EX1041; Williams, ¶95.



For example, wearable 400 includes high bandwidth radio transceivers 410 that use “high bandwidth mechanisms such as Wi-Fi, or the like” to “communicate with various devices,” including “biometric servers and cloud services.” EX1011, [0117]. The transceiver may be coupled to a dipole or other antenna “to facilitate the transmission and reception of wireless signals.” EX1011, [0104]. The wearable communicates with biometric servers and cloud services (e.g., server 116) via networks 108 and 110, where network 108 may employ 2G/3G/4G/5G “*radio* access for *cellular* systems.” EX1011, [0049], Fig. 1. Therefore, POSAs would have understood that the wearable’s high bandwidth radio transceivers 410 alone or coupled with antenna(e) comprise a “*cellular RF communications module*” as

claimed. EX1001, 5:31-37; Williams, ¶¶95-96; EX1011, [0047]-[0050]; EX1022, 1:9-2:28.

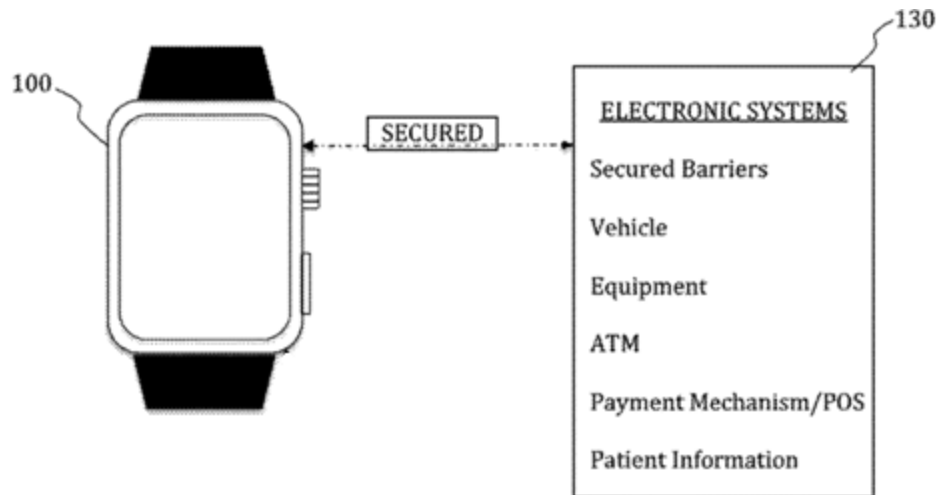
c. [1A-3] “a short-range RF communications module”

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, 6:41-45; EX1014, [0002]-[0003] (NFC); EX1018, 1:24-28 (Bluetooth); Williams, ¶¶97-98.

Agrafioti’s 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.” EX1011, [0117], [0030], [0094]-[0096], [0165]-[0166]; EX1014, [0013] (Bluetooth is a short-range communication technology). Thus, Agrafioti’s wearable includes “*a short-range RF communications module*” (e.g., low bandwidth radio transceiver 412) as claimed. Williams, ¶¶97-98.

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

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, Fig. 2; Williams, ¶¶99-102.



Agrafioti discloses the same type of secured, short-range RF communication between a wearable biometric device and “access points.” EX1011, [0030], [0166]. For example, Agrafioti’s 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.” EX1011, [0030], [0049], [0166], [0196]-[0199]; Williams, ¶¶99-102.

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.” EX1011, [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” and “proof of payment systems.” *Id.* Agrafioti’s “access points” are thus “*secured electronic systems*” as claimed. EX1001, 2:63-3:3 (SESeS include secured doors, parking meters, point-of-sale systems and secured databases); Williams ¶101.

Additionally or alternatively, as discussed *supra* §X.C, 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” and “an authorized person seeking entry into a restricted entry area” ([0036]-[0037])). Williams, ¶102. All such applications achieve “*secured, short-range RF communication between the wearable device*” and the types of SESeS expressly discussed in the ’480 patent. Williams, ¶102; EX1001, 2:60-3:3. Thus, Agrafioti modified in view of Berney satisfies [1B] for this additional reason. Williams, ¶102.

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

Agrafioti discloses “authenticating the user with” two of [1C]’s disjunctive alternatives, which is sufficient to satisfy [1C]. *See Brown v. 3M*, 265 F.3d 1349, 1352 (Fed. Cir. 2001) (satisfaction of one or more of a list of disjunctive options is sufficient for invalidity); *see* §IX ([1C] is disjunctive); Williams, ¶¶103-115.

a. [1C-1]

Agrafioti describes “authenticating users *using biometric devices.*” EX1011, [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. EX1011, [0028], [0089]-[0091], [0095], [0124]; Williams, ¶104. Agrafioti’s user’s biometric profile may be created “in the wearable biometric device itself” and stored on the wearable “to authenticate the user” ([0102]-[0103], [0124]). Williams, ¶¶104-106.

For example, Agrafioti teaches that a user “may be authenticated” by the wearable device using the wearable’s biometric sensors. EX1011, [0091] (biometric sensors capture “biometric signals and/or data... to uniquely identify the user”); *see also id.*, [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.” EX1011, [0028], [0091], [0124]. Alternatively or additionally, Agrafioti teaches authentication by the wearable by entering a password or PIN, the same type of user authentication by the wearable described in the ’480 patent. *Compare* EX1011, [0035] *with* EX1001, 3:11-15, 6:58-61; *see also* Williams, ¶¶105-106.

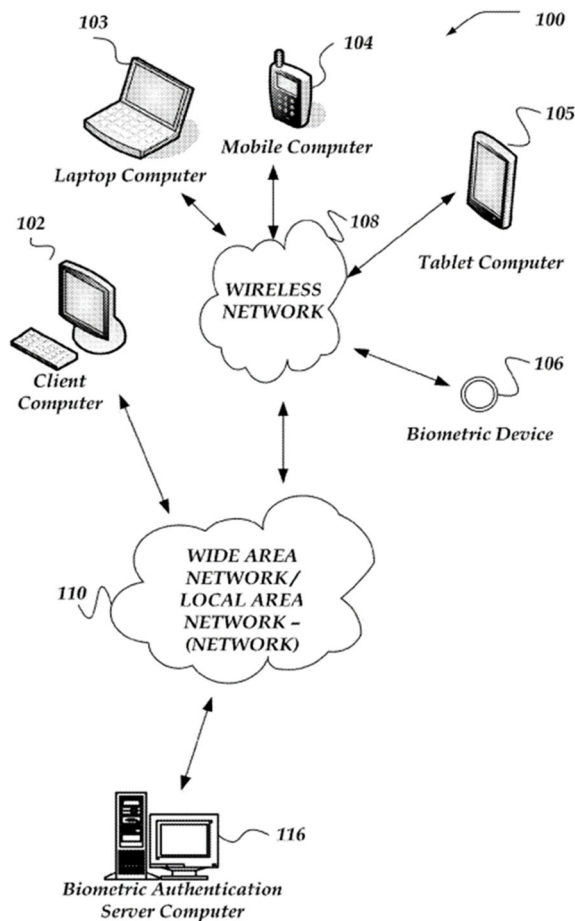
Thus, Agrafioti teaches multiple ways of authenticating the user “*with the wearable*” as claimed. Williams, ¶106.

b. [1C-2]

Agrafioti teaches authenticating the user by remote server in two ways. Williams, ¶¶107-115.

(1) User Authentication Through Biometric Authentication Server.

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.” EX1011, [0053], [0180], Fig. 1 (excerpt below); Williams, ¶¶108-111.



The user's biometric profile may be stored alternatively or additionally in this biometric authentication server. EX1011, [0211]; Williams, ¶¶109-110. Agrafioti thus describes embodiments in which the wearable transmits biometric data acquired by the wearable's sensors to biometric authentication server 116 for user authentication. EX1011, [0044]-[0045], [0052]-[0053].

The wearable communicates with biometric authentication server 116 via wireless network 108 and network 110. EX1011, [0047]-[0050], Fig. 1. Wireless network 108 includes 2G/3G/4G/5G "radio access for cellular systems" (EX1011, [0049]) which is supported by the wearable's modules that meet [1A-1]-[1A-2] as

discussed *supra* §§X.D.2.a-X.D.2b. Thus, authentication by Agraftoti's biometric authentication server 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. Williams, ¶111.

