

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

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

v.

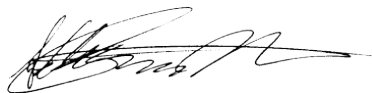
MAXELL, LTD.,
Patent Owner

Inter Partes Review No.: IPR2025-01313

**DECLARATION OF DR. SETH JAMES NIELSON IN SUPPORT OF
PETITION FOR *INTER PARTES* REVIEW OF
U.S. PATENT NO. 10,783,228**

I hereby declare under penalty of perjury under the laws of the United States of America that the following is true and correct, and that all statements made of my own knowledge are true and that all statements made on information and belief are believed to be true. I understand that willful false statements are punishable by fine or imprisonment or both under Section 1001 of Title 18 of the United States Code.

Date: 2025-08-28



Seth James Nielson, Ph.D.

TABLE OF CONTENTS

I.	INTRODUCTION	1
A.	Background and Qualifications	1
B.	Materials Considered.....	9
II.	LEGAL STANDARDS	9
A.	Date of Invention.....	9
B.	Anticipation	9
C.	Obviousness.....	10
D.	Standard of Proof.....	13
III.	THE '228 PATENT	13
A.	Summary of the '228 Patent.....	13
B.	Overview of the '228 Patent's File History	17
C.	A Person of Ordinary Skill in the Art	18
D.	Patent Owner's Infringement Contentions.....	18
IV.	CLAIM CONSTRUCTION	18
A.	“performs communication” (claim 1) and “performing communication” (claim 12).....	19
B.	“unlock” (claims 1 and 12).....	20
V.	PRIOR ART.....	20
A.	Aminzade.....	20
B.	Sowers	23
C.	Soli.....	24
1.	Soli Is Entitled to Its Provisional's Filing Date.	27
D.	Hong	27
1.	Hong Is Entitled to the Foreign Application's Filing Date.	29
E.	Altman	29
VI.	GROUND 1: CLAIMS 1-2, 4-7, 12-13, AND 15-18 ARE OBVIOUS IN LIGHT OF AMINZADE AND SOWERS.....	31
A.	Claim 1	31

2.	[1.pre] (“A system, comprising:”)	31
3.	[1.a] (“a first information processing device including:”).....	31
4.	[1.a.i] (“a dynamic biometric information acquisition sensor that acquires dynamic biometric information from a body of a user; and”)	32
5.	[1.a.ii] (“a first communication interface that transmits the acquired dynamic biometric information; and”).....	34
6.	[1.b] (“a second information processing device including:”)...	37
7.	[1.b.i] (“a static biometric information acquisition sensor that acquires static biometric information;”)	38
8.	[1.b.ii] (“a processor that performs user authentication based on the acquired static biometric information and obtains an authentication result;”)	40
9.	[1.b.iii] (“a second communication interface that performs communication relating to the authentication result with the first communication interface and receives the dynamic biometric information transmitted from the first communication interface; and”).....	45
10.	[1.b.iv] (“a display screen,”).....	50
11.	[1.c] (“wherein the first information processing device: performs communication relating to the authentication result between the first communication interface and the second communication interface and executes an unlock operation to unlock itself in response to the communication relating to the authentication result,”).....	50
12.	[1.d] (“acquires the dynamic biometric information from the dynamic biometric information acquisition sensor after unlocking, and”).....	54
13.	[1.e] (“maintains the unlocked state during a condition that the dynamic biometric information can be acquired,”)	56
14.	[1.f] (“wherein the second information processing device receives the dynamic biometric information via communication between the first communication interface and the second communication interface and the display screen displays information based on a state of the user that	

	is determined using the received dynamic biometric information.”).....	57
B.	Claim 2 (“The system according to claim 1, wherein the first communication interface and the second communication interface are Bluetooth interfaces and communication between the first communication interface and the second communication interface is Bluetooth wireless communication.”)	59
C.	Claim 4 (“The system according to claim 1, wherein the dynamic biometric information is one of heart rate, pulse, blood pressure, body temperature, amount of sweating, or brain wave and the static biometric information is one of finger print information, facial recognition information, retina information, vein information, or iris information.”).	60
D.	Claim 5 (“The system according to claim 1, wherein the first information processing device is a wearable device that acquires the dynamic biometric information at least by being physically in contact with the body.”)	61
E.	Claim 6 (“The system according to claim 1, wherein the first information processing device is a smartwatch and the second information processing device is a smartphone or tablet.”).....	62
F.	Claim 7 (“The system according to claim 1, wherein the first information processing device continuously acquires the dynamic biometric information after being unlocked and the second information processing device receives the dynamic biometric information transmitted from the first communication device continuously or based on starting of an application on the second information processing device.”)	62
G.	Claim 12	63
1.	[12.pre] (“A method, comprising:”)	63
2.	[12.a] (“acquiring dynamic biometric information from a body of a user by a dynamic biometric information acquisition sensor of a first device;”)	63
3.	[12.b] (“transmitting the acquired dynamic biometric information through a first communication interface of the first device to a second device;”)	63