(2) User Authentication Through the AAD. In another embodiment (e.g., Fig. 7), the user's biometric profile is stored on an AAD that “may be separate from the biometric” wearable. EX1011, [0033], [0100]-[0103], [0132]-[0135], [0137]-[0138]. The wearable transmits biometric feature(s) it captured to an AAD that performs user authentication. EX1011, [0142]-[0150].

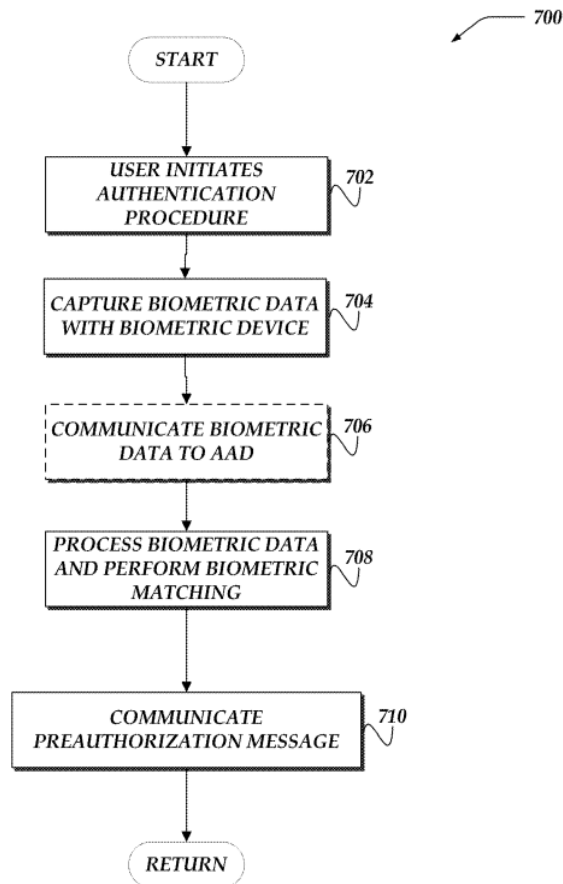


FIG. 7

Specifically, the AAD compares received biometric features to the stored biometric profile “that corresponds to the user.” EX1011, [0033], [0037], [0138], [0142]-[0150], [0219], Fig. 7.

If the features received by the AAD correspond to a user’s stored biometric profile, the wearable biometric “may be preauthorized for the user.” EX1011, [0033], [0037], [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. EX1011, [0055], [0146]-[0149], [0152], [0160]-[0162].

The wearable communicates with the AAD via “radios/transducers,” and the AAD may be one of client computers 103-105 with which the wearable communicates over network 108 (including cellular communications supported by the wearable’s modules that meet [1A-1]-[1A-2] as discussed *supra* §§X.D.2.a-X.D.2.b). EX1011, [0039], [0093]; Williams, ¶¶112-115. POSAs would therefore have understood that the corresponding authentication satisfies [1C-2]. Williams, ¶115.

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

Agrafioti describes granting the user access to an “access point” (i.e., the SES as claimed) after authenticating the user. EX1011, [0107], [0148], [0154]-[0163], Fig. 8 (showing authorization followed by enabling user access to one or more access points); Williams, ¶¶116-117. Thus, Agrafioti’s method provides the user access to the SES “*once authenticated*,” as claimed. Williams, ¶117.

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

Agrafioti describes a “wristwatch” wearable ([0044]) and teaches that the wearable includes a microphone and recognizes 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]). Williams, ¶118. POSAs would have understood that a wristwatch wearable as described in Agrafioti is a “*smartwatch*” including a microphone as claimed. Williams, ¶118.

Agrafioti teaches that the wristwatch wearable may include “photoplethysmogram sensors” and discusses near infrared sensors, light sensors, and optical sensors. EX1011, [0122]. 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 and measurement hardware*”—because they emit light (or other optical output) and measure a response to that light/illumination. Williams, ¶119.

Agrafioti teaches that the biometric wearable device (e.g., smart wristwatch) performs biometric authentication via pulse detection ([0108], [0116]). POSAs would have understood that PPG was a common and conventional implementation of pulse detection typically involving 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 Williams, ¶¶120-121; EX1030, 283-84 (PPG pulse sensing using “reflection from or transmission through the tissue”); EX1031, 829-30 (PPG pulse monitoring using “a light source to illuminate the skin tissue, and

a photodetector to measure small variations in light intensity”); EX1019, [0005] ; EX1020, 7:13-28; EX1021, 1:8-56.

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 biometric wearable devices (e.g., smart wristwatch) including a pulse detection light source and measurement sensor have “*skin illumination and measurement hardware*” as claimed. Williams, ¶¶121-122.

7. [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”

As discussed *supra* (§§X.D.4 (1[C]), X.A), Agrafioti describes biometric user authentication which may be performed by the wearable device, by a remote authentication server, or by an AAD. Williams, ¶123. In any implementation, the biometric user authentication may be based on voice/voiceprint or pulse detection. EX1011, [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* §X.A). Williams, ¶123. Additionally, for the reasons discussed *supra* §X.D.6 (1[E]), POSAs would have

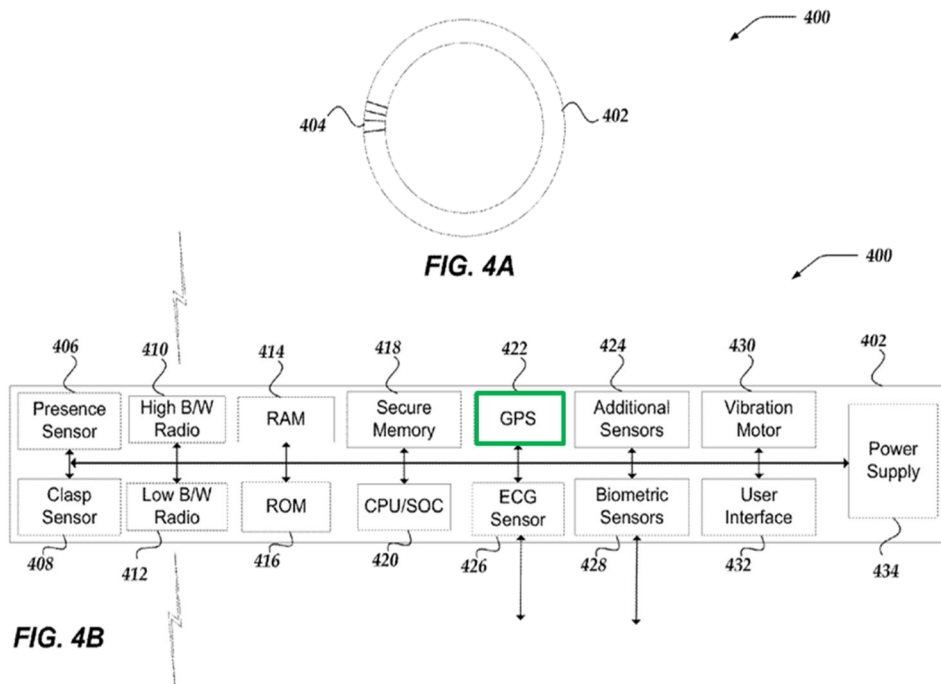
understood from Agrafioti and their knowledge and experience that pulse detection biometric authentication includes acquiring biometric information (the user's pulse patterns) from the skin illumination and measurement hardware (e.g., PPG-related sensors). Williams, ¶¶123. Thus, Agrafioti satisfies [1F]. *Id.*

E. Claim 2

[2PRE]-[2D] are identical to [1PRE]-[1D]. Agrafioti alone or combined with Berney satisfies [2PRE]-[2D] for the reasons discussed *supra* §§X.D.1-X.D.5. Williams, ¶¶124-135.

1. [2E]: “said wearable device includes a GPS module for determining location of the wearable device user with respect to the secured electronic system”

Agrafioti's wearable includes a GPS transceiver 422, which “may represent the radios, hardware, and instructions (e.g., software) for receiving geo-location.” EX1011, [0121], [0109], [0112]-[0115], Figs. 4A-4B (annotated below).



“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.” EX1011, [0121]. Agrafioti thus discloses “a *GPS module for determining location of the wearable device*” as claimed. Williams, ¶¶129-130.

To the extent Agrafioti does not expressly teach that the GPS module is for “*determining location of the wearable device user **with respect to the [SES]***,” it would have been obvious to configure Agrafioti’s wearable to do so in view of Agrafioti alone, or in combination with Berney in the manner discussed *supra* §X.C. Williams, ¶¶131-132.

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. Williams, ¶132. 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.*” EX1011, [0167], [0095]-[0096], [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.