4. [12.c] (“acquiring static biometric information by a static biometric information acquisition sensor of the second device;”) 64
 5. [12.d] (“performing user authentication to obtain an authentication result based on the acquired static biometric information;”).....64
 6. [12.e] (“performing communication with a second communication interface relating to the authentication result with the first communication interface and receiving the dynamic biometric information transmitted from the first communication interface;”) 64
 7. [12.f] (“performing communication relating to the authentication result between the first communication interface and the second communication interface and executing an unlock operation to unlock the first device in response to the communication relating to the authentication result;”).....64
 8. [12.g] (“acquiring the dynamic biometric information from the dynamic biometric information acquisition sensor of the first device after unlocking, and”) 65
 9. [12.h] (“maintaining the unlocked state during a condition that the dynamic biometric information can be acquired;”) 65
 10. [12.i] (“receiving the dynamic biometric information by the second device via communication between the first communication interface and the second communication interface; and”).....65
 11. [12.j] (“displaying on a display screen information based on a state of the user that is determined using the received dynamic biometric information.”) 65
- H. Claim 13 (“The method according to claim 12, wherein the first communication interface and the second communication interface are Bluetooth interfaces and the communication performed between the first communication interface and the second communication interface is Bluetooth wireless communication.”) 65
- I. Claim 15 (“The method according to claim 12, wherein the acquiring of dynamic biometric information acquires one of heart

	rate, pulse, blood pressure, body temperature, amount of sweating, or brain wave and the static biometric information is one of finger print information, facial recognition information, retina information, vein information, or iris information.”).....	66
J.	Claim 16 (“The method according to claim 12, wherein the acquiring of dynamic biometric information by the acquisition sensor of the first device acquires the dynamic biometric information with a wearable device at least by being physically in contact with the body.”)	66
K.	Claim 17 (“The method according to claim 12, wherein the dynamic biometric information is acquired by a smartwatch as the first device and the dynamic biometric information acquired by a smartphone or tablet as the second device.”)	66
L.	Claim 18 (“The method according to claim 12, wherein the dynamic biometric information is continuously acquired by the first device after being unlocked and the second device receives the dynamic biometric information transmitted from the first device continuously or based on starting of an application on the second device.”)	67
M.	Combining Sowers with Aminzade	67
VII.	GROUND 2: CLAIMS 1-2, 4-7, 12-13, 15-18 ARE OBVIOUS IN LIGHT OF AMINZADE AND SOLI	73
A.	Claim 1	73
1.	[1.pre] (“A system, comprising:”)	73
2.	[1.a] (“a first information processing device including:”).....	73
3.	[1.a.i] (“a dynamic biometric information acquisition sensor that acquires dynamic biometric information from a body of a user; and”)	73
4.	[1.a.ii] (“a first communication interface that transmits the acquired dynamic biometric information; and”).....	75
5.	[1.b] (“a second information processing device including:”)...	77
6.	[1.b.i] (“a static biometric information acquisition sensor that acquires static biometric information;”)	77