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].*” Williams, ¶¶132-133; EX1011, [0112].

2. [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”

Agrafioti teaches that the wearable provides “access control” based on “*determination of proximity/range of the wearable biometric device to the access point.*” EX1011, [0167], [0095]-[0096], [0106], [0112], [0169], [0187], [0194]. 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. Williams, ¶¶134-135.

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 §§X.C, X.E.1 ([2E]), and Agrafioti’s teachings that access control is based on the proximity of the wearable to an access point. Williams, ¶135. For example, it would have been obvious to POSAs to configure Agrafioti in view of Berney such that access to the SES is granted only when the wearable’s GPS location indicates that the wearable is in a particular location (and additionally close to the access point). Williams, ¶135.

F. Claim 3

1. [3PRE] – [3D]

[3PRE]-[3D] are identical to [1PRE]-[1D]. Agrafioti alone or combined with Berney satisfies [3PRE]-[3D] for the reasons discussed *supra* §§X.D.1-X.D.5. Williams, ¶¶136-140.

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

The ’480 patent states that the registration module (a.k.a. “electronic system registration module”) is “for registering secured electronic devices.” EX1001, 4:12-13, Abstract. 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.

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 that will exist “onboard the biometric device” and be “checked to determine” permissions. EX1011, [0034], [0174], [0179]; Williams, ¶¶137-138. Agrafioti’s list of accessible/inaccessible access points (or the software that accesses/uses it) is the type of “*registration module*” claimed including because the wearable receives the information and “registers” the access points by listing them with accessible/ inaccessible status. Williams, ¶138; EX1011, [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-3] the user biometrically authenticated for access by remote server, [3F-4] the user granted access based on location, and [3F-5] the user granted access based on proximity to a secured electronic system”**

[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. Access may be provided by the wearable device, the registration module, or both. *Supra* §§IX. Agrafioti satisfies “*providing a user access to or through the secured electronic*

system” at least by the wearable for the reasons discussed in §X.D.5. Williams, ¶¶139-140.

Agrafioti satisfies [3F-1] for substantially the same reasons as [1C-1]—*“authenticating the user with ...the wearable device.”* See §X.D.4.a; Williams, ¶140. For substantially the same reasons discussed *supra* §X.D (Claim 1) Agrafioti also discloses or renders obvious at least “[3F-3] *the user biometrically authenticated for access by remote server*” (§X.D.4.b); “[3F-4] *the user granted access based on location*” (§§X.E.1.-X.E.2); and “[3F-5] *the user granted access based on proximity to a secured electronic system*” (§§X.E.1.-X.E.2).

G. Claim 4

Claim 4 depends from claim 2 and recites the identical requirements of [1E]-[1F]. Agrafioti alone or combined with Berney satisfies claim 4 for the reasons discussed *supra* §§X.D.6-X.D.7. Williams, ¶141.

H. Claim 5

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 4 for substantially the same reasons discussed *supra* §§X.E.1-X.E.2. Claim 5 differs from [2F] by further reciting the clause *“in relationship to the [SESeS].”* Agrafioti combined with Berney satisfies this requirement at least because the combination discussed *supra* §X.C requires that “accurate location

information” from a GPS receiver “agree with proximity communications devices in order to authenticate a transaction” (EX1008, [0040]), which is “*location ... in relationship to the [SEses]*” as claimed. Williams, ¶142.

I. Claim 6

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

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

A. Lee (EX1009)

Lee describes a wrist wearable such as a watch with contact sensors “for authenticating a user based on a wrist vein pattern.” EX1009, [0003]. Wrist contact sensors have an array of illuminators and sensors on a surface of the watch that is opposite the user’s wrist when the device is worn. EX1009, [0031]. “The illuminators [] produce illumination in the infrared spectrum which is directed into the skin of the palmar side of the wrist.” EX1009, [0031], [0036]. The wrist contact sensor obtains “digital data representing a wrist vein pattern for the user.” EX1009, [0003]. The user’s wrist vein pattern is compared to stored wrist vein pattern information to authenticate the user. EX1009, [0005], [0070]. The digital data may be encrypted and transferred for authentication of the user. EX1009, [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 security or monitoring of activity over time.” EX1009, [0026]; Williams, ¶144.

B. Agrafioti, Berney, and Lee

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]). Williams, ¶¶145-146. 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 the user’s wrist as taught by Lee (EX1009, [0031], [0036]) to obtain “digital data representing a wrist vein pattern for the user” (EX1009, [0003], [0005], [0070]). Williams, ¶145.

POSAs would have had such motivation to implement Agrafioti’s wearable itself and/or as modified in view of Berney (as discussed *supra* §X.C) to obtain vein patterns based on Lee’s teachings. Williams, ¶146. Both options are collectively discussed herein as “Agrafioti-Berney-Lee.” POSAs would have reasonably expected success in implementing 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). EX1011, Fig. 4B, [0089], [0104],

[0112]-[0115], [0121]; EX1008, [0028]-[0029], [0032], claim 2; EX1009, [0005], [0070]; Williams, ¶146.

C. Claims 1-6

To the extent that Agrafioti alone or combined with Berney does not satisfy the “*skin illumination*” claim requirements of claims 1-6 (i.e., [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 *supra* §§X.D-X.I. Williams, ¶¶147-151.

1. [1E]/[4A]/[6A]

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 *supra* §X.A. EX1011, [0044], [0089], [0099]; Williams, ¶148.

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]; Williams, ¶149; *supra* §XI.A-XI.B. Agrafioti-Berney-Lee’s array of illuminators and sensors comprise “*skin illumination and measurement hardware,*” as claimed. Williams, ¶¶148-149; EX1009, [0030]-[0031], [0058].

2. [1F]/[4B]/[6B]

Agrafioti-Berney-Lee satisfies [1F]/[4B]/[6B] for the reasons discussed *supra* §X.

Agrafioti-Berney-Lee additionally implements Lee’s teaching that its array of illuminators is illuminated (e.g., sequentially) to illuminate skin of the wrist proximate the illuminators. EX1009, [0036]-[0037]. Thus, from Lee, POSAs would have configured Agrafioti-Berney-Lee’s wearable to generate a user’s biometric profile based on wrist vein pattern data. EX1011, [0028], [0091], [0124]; EX1009, [0038], [0058]; Williams, ¶¶150-151. POSAs would have configured Agrafioti-Berney-Lee to authenticate users by comparing gathered sensed wrist-vein pattern data to a stored wrist-vein pattern biometric profile. EX1009, [0038], [0058]-[0059]; EX1011, [0091]; Williams, ¶151. Agrafioti-Berney-Lee satisfies authenticating the user “*based on biometric information obtained from the user via ...the skin illumination and measurement hardware*” (i.e., [1F]/[4B]/[6B]) for these additional reasons. Williams, ¶¶150-151.

D. Claim 7

1. [7PRE]

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* §X.D.1) and because Agrafioti discloses a smartwatch (*see* §X.D.6([1E])). Williams, ¶152.

2. [7A]

Agrafioti-Berney-Lee discloses placing a wearable device in contact with a user (§X.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 (EX1011, [0109]); §§X.F.2 ([3E]), X.D.2.c ([1A-3]). Finally, including [4] skin illumination and measurement hardware was obvious as discussed in §X.D.6 ([1E]). Williams, ¶153.

3. [7B]-[7D]

Agrafioti-Berney-Lee renders obvious [7B]-[7D] for the reasons discussed *supra* §§X.D.3 ([1B]), X.D.4 ([1C]), X.D.7 ([1F]), and X.D.5 ([1D]), respectively. Williams, ¶154.

4. [7E]¹¹

Limitation [7E] recites “*a subscriber identification module (SIM) and a cellular communications module.*” Agrafioti discloses cellular communications and

¹¹ [7E] renders claim 7 indefinite because it recites an apparatus when claim 7 is a method claim. *See IPXL Holdings v. Amazon.com*, 430 F.3d 1377, 1384 (Fed. Cir. 2005); *Samsung v. Prisia Eng’g*, 948 F.3d 1342, 1355 (Fed. Cir. 2020). *IPXL-type*

includes a “*telecommunications carrier access identification module*” and “*cellular RF communications module*,” as discussed *supra* §§X.D.2.a-X.D.2.b ([1A-1]-[1A-2]). *See* EX1011, [0047], [0049]. POSAs would understand that including a SIM was a well-known implementation for Agrafioti’s telecommunications carrier access identification module for identifying the device to implement a cellular wireless connection. Williams, ¶155-157. Indeed, the ’480 patent admits that smartwatches incorporating SIMs were known. EX1001, 1:43-47; *see* Williams, ¶¶156-157 (discussing EX1032, 8:16-17).

The biometric data may be transferred via a secure wireless connection. EX1011, [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

Claim 8 depends from claim 7 and recites substantively the same requirements of claim 5 except that claim 8 specifically recites a “*smartwatch*.” Williams, ¶158. Agrafioti-Berney-Lee satisfies claim 8 for the same reasons that Agrafioti-Berney

indefiniteness does not preclude instituting IPR. *See Prisia Eng’g v. Samsung*, 2021-1960, 2023 WL 4287194, *2 (Fed. Cir. June 30, 2023).

satisfies claim 5, and because Agrafioti’s wearable includes a smartwatch. *Id.*; *supra* §§X.D.6, X.H.

F. Claim 9

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 *supra* §§X.D.4, X.F.3. Williams, ¶159.

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

A. Jun (EX1010)

Jun qualifies as prior art pursuant to §102(a)(2) because it (1) meets the “ministerial requirements for claiming priority to” an earlier application; and (2) the earlier application describes the same subject matter from Jun that Petitioner relies upon. *Penumbra, Inc. v. Rapidpulse, Inc.*, No. IPR2021-01466, 2023 WL 2605070, *14 (P.T.A.B. Mar. 10, 2023) (precedential). Williams, ¶¶160-162.

Jun meets the “ministerial requirements” because it claims priority under § 119(a) to Korean Patent Application 10-2015-0068739 (“Jun-739”) (filed May 18, 2015) and was timely filed within one year of the filing of Jun-739. EX1010, 1:7-11. Further, a certified translation of Jun-739 (EX1039) and a redline comparison of Jun-739 and Jun (EX1040) show that Jun-739 contains the Jun disclosures relied upon in this Petition. *See Penumbra*, 2023 WL 2605070, *14.

Jun describes a wearable (e.g., smartwatch) that transmits short-range RF signals to unlock a target object (e.g., vehicle) as shown in Figure 9. EX1010, Abstract, 4:65-5:5, 6:65-7:9, 8:20-56, 11:53-57, 13:49-57; Williams, ¶¶161-162.

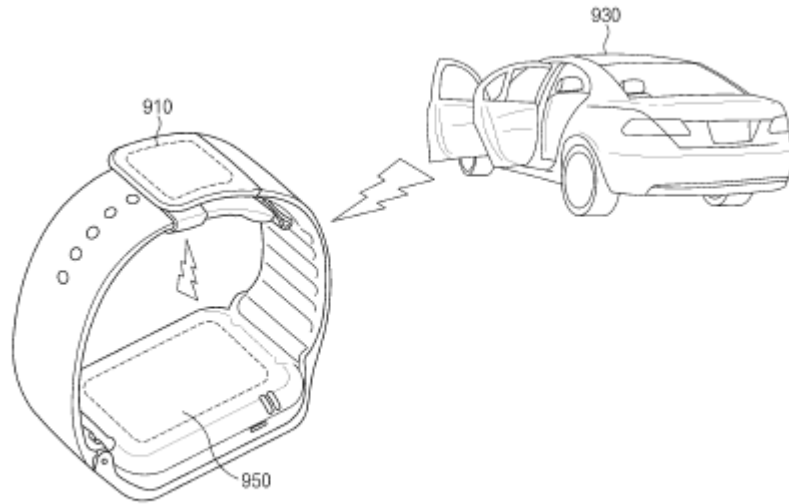


FIG. 9

Jun describes using the wearable to extract authentication information from the target object and then determine “whether the target object [] is an authenticated object.” EX1010, 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.” EX1010, 14:10-61, 8:6-7. Jun teaches using its wearable’s GPS sensor to “detect[] an approach of the smart key [] to the target object” and unlock the target. EX1010, 15:10-16.

B. Combining Agrafioti and Jun

POSAs would have had reasons to combine Agrafioti’s wearable and Jun’s location-based access control (e.g., door unlocking) technique (“Agrafioti-Jun”).

Agrafioti and Jun each describe a wearable device having GPS capabilities 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. EX1011, [0109], [0112], [0121], [0163]-[0164]; EX1010, 4:65-5:10, 14:32-61, 15:10-16; Williams, ¶163.

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. EX1010, 15:10-16; EX1011, [0210] ("[A] user may be restricted or enabled access to access points based on geolocation."); *supra* §X.A, XII.A. For example, POSAs would have been motivated to apply Jun's teachings to Agrafioti to provide additional security. *See* EX1010, 13:49-14:5 (explaining that its techniques provide ways to authenticate a user before permitting access to a secured system); *see* EX1033, 3:4-14, 16:3-14 (corroborating POSA's background knowledge of security benefits of controlling "entry door to a secure room" using claimed two-factor authentication); EX1034, 2 (multifactor authentication "add[s] to the consumer's security"); Williams, ¶164.

POSAs would have reasonably expected success in modifying Agrafioti's system and method to include Jun's GPS-based techniques, including because implementing GPS location technology in a wearable was well understood by POSAs long before the '480's priority date. Williams, ¶165. 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. *See* EX1010, 11:53-57, 13:49-53.

C. Claims 2, 5, 8

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 §§X.E, X.H, XI.D, XI.E and Jun's teachings discussed below respecting limitations [2E]-[2F], [5A]-[5B], and [8A]-[8B]. Williams, ¶166.

1. [2E]/[5A]/[8A]

Jun's wearable, like Agrafioti's, includes a GPS module for determining location of the wearable user. EX1010, 7:47-49, 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). EX1010, 15:10-16 (wearable detects "approach ...to the target object"); *see* §X.E.1 ([2E]); Williams, ¶167.

2. [2F]/[5B]/[8B]

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. EX1010, 15:10-23 ("lock releasing function"; "opening of a door"); *see* §X.E.2 ([2F]); ¶168.

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

A. Tharappel (EX1007)

Tharappel describes 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). EX1007, 1:14-29, 2:16-4:15 (discussing challenges associated with the “proliferat[ion]” of wearables); Williams, ¶¶169-175.

Figure 1 depicts an example trust group with two smart devices: wearable 40 and smart device 20. EX1007, 2:24-26.

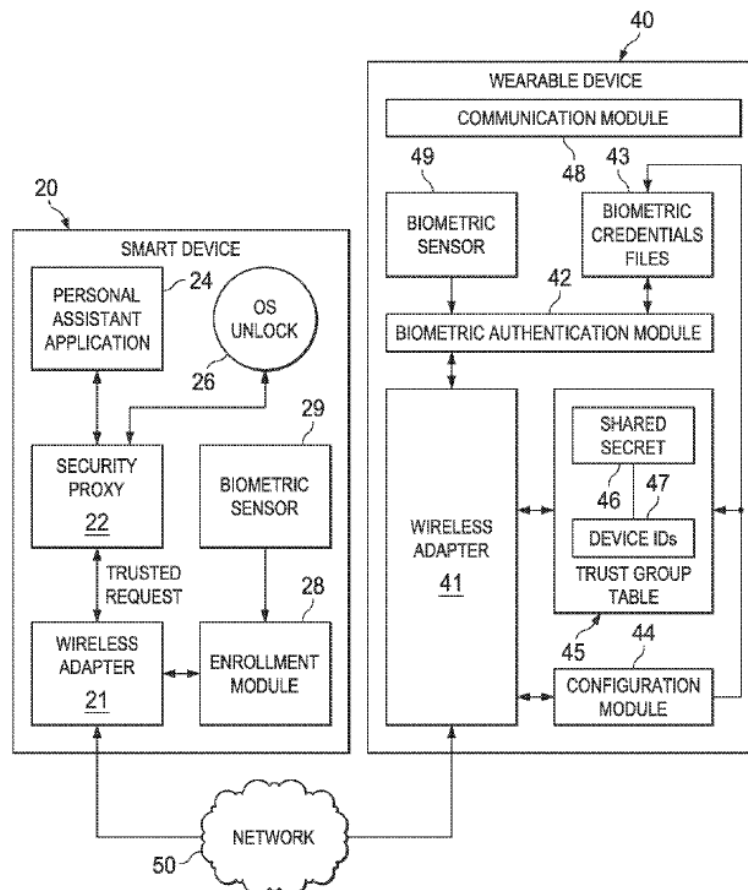


FIG. 1

Wearable 40 is “any smart device capable of voice audio, media, or data exchanges” (3:14-20), including a watch or bracelet (3:58-61). Wearable 40 has biometric authentication capabilities. EX1007, 2:28-29; 3:58-61; Williams, ¶¶170-171.