7. [1.b.ii] (“a processor that performs user authentication based on the acquired static biometric information and obtains an authentication result;”) 77
 8. [1.b.iii] (“a second communication interface that performs communication relating to the authentication result with the first communication interface and receives the dynamic biometric information transmitted from the first communication interface; and”).....77
 9. [1.b.iv] (“a display screen,”).....79
 10. [1.c] (“wherein the first information processing device: performs communication relating to the authentication result between the first communication interface and the second communication interface and executes an unlock operation to unlock itself in response to the communication relating to the authentication result,”).....79
 11. [1.d] (“acquires the dynamic biometric information from the dynamic biometric information acquisition sensor after unlocking, and”).....79
 12. [1.e] (“maintains the unlocked state during a condition that the dynamic biometric information can be acquired,”) 82
 13. [1.f] (“wherein the second information processing device receives the dynamic biometric information via communication between the first communication interface and the second communication interface and the display screen displays information based on a state of the user that is determined using the received dynamic biometric information.”).....83
- B. Claim 2 (“The system according to claim 1, wherein the first communication interface and the second communication interface are Bluetooth interfaces and communication between the first communication interface and the second communication interface is Bluetooth wireless communication.”) 87
- C. Claim 4 (“The system according to claim 1, wherein the dynamic biometric information is one of heart rate, pulse, blood pressure, body temperature, amount of sweating, or brain wave and the static biometric information is one of finger print information,

	facial recognition information, retina information, vein information, or iris information.”)	87
D.	Claim 5 (“The system according to claim 1, wherein the first information processing device is a wearable device that acquires the dynamic biometric information at least by being physically in contact with the body.”)	89
E.	Claim 6 (“The system according to claim 1, wherein the first information processing device is a smartwatch and the second information processing device is a smartphone or tablet.”).....	89
F.	Claim 7 (“The system according to claim 1, wherein the first information processing device continuously acquires the dynamic biometric information after being unlocked and the second information processing device receives the dynamic biometric information transmitted from the first communication device continuously or based on starting of an application on the second information processing device.”)	90
G.	Claim 12	91
2.	[12.pre] (“A method, comprising:”)	91
3.	[12.a] (“acquiring dynamic biometric information from a body of a user by a dynamic biometric information acquisition sensor of a first device;”)	91
4.	[12.b] (“transmitting the acquired dynamic biometric information through a first communication interface of the first device to a second device;”).....	91
5.	[12.c] (“acquiring static biometric information by a static biometric information acquisition sensor of the second device;”).....	91
6.	[12.d] (“performing user authentication to obtain an authentication result based on the acquired static biometric information;”).....	92
7.	[12.e] (“performing communication with a second communication interface relating to the authentication result with the first communication interface and receiving the dynamic biometric information transmitted from the first communication interface;”)	92

8. [12.f] (“performing communication relating to the authentication result between the first communication interface and the second communication interface and executing an unlock operation to unlock the first device in response to the communication relating to the authentication result,”).....92
9. [12.g] (“acquiring the dynamic biometric information from the dynamic biometric information acquisition sensor of the first device after unlocking, and”) 92
10. [12.h] (“maintaining the unlocked state during a condition that the dynamic biometric information can be acquired;”).....92
11. [12.i] (“receiving the dynamic biometric information by the second device via communication between the first communication interface and the second communication interface; and”).....93
12. [12.j] (“displaying on a display screen information based on a state of the user that is determined using the received dynamic biometric information.”) 93
- H. Claim 13 (“The method according to claim 12, wherein the first communication interface and the second communication interface are Bluetooth interfaces and the communication performed between the first communication interface and the second communication interface is Bluetooth wireless communication.”) 93
- I. Claim 15 (“The method according to claim 12, wherein the acquiring of dynamic biometric information acquires one of heart rate, pulse, blood pressure, body temperature, amount of sweating, or brain wave and the static biometric information is one of finger print information, facial recognition information, retina information, vein information, or iris information.”).....93
- J. Claim 16 (“The method according to claim 12, wherein the acquiring of dynamic biometric information by the acquisition sensor of the first device acquires the dynamic biometric information with a wearable device at least by being physically in contact with the body.”) 94
- K. Claim 17 (“The method according to claim 12, wherein the dynamic biometric information is acquired by a smartwatch as the