Wearable 40 and smartphone 20 communicate “via a secure network 50.” EX1007, 2:26-27, Fig. 1. Smart device 20 and wearable 40 include “respective wireless adapters 41 and 21” that include “wireless communication circuitry” such as Wi-Fi, Bluetooth, NFC, satellite, and/or any cellular technologies (including “3G/4G/5G/nG”). EX1007, 4:50-5:30; Williams, ¶172.

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, palm prints, and “pulse features.” EX1007, 6:31-41; Williams, ¶173. Biometric sensors 29, 49 are any suitable sensor for sensing the desired biological characteristic (e.g., “a pulse sensor” to sense pulse features). EX1007, 6:41-49; Williams, ¶173. Wearable 40 includes “biometric authentication module 42” (2:28-29), which allows the user to “authenticate[] to the wearable device based on” one or multiple user-specific biometric credentials (4:16-25). EX1007, 2:24-45; Williams, ¶173.

Smart device 20 includes enrollment module 28, which allows the user to enroll his/her biometric characteristic “to enable biometric authentication.” EX1007, 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. EX1007, 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].” EX1007, 18:14-18; Williams, ¶174.

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. *Infra* §§XIII.D2-XIII.D.3; Williams, ¶175.

B. Combining Tharappel and Berney

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. Williams, ¶¶176-183. 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. Williams, ¶176; EX1007, 1:14-31, 3:21-43, 4:20-28; EX1008, [0002]-[0010], [0026]-[0027], [0038]; EX1013, 1:15-33, 1:54-2:50.

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. EX1008, [0040]; Williams, ¶177. Berney discloses that using location and/or proximity information *in addition* to biometric-based authentication beneficially makes "forgery...much more difficult." Williams, ¶177; EX1008, [0029], [0040].

Tharappel teaches that a wearable device configured for biometric authentication may also be "configured to accept other types of authentication credentials." EX1007, 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. Williams, ¶178; EX1008, [0037]-[0038], [0040].

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). Williams, ¶179; EX1008, [0038]; EX1007, 3:55-58.

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," "an authorized person seeking entry into a restricted entry area" ([0036]-[0037])). Williams, ¶180.

POSAs would have reasonably expected success in implementing the above-described Tharappel-Berney combination, e.g., with the system described in Tharappel, (e.g., smart device 20, wearable device 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. Williams, ¶181; EX1008, Fig. 6, [0039]; EX1007, Figs. 10-11, 19:13-14.

Both Berney and Tharappel describe wearable devices that include a GPS component and perform user authentication. EX1007, 19:18-44; EX1008, [0029], [0040]. Thus, POSAs would have expected success in implementing proximity authentication with GPS backup in Tharappel's wearable based on Berney's teachings. Williams, ¶182. Such a modification could be implemented with software modifications to use GPS location data for authentication. Williams, ¶182. Further, implementing GPS location technology in wearables was well understood

by POSAs by 2015. Williams, ¶182; *see* EX1027, Abstract; EX1028, 4:61-67; EX1029, 1:25-35, 3:61-63.

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 (EX1008, [0035]-[0037])), at least because Tharappel already discloses a flexible understanding of smart devices including e.g., “embedded controllers, car infotainment systems, navigation systems” (EX1007, 3:4-13) and uses proximity of the wearable device to the smart device as part of forming a secure connection. EX1007, 4:16-20, 18:3-6; Williams, ¶183.

C. Claim 1

1. [1PRE]

To the extent [1PRE] is limiting, Tharappel-Berney satisfies it via Tharappel’s methods (augmented by Berney’s techniques discussed *supra* §§X.B, X.D.1) for using “[a] *wearable* electronic *device*” to provide “*users*” with “*secure*, convenient *access* to multiple smart *electronic* devices,” including smartphones. EX1007, 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. EX1007, 4:28-41, 6:62-7:15; Williams, ¶184. As explained *infra* §X.D.3, Patent Owner argues that locked smartphones are SESes. Further,

even under a narrower interpretation of SES, Tharappel-Berney satisfies [1PRE].
See §§X.D.1, X.D.3; Williams, ¶184.

2. [1A]

Tharappel-Berney satisfies [1A] because Tharappel-Berney’s “*wearable device*...can be worn by a user” in contact with (“by attachment to”) a user’s “body part.” EX1007, 3:14-20, 14:15-19, 14:49-50, Fig. 3B. Tharappel-Berney’s wearable can be a bracelet or watch, which POSAs understood (and Berney corroborates) to be worn in contact with the user. Williams, ¶185; EX1008, [0032] (“a sensor...on the back of watch 100...could read body temperature” or “vein patterns on the wearer’s wrist”).

a. [1A-1]

Tharappel-Berney satisfies [1A-1] via the wearable’s “subscriber identity module (SIM) I/F 1030.” Williams, ¶186; EX1007, 15:28-32, 16:51-55, 17:35-39, 19:12-45. According to the ’480 patent, a “SIM” is a 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; Williams, ¶186.

b. [1A-2]

Tharappel-Berney’s wearable includes Tharappel’s “wireless adapter[,],” including circuitry for communications via “*cellular* technologies (e.g., 3G/4G/5G/nG), other *radio frequencies* ...and/or any other networking protocols

that facilitate wireless *communications*.” EX1007, 4:50-5:8, 5:9-30, 19:27-45, Fig. 1. Tharappel-Berney’s “wireless adapter” with at least “3G” “cellular technologies” is a “*cellular RF communications module*” as claimed. Williams, ¶¶187-188; EX1001, 5:31-37 (discussing cellular RF communications module using GSM or CDMA); EX1024, 7:48-50 (corroborating that 3G cellular used CDMA); EX1025, 6:36 (corroborating same).

c. [1A-3]

In addition to the “*cellular communications module*” (e.g., wireless adapter configured for 3G/4G/5G/nG cellular communications), 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*.” EX1007, 4:50-5:30, 19:27-45, Fig. 1, 5:28-30; EX1001, 2:6-10, 5:22-25, 6:23-45; EX1014, [0013]; Williams, ¶¶189-190.

3. [1B]

Tharappel-Berney satisfies [1B] in two alternative ways. Williams, ¶¶191-195.

a. Locked Smartphone as SES

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. In district court, Patent Owner 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”); *see also* EX1015, 6-7 (“[T]he mobile phone is a[n SES] accessible by the accused watch.”); *id.* (“Access to or through the [SES] occurs during pairing of the accused watch to the mobile phone.”). Patent Owner should be held to that interpretation here. *See 10X Genomics v. Bio-Rad Labs.*, IPR2020-00087, Paper 9, 16-17 (PTAB Apr. 27, 2020) (judicial efficiency enhanced by allowing Petitioner to rely upon claim construction Patent Owner relies upon in district court). Williams, ¶192.

Under Patent Owner’s interpretation of SES, Tharappel-Berney’s locked smartphone (e.g., smart device 20) is an SES. EX1007, 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.”); Williams, ¶¶192-193. 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 “security proxy 22” electronically unlocks it. EX1007, 2:49-51, 6:64-7:6, 7:38-53, 8:4-7.

b. Other Types of SES

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 into a restricted entry area” ([0037]), and “paying for a store-bought purchase by the use of” a wearable device ([0035]).

Supra §XIII.B. Tharappel-Berney’s “wireless transactions” are the ***exact same types*** of SESes expressly discussed in the ’480 patent. EX1001, 2:60-3:3 (providing examples of SESes: “secured entry barriers (e.g., doors, gates, safes),” payment mechanisms (e.g., vending machines, parking meters), point-of-sale (POS)); Williams, ¶194.

c. Achieving Secured, Short-Range RF Communication

Tharappel-Berney’s “wearable device 40 communicates with a smart device 20 via a ***secure*** network 50.” EX1007, 2:24-45, 4:16-49 (“When 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.” EX1007, 5:28-30; Williams, ¶195; *see* §X.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. Williams, ¶195; EX1008, [0036]-[0038].

Thus, Tharappel-Berney satisfies [1B]. Williams, ¶195.

4. [1C]

Tharappel-Berney satisfies [1C] if it satisfies any one or more of the three alternatives—[1C-1]-[1C-3]. *Supra* §IX; *Brown*, 265 F.3d at 1352; Williams, ¶¶196-204.

a. [1C-1]

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. EX1007, 6:9-29. The wearable’s biometric sensors can detect “voice patterns, speech, fingerprints, ...hand features, palm prints, and pulse features.” EX1007, 6:30-49, 13:52-14:2, 17:29-18:18; Williams, ¶197. If the “biometric input data” acquired by the sensors matches the user’s previously enrolled biometric credentials, then “authentication is successful.” EX1007, 17:43-18:18; Williams, ¶197. 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, 6:58-61; Williams, ¶¶197-198; *see* §XIII.A.

Claim 1 does not require that the user authentication in [1C-1] be performed *after* the “*secured...communication*” of [1B]. *See Altiris v. Symantec*, 318 F.3d 1363, 1369-70 (Fed. Cir. 2003) (describing two-part test for determining if method claim steps must be performed in the order written); *Interactive Gift Exp., Inc. v.*

Compuserve, 256 F.3d 1323, 1342 (Fed. Cir. 2001) (method claims steps “are not ordinarily construed to require” a specific sequence).

Nothing in the claim language’s “logic or grammar” requires [1B] occur before [1C-1]; Williams, ¶199. 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 id.*, 6:46-53 (authentication before communication).

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 EX1007, 14:57-15:47, 9:46-10:15, 12:12-15, Figs. 4-5. Communication of 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 [1B] and occurs ***before*** the wearable uses those credentials to biometrically authenticate the user. EX1007, 17:46-53. Thus, this implementation of Tharappel-Berney performs step

¹² In other embodiments, the wearable receives the credentials via the cloud rather than directly from the smart device. EX1007, 9:61-64.

[1B] (Tharappel's step 406/502) before Tharappel-Berney performs step [1C-1] (Tharappel's steps 802-804). Williams, ¶200.

b. [1C-2]

Tharappel-Berney authenticates the user with a remote server via cellular communications as recited by [1C-2] for the reasons discussed *infra* §XIII.I.4. Williams, ¶201.

c. [1C-3]

Tharappel-Berney additionally satisfies authenticating the user with the SES via the secured short-range RF communication as recited by [1C-3]. Williams, ¶¶202-204.

Tharappel teaches that a 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.” EX1007, 19:3-11. This is authenticating the user with the SES. Williams, ¶203; EX1007, 2:46-55, 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* EX1007, 8:13-24. Thus, Tharappel’s techniques in Tharappel-Berney meet [1C-3]. Williams, ¶203.

Additionally, Tharappel-Berney includes Berney’s “authorized entry” use case in which the SES is part of the authentication process. EX1008, [0037]-[0038]; Williams, ¶204. In this implementation, the wearable transmits identity data to “a counterpart device” via the Bluetooth RF communication. EX1008, [0037]-[0038]. A “security system associated with the secured area” determines “whether the validly identified user is” authorized. *Id.* Applying Tharappel’s wearable in this use case in Tharappel-Berney additionally meets [1C-3]. Williams, ¶204; *supra* §XIII.A.

5. [1D]

Tharappel teaches that “[w]hen appropriate biometric credentials have been provided, the accessed smart device [SES] can unlock its operating system to allow the user to interact with the smart device.” EX1007, 4:29-31, 2:49-51, 7:6-15. “[U]nlocking” allows users to access “applications data, and/or other capabilities of the smart device.” EX1007, 6:67-7:6; Williams, ¶¶205-207. Unlocking constitutes providing access to/through the SES as claimed. EX1001, 6:38-45; Williams, ¶¶204-205.

Tharappel teaches that a user may be granted access to the SES only after authentication. EX1007, 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. Williams, ¶207. Additionally, based on Berney, it would have been obvious to “*provide the user with access to or through*” Berney’s wireless transaction SEses “*once authenticated*” as claimed. Williams, ¶207; *supra* §X.B.

Tharappel-Berney thus satisfies [1D]. Williams, ¶207,

6. [1E]

Tharappel-Berney includes Tharappel’s “biometric authentication capability” for any type of suitable biometric authentication, such as voice, pulse, or vein pattern (taught by Berney). *See* EX1007, 2:28-29, 3:58-64, 4:16-41, 6:11-49, 9:65-10:32, 13:27-64, 15:4-8, Fig. 1; EX1008, [0036]; Williams, ¶¶208-213. Tharappel-Berney’s wearable thus includes a microphone and voice authentication capabilities as taught by Tharappel. *See* EX1007, 6:44-45 (“microphone can be used to sense a voice” for “voice identification”), 13:30-35, 13:52-56.

Tharappel-Berney’s biometric authentication includes pulse authentication (EX1007, 3:58-64) with appropriate sensors (*id.*, 6:43-48). For example, “a pulse sensor can be used to sense pulse features.” EX1007, 6:43-48. POSAs would have understood that a typical, conventional, and obvious implementation of “a pulse sensor” was a reflection-type pulse sensor (and light emitting and measurement hardware), as discussed *supra* §§X.C, X.D.6. Williams, ¶209.

Thus, Tharappel-Berney satisfies “*skin illumination and measurement hardware*” for substantially the same reasons that Agrafioti-Berney satisfies “*skin illumination and measurement hardware*.” Williams, ¶209.

Additionally, from Berney, POSAs understood that biometric authentication can be based on a user’s wrist “vein patterns.” EX1008, [0032]. 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. Williams, ¶210. For example, POSAs understood that illuminators and measurement sensors were commonly used to collect wrist vein pattern data for authentication purposes. Williams, ¶211 (discussing as corroboration EX1009, [0030]-[0031], [0058]; EX1037, [0040], [0053]; EX1013, 9:48-53). 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* EX1007, 3:61-66, 6:37-41; EX1008, [0032]; Williams, ¶¶212-213; §XI.B.

7. [1F]

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]. Williams, ¶214; *supra* §XIII.C.6. Thus, Tharappel-Berney satisfies [1F].

D. Claim 2

1. [2PRE]-[2D]

[2PRE]-[2D] are identical to [1PRE]-[1D]. Tharappel-Berney satisfies [2PRE]-[2D] for the reasons discussed *supra* §XII.C. Williams, ¶215.

2. [2E]

Tharappel-Berney's wearable includes a GPS module. Williams, ¶¶216-218; EX1007, 19:41-44; EX1008, [0029], [0040]. As discussed *supra* §XIII.B, Tharappel-Berney incorporates Berney's teaching to use the GPS module to acquire absolute location information from at least two devices and compare those locations as back-up for proximity information. EX1008, [0040]; Williams, ¶¶216-217.

Thus, Tharappel-Berney's wearable device can determine the location of the wearable device user with respect to Tharappel-Berney's SESes (including Tharappel's smartphone and Berney's wireless transactions). EX1008, [0040]; Williams, ¶218; §§X.B (Berney), X.E.2 ([2F]), XIII.B (Tharappel-Berney).

3. [2F]

As discussed *supra* §XII.B-.C, Tharappel-Berney implements a comparison of the "very accurate location information" (EX1008, [0040]) 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 make “forgery” more difficult. Williams, ¶¶219-221; EX1008, [0040]. Tharappel-Berney also authenticates the wearable user’s identity. Williams, ¶219; EX1008, [0031].

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 reasons discussed in §§XIII.B, X.E.2, Berney’s teachings that GPS location is “very accurate,” and POSAs’ familiarity with many possible uses of GPS location information. Williams, ¶220. For example, it would have been obvious to POSAs to configure Tharappel-Berney such that access to the SES is granted only when the wearable’s GPS location indicates the wearable is in a particular location. Williams, ¶¶220-221; §X.C (Agrafioti-Berney).

E. Claim 3

1. [3PRE]-[3D]

[3PRE]-[3D] are identical to [1PRE]-[1D]. Tharappel-Berney satisfies [3PRE]-[3D] for the reasons discussed *supra* §§XIII.C.1-XIII.C.5. Williams, ¶222.

2. [3E]

Tharappel-Berney’s wearable includes Tharappel’s trust group table and software to “search[]” the table, which constitute a “*registration module*” as recited by [3E]. Williams, ¶¶223-224; EX1007, 2:36-45, 10:33-65, 18:3-18. Tharappel describes “extending user authentication across a trust group.” EX1007, 2:16-19.