	first device and the dynamic biometric information acquired by a smartphone or tablet as the second device.”).....	94
L.	Claim 18 (“The method according to claim 12, wherein the dynamic biometric information is continuously acquired by the first device after being unlocked and the second device receives the dynamic biometric information transmitted from the first device continuously or based on starting of an application on the second device.”)	94
M.	Combining Soli with Aminzade	94
VIII.	GROUND 3: CLAIMS 3, 10-11, 14, 21-22 ARE OBVIOUS IN LIGHT OF AMINZADE, SOWERS, AND HONG	100
A.	Claim 3 (“The system according to claim 1, wherein the first communication interface and the second communication interface are Wi-Fi interfaces and communication between the first communication interface and the second communication interface includes establishing a Wi-Fi Direct connection.”)	100
B.	Claim 10 (“The system according to claim 1, wherein upon determining that the user is in a state matching predetermined criteria, the second information processing device limits an operation of the second information processing device by displaying a screen seeking confirmation from the user that the user intended to execute the operation.”).....	101
C.	Claim 11 (“The system according to claim 10, wherein the operation is executed on the second information processing device after the user provides confirmation in response to displaying of the screen.”).....	103
D.	Claim 14 (“The method according to claim 12, wherein the first communication interface and the second communication interface are Wi-Fi interfaces and the communication performed between the first communication interface and the second communication interface includes establishing a Wi-Fi Direct connection.”)	104
E.	Claim 21 (“The method according to claim 12, wherein upon determining that the user is in a state matching predetermined criteria, the second device limits an operation of the second device by displaying on the display screen a message seeking confirmation from the user that the user intended to execute the operation.”).....	104

F.	Claim 22 (“The method according to claim 21, wherein the operation is executed on the second device after the user provides confirmation in response to the displaying of the message on the display screen.”)	105
G.	Combining Hong with Aminzade (and Sowers).....	105
IX.	GROUND 4: CLAIMS 3, 10-11, 14, 21-22 ARE OBVIOUS IN LIGHT OF AMINZADE, SOLI, AND HONG.....	106
X.	GROUND 5: CLAIMS 8-9 AND 19-20 ARE OBVIOUS IN LIGHT OF AMINZADE, SOWERS, AND ALTMAN.....	107
A.	Claim 8 (“The system according to claim 1, wherein the second information processing device gets position information denoting a position of the second information processing device and automatically transmits the position information to a predetermined address based on reception of a user input that is determined to be a predetermined type of user input during a time period, wherein the predetermined address is not inputted by the user during the time period.”)	107
B.	Claim 9 (“The system according to claim 8, wherein the position information is automatically transmitted in response to the user input and without requiring additional user input that explicitly requires approval of the automatic transmission of the position information during the time period.”)	110
C.	Claim 19 (“The method according to claim 12, wherein the second device gets position information denoting a position of the second device and automatically transmits the position information to a predetermined address based on reception of a user input that is determined to be a predetermined type of user input during a time period, wherein the predetermined address is not inputted by the user during the time period.”)	112
D.	Claim 20 (“The method according to claim 19, wherein the position information is automatically transmitted in response to the user input and without requiring additional user input that explicitly requires approval of the automatic transmission of the position information during the time period.”)	112
E.	Combining Altman with Aminzade (and Sowers).....	112

XI.	GROUND 6: CLAIMS 8-9 AND 19-20 ARE OBVIOUS IN LIGHT OF AMINZADE, SOLI, AND ALTMAN	113
XII.	CONCLUSION.....	113

EXHIBITS

Exhibit No.	Description
1001	U.S. Patent No. 10,783,228 (“the “ ’228 patent ”).
1002	File History of U.S. Patent No. 10,783,228.
1003	Declaration of Dr. Seth Nielson.
1004	U.S. Patent No. 8,976,965 (“ Aminzade ”).
1005	U.S. Patent App. Pub. No. 2014/0343371 (“ Sowers ”).
1006	U.S. Patent App. Pub. No. 2015/0347711 (“ Soli ”).
1007	U.S. Provisional App. No. 62/006,032, to which Soli claims priority.
1008	U.S. Patent App. Pub. No. 2015/0278498 (“ Hong ”).
1009	A certified translation of Korean Patent App. No. 10-2014-0037156, to which Hong claims priority.
1010	U.S. Patent No. 8,099,109 (“ Altman ”).
1011	U.S. Patent App. Pub. No. 2014/0107493 (“ Yuen ”).
1012	U.S. Patent App. Pub. No. 2013/0231574 (“ Tran ”).
1013	Patent Owner’s infringement contentions cover pleading from <i>Maxell, Ltd. v. Samsung Elecs. Co., Ltd.</i> , No. 5:25-cv-00052 (E.D. Tex.).
1014	Patent Owner’s ’228 patent infringement contentions claim chart from <i>Maxell, Ltd. v. Samsung Elecs. Co., Ltd.</i> , No. 5:25-cv-00052 (E.D. Tex.).