The devices in the trust group are identified within a “trust group table” stored on the wearable device. EX1007, 10:33-37. The trust group table includes a “device ID” of each smart device in the trust group. *Id.* The device ID in Tharappel’s trust group table “can be an index” providing “uniquely identifying information” (e.g., a different shared secret) for each smart device. EX1007, 10:42-46. The shared secret “may be used to secure a wireless connection between [a] wearable device [] and [a] smart device.” EX1007, 10:50-52. Additionally, Tharappel’s “device IDs can be mapped to wireless connection security information.” EX1007, 10:66-11:8.

Presence of a device in the trust group table may be used to determine whether the device is a member of the trust group. EX1007, 18:10-12, 32:19-29. When “the smart device is included in [the] trust group,” an authenticated user can “send a communication to unlock the smart device.” EX1007, 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. Williams, ¶¶223-224.

3. [3F]

[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.*”

Tharappel-Berney can authenticate the user using the wearable device as discussed *supra* §XIII.C.4 ([1C]). Tharappel-Berney can also authenticate the user using the trust group table, *i.e.*, a registration module. Williams, ¶¶225-227; *compare* EX1007, 18:6-16 (when smart device is determined to be in trust group, “*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”).

[3F] next recites that the providing access step is “*based on at least one of*” five disjunctive options. Tharappel-Berney satisfies three of those options, thus rendering limitation [3F] obvious (*supra* §IX): [3F-1] for the reasons discussed *supra* §XIII.C.4.a ([1C-1]); [3F-4] for the reasons discussed *supra* §XIII.D.3 ([2F]); and [3F-5] for the reasons discussed *supra* § XIII.D.3 ([2F]). In each case, “*providing a user access*” is based on the respective authentication, as explained *supra* §XIII.C.5 ([1D]). Williams, ¶227.

F. Claim 4

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

G. Claim 5

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. Williams, ¶229. Tharappel-Berney satisfies claim 5 for the reasons discussed *supra* §§XIII.D.2-XIII.D.3. Williams, ¶229.

H. Claim 6

Claim 6 depends from claim 3 and recites the identical requirements of [1E]-[1F]. Tharappel-Berney satisfies claim 6 for the reasons discussed *supra* §§XIII.C.6-XIII.C.7. Williams, ¶230.

I. Claim 7

1. [7PRE]

[7PRE] is nearly identical to [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. EX1007, 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. *Supra* §XIII.C.1; Williams, ¶231.

2. [7A]

[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 *supra* §XIII.C.2. Williams, ¶232.

3. [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* §§XIII.C.3-XIII.C.5. Williams, ¶233.

4. [7E]

As discussed *supra* §XIII.C.2, Tharappel-Berney includes a SIM and a cellular communications module that support cellular communications. Williams, ¶¶234-236.

Tharappel-Berney's biometric data may be transferred via a secure wireless connection. EX1007, 12:12-29. For example, "the biometric credentials" may be "transferred to the cloud and then transferred to a primary wearable device 60." EX1007, 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. Williams, ¶235. 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. EX1007, 4:59-5:2 (“WiFi” and “cellular technologies”), 5:24-27 (same); Williams, ¶235.

Accordingly, cellular data is a disclosed option, as well as one of a finite number of known, conventional options for accessing the cloud. EX1007, 4:59-5:2, 12:22-25; Williams, ¶¶234-236. 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

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

K. Claim 9

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

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

A. Tharappel-Berney-Lee

Lee provided POSAs reasons to further modify Tharappel-Berney to incorporate Lee’s wrist-vein-pattern biometric authentication techniques discussed *supra* §XI.A (“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 describe in detail a wrist-contact authentication technique as mentioned in Berney. Williams, ¶¶239-241; EX1009, [0005], [0070]; EX1007, 8:53; EX1008, [0032]; *supra* §§XI.A-XI.B. POSAs would have understood that including Lee’s biometric authentication methods furthers Tharappel’s goal of providing “secure, convenient access to” multiple smart devices. Williams, ¶239; EX1007, 3:55-58.

Incorporating Lee’s biometric authentication teachings in Tharappel-Berney-Lee would have been implementing a known biometric authentication method using Lee’s techniques. Williams, ¶240. POSAs would have reasonably expected success in implementing Lee’s wrist-vein-pattern biometric-sensor-based authentication in Tharappel-Berney-Lee’s wearable. Williams, ¶¶240-241. Tharappel, Berney, and Lee each have similar form factors (*e.g.*, watches) and describe similar platforms (including processors, memory, biometric readers, and antennas). Williams, ¶241; EX1009, Fig. 4A, [0045]-[0046]; EX1007, Figs. 10-11, 19:13-14; EX1008, 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, systems, and/or areas. Williams, ¶241. Further, biometric sensors generally and biometric-based

authentication methods were well understood by POSAs by the '480 patent's priority date. *Id.*

B. Claims 1-9

Tharappel-Berney-Lee satisfies claims 1-9 for substantially the same reasons that Tharappel-Berney satisfies claims 1-9. *Supra* §XIII; Williams, ¶¶242-244. 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]/[4A]/[6A]/[7A]

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. Williams, ¶243; *supra* §§XI.A, XI.C.1 ; EX1009, [0030]-[0031], [0058].

2. [1F]/[4B]/[6B]/[7C]

Tharappel-Berney-Lee satisfies [1F]/[4B]/[6B]/[7C] based on Tharappel's microphone and biometric voice authentication capabilities as discussed in §XI.C.2. Williams, ¶244. 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 that illuminate the wrist skin. EX1009, [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.” EX1009, [0058]-[0059]; Williams, ¶244.

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

A. Combining Tharappel and Jun

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 *supra* §XII.A (resulting in “Tharappel-Jun”). Williams, ¶¶245-247. 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. EX1007, 2:16-23, 4:37-41, 19:18-45; EX1010, 14:32-61, 15:10-16. POSAs would have recognized Jun’s techniques as applicable and beneficial to Tharappel. Williams, ¶245.

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* EX1010, 13:49-14:5, 15:10-16; EX1007, 4:16-28; *supra* §X.C (describing recognized benefits of user authentication and security enhancement via multiple authentication mechanisms); Williams, ¶246.

POSAs would have reasonably expected success in modifying Tharappel’s wearable to include Jun’s GPS-based authentication, including because GPS

location technology and authentication methods were well-understood by POSAs long before the '480's invention date. Williams, ¶247. Further, Jun explains a GPS-based, proximity authentication technique is successfully implementable in a wrist-wearable device of the same form as Tharappel's wearable device and with biometric authentication. EX1010, 11:53-57; 13:49-53, 14:37-61.

B. Claim 2

1. [2PRE]

Tharappel-Jun includes Tharappel's system and methods for providing "secure, convenient access to multiple smart electronic devices," including smartphones. EX1007, 3:55-58; *see* §XIII.C.1 ([1pre]). 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. *See* Williams, ¶248; EX1010, 7:52-57, 8:3-56, 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 (similar).

2. [2A]

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. *Supra* §§XIII.A (Tharappel), XV.A (Tharappel-Jun); Williams, ¶249. As discussed in §§XIII.A (Tharappel), XIII.C.2 ([1A]), Tharappel-Jun's method "*places a wearable device in contact with a user*" as claimed. Williams,

¶249. Additionally, Tharappel-Jun’s method of using a wearable includes the circuitry disclosed in Tharappel and discussed in §§XIII.A (Tharappel); XIII.C.2 ([1A]). Thus, Tharappel-Jun satisfies [2A1]-[2A2]. Williams, ¶249.

3. [2B]

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. Williams, ¶250; *supra* §XIII.A. Under Patent Owner’s interpretation of SES, Tharappel-Jun’s locked smartphone (e.g., smart device 20) is an SES. EX1007, 3:4-10, 3:64-65, 4:28-37, 6:62-7:15, 8:4-7; Williams, ¶250.

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” such as a vehicle door or a gate. EX1010, 8:2-10; *see also id.*, 14:9-16. Jun also uses the wearable device to “turn[] on a starter of a vehicle.” *Id.*, 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. EX1001, 2:60-3:3. Thus, Tharappel-Jun satisfies [2B] for this additional reason. Williams, ¶250.

4. [2C]

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]. EX1007, 6:9-49, 13:52-14:2, 17:29-18:18; EX1001, 3:11-15, 6:58-61; Williams, ¶¶251-253; *supra* §XIII.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. EX1007, 14:57-15:47; *see 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. EX1007, 17:46-53. Williams, ¶252.

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." EX1007, 19:3-11; Williams, ¶253; *supra* §XIII.C.4 ([1C]) (discussing Tharappel's "security proxy").