TABLE OF CLAIMS

[1.pre] A system, comprising:
[1.a] a first information processing device including:
[1.a.i] a dynamic biometric information acquisition sensor that acquires dynamic biometric information from a body of a user; and
[1.a.ii] a first communication interface that transmits the acquired dynamic biometric information; and
[1.b] a second information processing device including:
[1.b.i] a static biometric information acquisition sensor that acquires static biometric information;
[1.b.ii] a processor that performs user authentication based on the acquired static biometric information and obtains an authentication result;
[1.b.iii] a second communication interface that performs communication relating to the authentication result with the first communication interface and receives the dynamic biometric information transmitted from the first communication interface; and
[1.b.iv] a display screen,
[1.c] wherein the first information processing device: performs communication relating to the authentication result between the first communication interface and the second communication interface and executes an unlock operation to unlock itself in response to the communication relating to the authentication result,
[1.d] acquires the dynamic biometric information from the dynamic biometric information acquisition sensor after unlocking, and
[1.e] maintains the unlocked state during a condition that the dynamic biometric information can be acquired,
[1.f] wherein the second information processing device receives the dynamic biometric information via communication between the first communication interface and the second communication interface and the display screen displays information based on a state of the user that is determined using the received dynamic biometric information.
[2] The system according to claim 1, wherein the first communication interface and the second communication interface are Bluetooth interfaces and communication between the first communication interface and the second communication interface is Bluetooth wireless communication.
[3] The system according to claim 1, wherein the first communication interface and the second communication interface are Wi-Fi interfaces and communication

between the first communication interface and the second communication interface includes establishing a Wi-Fi Direct connection.
[4] The system according to claim 1, wherein the dynamic biometric information is one of heart rate, pulse, blood pressure, body temperature, amount of sweating, or brain wave and the static biometric information is one of finger print information, facial recognition information, retina information, vein information, or iris information.
[5] The system according to claim 1, wherein the first information processing device is a wearable device that acquires the dynamic biometric information at least by being physically in contact with the body.
[6] The system according to claim 1, wherein the first information processing device is a smartwatch and the second information processing device is a smartphone or tablet.
[7] The system according to claim 1, wherein the first information processing device continuously acquires the dynamic biometric information after being unlocked and the second information processing device receives the dynamic biometric information transmitted from the first communication device continuously or based on starting of an application on the second information processing device.
[8] The system according to claim 1, wherein the second information processing device gets position information denoting a position of the second information processing device and automatically transmits the position information to a predetermined address based on reception of a user input that is determined to be a predetermined type of user input during a time period, wherein the predetermined address is not inputted by the user during the time period.
[9] The system according to claim 8, wherein the position information is automatically transmitted in response to the user input and without requiring additional user input that explicitly requires approval of the automatic transmission of the position information during the time period.
[10] The system according to claim 1, wherein upon determining that the user is in a state matching predetermined criteria, the second information processing device limits an operation of the second information processing device by displaying a screen seeking confirmation from the user that the user intended to execute the operation.
[11] The system according to claim 10, wherein the operation is executed on the second information processing device after the user provides confirmation in response to displaying of the screen.
[12.pre] A method, comprising:

[12.a] acquiring dynamic biometric information from a body of a user by a dynamic biometric information acquisition sensor of a first device;
[12.b] transmitting the acquired dynamic biometric information through a first communication interface of the first device to a second device;
[12.c] acquiring static biometric information by a static biometric information acquisition sensor of the second device;
[12.d] performing user authentication to obtain an authentication result based on the acquired static biometric information;
[12.e] performing communication with a second communication interface relating to the authentication result with the first communication interface and receiving the dynamic biometric information transmitted from the first communication interface;
[12.f] performing communication relating to the authentication result between the first communication interface and the second communication interface and executing an unlock operation to unlock the first device in response to the communication relating to the authentication result,
[12.g] acquiring the dynamic biometric information from the dynamic biometric information acquisition sensor of the first device after unlocking, and
[12.h] maintaining the unlocked state during a condition that the dynamic biometric information can be acquired;
[12.i] receiving the dynamic biometric information by the second device via communication between the first communication interface and the second communication interface; and
[12.j] displaying on a display screen information based on a state of the user that is determined using the received dynamic biometric information.
13. The method according to claim 12, wherein the first communication interface and the second communication interface are Bluetooth interfaces and the communication performed between the first communication interface and the second communication interface is Bluetooth wireless communication.
14. The method according to claim 12, wherein the first communication interface and the second communication interface are Wi-Fi interfaces and the communication performed between the first communication interface and the second communication interface includes establishing a Wi-Fi Direct connection.
15. The method according to claim 12, wherein the acquiring of dynamic biometric information acquires one of heart rate, pulse, blood pressure, body temperature, amount of sweating, or brain wave and the static biometric information is one of finger print information, facial recognition information, retina information, vein information, or iris information.

16. The method according to claim 12, wherein the acquiring of dynamic biometric information by the acquisition sensor of the first device acquires the dynamic biometric information with a wearable device at least by being physically in contact with the body.
17. The method according to claim 12, wherein the dynamic biometric information is acquired by a smartwatch as the first device and the dynamic biometric information acquired by a smartphone or tablet as the second device.
18. The method according to claim 12, wherein the dynamic biometric information is continuously acquired by the first device after being unlocked and the second device receives the dynamic biometric information transmitted from the first device continuously or based on starting of an application on the second device.
19. The method according to claim 12, wherein the second device gets position information denoting a position of the second device and automatically transmits the position information to a predetermined address based on reception of a user input that is determined to be a predetermined type of user input during a time period, wherein the predetermined address is not inputted by the user during the time period.
20. The method according to claim 19, wherein the position information is automatically transmitted in response to the user input and without requiring additional user input that explicitly requires approval of the automatic transmission of the position information during the time period.
21. The method according to claim 12, wherein upon determining that the user is in a state matching predetermined criteria, the second device limits an operation of the second device by displaying on the display screen a message seeking confirmation from the user that the user intended to execute the operation.
22. The method according to claim 21, wherein the operation is executed on the second device after the user provides confirmation in response to the displaying of the message on the display screen.

I. INTRODUCTION

1. I, Dr. Seth Nielson, have been retained by counsel for Petitioners Samsung Electronics Co. Ltd. and Samsung Electronics America, Inc. (collectively, “Samsung”) as an expert witness in this *inter partes* review. I have been asked to provide my opinion about the patentability of the claims of U.S. Patent No. 10,783,228 (“’228 patent,” EX1001).

2. I have been retained at my normal hourly rate of \$750 per hour. My compensation is not contingent upon my performance, the outcome of this matter, or any issues involved in or related to this matter

3. In summary, it is my opinion that the prior art references that I analyze below render obvious the ’228 patent’s claims, as summarized in the table below:

Ground	Claims	Statutory Basis	Prior Art
1	1-2, 4-7, 12-13, 15-18	35 U.S.C. § 103	Aminzade and Sowers
2	1-2, 4-7, 12-13, 15-18	35 U.S.C. § 103	Aminzade and Soli
3	3, 10-11, 14, 21-22	35 U.S.C. § 103	Aminzade, Sowers, and Hong
4	3, 10-11, 14, 21-22	35 U.S.C. § 103	Aminzade, Soli, and Hong
5	8-9, 19-20	35 U.S.C. § 103	Aminzade, Sowers, and Altman
6	8-9, 19-20	35 U.S.C. § 103	Aminzade, Soli, and Altman

A. Background and Qualifications

4. I received my B.S. in Computer Science from Brigham Young

University (“BYU”) in April of 2000. I received my M.S. in Computer Science from BYU in August of 2004. I received my Ph.D. in Computer Science from Rice University in December 2009.

5. I have been working as a computer scientist professionally for over twenty-five years, including projects in industry, academia, government, and non-profits. I have extensive experience in cybersecurity, computer networks, and software engineering.

6. Currently, I am the Founder and Chief Scientist of Crimson Vista, a computer security research and engineering company. I started Crimson Vista in March 2016. Prior to that, I worked as a Software Engineer at Quallaby in 2000, Lineo/Metrowerks from 2001-2003, and Google in the summer of 2005. I worked in technical consulting from 2005-2011 at Independent Security Evaluators and at Harbor Labs from 2011-2015.

7. I currently hold appointments at the University of Texas at Austin as an Adjunct Associate Professor in the department of Computer Science, and as a Cybersecurity Fellow in the Robert Strauss Center for International Security and Law. I previously held appointments as an Adjunct Research Scientist in the Computer Science department of The Johns Hopkins University from 2014-2019. From 2016-2019, I was also the Director of Advanced Research Projects in the Information Security Institute.