5. [2D]

Tharappel-Jun includes Tharappel's functionality for unlocking the smart phone only after "appropriate biometric credentials" have been provided and verified. EX1007, 4:29-31; *see id.*, 2:49-51, 7:6-15; Williams, ¶254. "[U]nlocking" allows users to access "applications, data, and/or other capabilities of the smart device" (EX1007, 6:67-7:6) and constitutes providing access to/through the SES as claimed (EX1001, 6:38-45). Williams, ¶254. 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. EX1010, 8:3-10, 14:9-61. Thus, Tharappel-Jun satisfies [2D] in two alternative ways. Williams, ¶254.

6. [2E]

Tharappel-Jun's wearable includes "a global positioning system (GPS)." EX1007, 19:18-44. 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). EX1010, 7:47-49, 13:49-57, 14:32-35, 15:10-16; §XV.A (Tharappel-Jun); Williams, ¶¶255-256.

Based on Jun (e.g., EX1010, 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. Williams, ¶256.

7. [2F]

Tharappel-Jun meets [2F] because it implement's Jun's teaching that the wearable "performs a control function," *e.g.*, "a lock releasing function" (EX1010, 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" (EX1010, 15:18-23). Williams, ¶¶257-258. Tharappel-Jun also provides user access *dependent* on the location of the wearable device user as taught by Jun. EX1010, 15:10-23, 15:18-23. Williams, ¶258.

C. Claim 4

1. [4A]

Tharappel-Jun includes Tharappel's biometric authentication using microphone and voice authentication and fingerprint/hand input, as discussed in §XIII.C.6 ([1E]). The claimed biometric authentication was also obvious over Jun's biometric data collection and authentication including fingerprint scan. EX1010, 14:37-61. Thus, Tharappel-Jun meets [4A]. Williams, ¶259.

2. [4B]

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. Williams, ¶260.

XVI. NO BASIS FOR DISCRETIONARY DENIAL

A. Section 314(a)

Under the Director’s Interim Procedure for Discretionary Denials (June 21, 2022), “the PTAB will not deny institution based on *Fintiv*¹³ if there is compelling evidence of unpatentability,” which this Petition provides. That should conclude the *Fintiv* analysis here. *Nokia. v. TQ Delta*, IPR2022-00471, Paper 11, 19-21 (Aug. 18, 2022). Regardless, the *Fintiv* factors also weigh against discretionary denial.

1. Potential for Stay

Petitioner will seek a pre-institution stay of the parallel litigation, but without “specific evidence” how the court will rule, this factor is neutral. *Sand Revolution II v. Continental Intermodal Group–Trucking*, IPR2019-01393, Paper 24, 7 (June 16, 2020) (informative).

2. Timing of Trial

The parallel litigation has been transferred to the Northern District of California with an initial case management conference scheduled for May 22, 2024. No. 3:24-cv-00937-TSH, Dkt. 43 (Mar. 1, 2024). No trial date has yet been set; and the median time to trial is 48.9 months, corresponding to June 2027. EX1017, Dkt. 43; EX1038, 66. Accordingly, the Board’s final written decision will likely issue well before the district court’s trial, weighing against discretionary denial. *BMW v.*

¹³ *Apple v. Fintiv*, IPR2020-00019, Paper 11 (Mar. 20, 2020) (precedential).

Michigan Motor Techs., IPR2023-01224, Paper 15, 11 (Feb. 15, 2024) (“Factor 2 favors institution” where “no trial date was set in district court”).

Regardless, Petitioner filed this petition with diligence. Petitioner’s motion to dismiss is pending and no answer has been filed. EX1017. This factor thus weighs against discretionary denial. *Fintiv*, IPR2020-00019, Paper 11, 11 (where petitions are filed “expeditiously...this fact has weighed against [denial]”); *Dish Network v. Broadband iTV*, IPR2020-01332, Paper 14, 28-29 (Jan. 27, 2021) (instituting and finding reasonable diligence where petition was filed less than three months after receiving identification of asserted claims).

3. Litigation Investment

Other than initial motion practice and preliminary contentions, the parties have invested little in litigating invalidity issues in the district-court litigation, weighing against denial. *BMW*, IPR2023-01224, Paper 15, 11.

4. Overlap of Issues

Petitioner challenges all nine claims of the ’480 patent, whereas patent owner asserts only claim 2 in district court. EX1005-1006. This weighs against denial. *Markforged v. Continuous Composites*, IPR2022-00679, Paper 7, 32-33 (Oct. 25, 2022).

5. Litigation Defendants

Petitioner is the defendant in district court. Because the Board’s decision will likely issue before the district-court trial, this factor weighs against denial. *Uber Techs. v. LBT IP II*, IPR2020-00880, Paper 8, 13 (Dec. 7, 2022).

6. Other Circumstances

The Petition’s “strong evidence on the merits” weighs against denial. Interim Procedure, 3-5.

B. Section 325(d)

Discretionary denial under §325(d) is only applicable where “the same or substantially the same prior art or arguments previously were presented.” 35 U.S.C. §325(d); *Advanced Bionics v. Med-El Elektromedizinische Geraete*, IPR2019-01469, Paper 6, 7-8 (Feb. 13, 2020) (precedential) (“AB”).

1. Step One: The Petition Advances Art and Arguments Not Previously Considered.

The Office has never considered the patentability of the challenged claims over any of this Petition’s combinations. That weighs heavily against discretionary denial. *Samsung Elecs. v. Netlist*, IPR2022-00063, Paper 13, 13-14 (May 5, 2022) (step one not satisfied where only one of petition’s four references was cited in an IDS). The Office did not consider Tharappel, Berney, Lee, or Jun in connection with the challenged claims. EX1001, (56). While Agrafioti was considered alone and with respect to anticipation only, it was not considered in connection with any of

Berney, Lee, or Jun. EX1002, 61-62. Berney, Lee, and Jun are not cumulative because *no secondary references were applied or even discussed* in prosecution.

Id. Accordingly, all obviousness arguments presented in the Petition are new.

2. Step Two: The Office Erred Materially

First, because the Office never considered any of the combinations asserted, the Board need not consider step two and may proceed on the merits. *See Thorne Research v. Trs. of Dartmouth Coll.*, IPR2021-00491, Paper 18, 8-9 (Aug. 12, 2021) (where only one reference of combination was previously cited, the Board “need not reach the second part of the [AB] framework”).

Second, even if step two analysis is performed, discretionary denial is inappropriate because “the Office erred in a manner material to the patentability of challenged claims.” *AB*, IPR2019-01469, Paper 6, 8. The Examiner never expressly considered *obviousness* over Agrafioti (nor over any other reference) and provided *no* analysis supporting the conclusion that dependent claims presented allowable subject matter. EX1002, 61-62, 25. “[I]f the record of the Office’s previous consideration of the art is not well developed or silent, then a petition may show the Office erred by overlooking something persuasive.” *AB*, IPR2019-01469, Paper 6, 10. As shown in Grounds 1-6, the Examiner erred in failing to identify teachings in Agrafioti at least rendering challenged claims obvious, and the secondary references contain persuasive teachings overlooked in examination. Accordingly, the

Examiner erred in failing to address obviousness over Agrafioti, alone and in view of secondary references.

XVII. CONCLUSION

The Board should institute IPR and cancel claims 1-9.

Dated: April 26, 2024

Respectfully submitted,

/Elisabeth Hunt/

Elisabeth Hunt, Reg. No. 67,336

CERTIFICATE OF SERVICE UNDER 37 C.F.R. § 42.6 (E)(4)

I certify that on April 26, 2024, I will cause a copy of the foregoing document, including any exhibits or appendices filed therewith, to be served via Priority Express Mail at the following correspondence address of record for the patent:

ORTIZ & LOPEZ, PLLC
PO Box 4484
Albuquerque, NM 87196-4484

Date: April 26, 2024

/MacAulay Rush/
MacAulay Rush
Paralegal
WOLF, GREENFIELD & SACKS, P.C.

CERTIFICATE OF WORD COUNT

Pursuant to 37 C.F.R. § 42.24, the undersigned certifies that the foregoing IPR petition contains 13,981 words excluding a table of contents, a table of authorities, Mandatory Notices under § 42.8, a certificate of service or word count, or appendix of exhibits or claim listing. Petitioners have relied on the word count feature of the word processing system used to create this paper in making this certification.

Date: April 26, 2024

/MacAulay Rush/

MacAulay Rush

Paralegal

WOLF, GREENFIELD & SACKS, P.C.

XVIII. 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.