8. I am also the co-founder of the non-profit Crypto Done Right foundation, which concluded operations in 2025.

9. During my work as a software engineer at Quallaby, Metrowerks, and Google, I created, tested, and/or maintained hundreds of thousands of lines of source code in a wide range of computer programming languages. This included components related to computer networking, graphical user interfaces (GUIs), operating system build/configuration, web communications, automated deployment of software, virtual machines, and secure communications.

10. Moreover, while consulting at Independent Security Evaluators (ISE), I was also the technical lead for the development of software for a client. I designed and managed the implementation of the system, which involved improved communication systems for secure channels on the Internet. This system provided new benefits for distributing trust in Certificate Authorities, which are often the weak link in Transport Layer Security.

11. At ISE, I worked on a wide range of development projects for clients related to security features. These projects included a software encryption library, including the necessary tests and procedures for Federal Information Processing Standards (“FIPS”) certification. The encryption library also provided advanced operations such as secure data splitting and recovery. I also developed a parallel-program for massive code coverage analysis, GPU hardware-accelerated AES

encryption, and distributed (encrypted) file-system prototypes.

12. In my work as a cybersecurity analyst at ISE, Harbor Labs, and Crimson Vista, I have performed security evaluation services that included port-scanning analyses, security protocol analysis using formal and exploratory methods, and security breach investigations. Clients include large banks, major medical device manufacturers, the MPAA and RIAA jointly, hospitals, cyber-insurance companies, startup companies, media companies, and financial institutions. My analyses include reviews of programming code (*e.g.*, for bugs/vulnerabilities), cryptography, and forensics.

13. As a security consultant, I offered services broadly within the scope of security engineering. This holistic process provides comprehensive analysis, design, and insight into cybersecurity concerns before, during, and after development. A key component of my approach to security engineering includes data discovery, architecture, and quality control as a critical first step in security (*i.e.*, “you can’t secure data you don’t know about”). I have applied these models to various clients including clients for whom I have provided contract Chief Information Security Officer (CISO) services.

14. I have also provided technical guidance to an antitrust team in the United States Department of Justice. Although the technologies and parties are confidential, I can disclose that I provided in-person training on technical topics

and analyses of competing security products.

15. In addition to consulting with companies, I have also provided training on security and privacy at the Data Architecture Summit and Enterprise Data World conferences.

16. I also am experienced in forensic analysis, including analysis of source code. For over a decade, at Harbor Labs and Crimson Vista, I have performed a wide range of code reviews for diverse technologies including CAD software, video game systems, digital mobile radios (DMRs), video streaming, networking, cryptography, antivirus, and digital rights management (DRM). As Crimson Vista has grown, I have also directed teams of associates in security, forensic, and research efforts.

17. Our services, which I lead and manage, also include security and compliance audits, AI evaluation and assessment, and security services enhancement for managed service providers. We also provide contract design guidance and engineering on security tools and systems.

18. Beyond my work as an engineer and technical consultant, I have been involved in academic teaching, development, and research since my undergraduate degree. I first engaged in research in the Fall of 2000 on a project in the BYU computer science department related to networks and network resource management. Our work was published in the research paper “Effective Bandwidth

for Traffic Engineering.”

19. While earning my master’s degree, I conducted research in software engineering topics, with a special emphasis on how programmers think while creating and modifying code. My research included a study of software architectural patterns and their evolution over time. My research was published as “Design Dysphasia and the Pattern Maintenance Cycle,” in the Journal Information and Software Technology, August 2006. My thesis, which I completed in 2004, was largely based on this research.

20. During my Ph.D. work at Rice University, I conducted research into multiple topics, including computer vulnerabilities and distributed computer security. In my research, I identified a security vulnerability in a Google product that existed at the time (Google Desktop Search). After contacting Google and assisting them in closing the vulnerability, we published the details of our investigation. I also published various papers including “A Taxonomy of Rational Attacks.” I defended my thesis, “Designing Incentives for Peer-to-Peer Systems,” in late 2009.

21. I began teaching as an adjunct professor in 2014 at The Johns Hopkins University. I taught undergraduate and graduate studies in computer security. In 2016, the Information Security Institute appointed me as the Director of Advanced Research Projects. I collaborated with companies, government agencies, and other

academic institutions to develop the research programs of the Information Security Institute. I also mentored student capstone projects related to cryptography, drone security, iOS security, bitcoin, SSL vulnerabilities, and Twitter “botnets.” My students and I have published multiple papers from these capstone projects, including published research on cracking a portable chemical manufacturing system.

22. I began teaching at the University of Texas at Austin as an adjunct professor in 2019. I taught the undergraduate computer security class in the computer science department. I currently teach a special class on cybersecurity technology in the UT law school.

23. In all of these classes, I have developed my own curriculum. I created an experimental set of projects at The Johns Hopkins University about which I subsequently published a paper in the Journal of Computer Science Education entitled, “PLAYGROUND: Preparing Students for the Cyber Battleground.”

24. I also continue research at Crimson Vista. I was the primary investigator on a government funded research project. The project dealt with automatic recovery from ransomware attacks and was funded by the United States Army. The project was collaborative with academia, and I led a team of student researchers from Johns Hopkins and BYU in developing my design and implementing a prototype.

25. I also helped to design and test secure enclave systems funded by the NSF, and am currently researching techniques for protecting data from exfiltration by executives or other high-ranking (high-access) individuals.

26. I am also a contributor to another small-business research project begun by a former student and funded by the National Science Foundation. We are researching the development of a new system for secure data storage that is protected even against “insider” threats, such as a rogue IT administrator.

27. I am also the author of “Cryptography in Python: Learning Correct Cryptography by Example.” I am also the author of the book “Discovering Cyber-security: A Technical Introduction for the Absolute Beginner,” which I use as my textbook for my students at UT. My next book, “Cybersecurity Governance,” is expected to be published in Q3 or Q4 of 2025.

28. Of the experience listed in this section, much of it includes biometrics and/or biometric sensors. In my teaching at both Johns Hopkins and the University of Texas at Austin, I lectured on different forms and mechanisms for user authentication including biometrics. These lectures included known advantages and disadvantages of biometric authentication and the relevant security parameters for the sensors employed. My book, “Discovering Cyber-security: A Technical Introduction for the Absolute Beginner,” includes sections drawn, in part, from these lectures. Additionally, I have reviewed various portions of the source code

for biometric sensors for both Android and iOS devices. In some cases, I have reviewed source code for the actual sensor itself, which is separate from the source code for the operating system. Moreover, in auditing the security of client systems, I consider the recommendations, guidelines, and requirements that include biometric identifiers (*e.g.*, NIST SP800-171 03.05.01, 03.05.03, 03.05.12, and 03.10.07).

29. My qualifications, publications, professional experience and expertise are set forth more fully in my curriculum vitae, attached as Appendix A.

B. Materials Considered

30. In preparing this declaration and forming my opinions, I have considered the materials referenced in this declaration, including in the table of exhibits at the beginning of this declaration. My opinions also are based on my years of education, research, and experience, as well as my review of relevant materials.

II. LEGAL STANDARDS

A. Date of Invention

31. I have been asked to use the date of the earliest application to which the '228 patent claims priority (June 12, 2014) as the date of the purported invention for purposes of my analysis.

B. Anticipation

32. I understand from counsel that a patent claim is invalid under 35

U.S.C. § 102 if a prior art disclosure teaches every element required by the claim, either expressly or inherently. The identical invention must be shown in as complete detail as is contained in the claim. When a claim covers several structures or compositions, either generically or as alternatives, the claim is deemed anticipated if any of the structures or compositions within the scope of the claim is known in the prior art.

C. Obviousness

33. I understand from counsel that a patent claim is invalid under 35 U.S.C. § 103 if the differences between the invention and the prior art are such that the subject matter as a whole would have been obvious at the time of the invention to a person having ordinary skill in the art to which the subject matter pertains. Obviousness, as has been explained to me, is based on (i) the scope and content of the prior art, (ii) the differences between the prior art and the claim, (iii) the level of ordinary skill in the art, and (iv) any secondary indicia of non-obviousness (e.g., “secondary considerations” such as commercial success in the market place of the claimed invention), to the extent that they exist.

34. I further understand from counsel that obviousness may be demonstrated by showing that it would have been obvious to combine the teachings of more than one item of prior art. In determining whether a piece of prior art could have been combined with other prior art or with other information

within the knowledge of a person having ordinary skill in the art, the following are examples of approaches and rationales that may be considered:

- Combining prior art elements according to known methods to yield predictable results;
- Simple substitution of one known element for another to obtain predictable results;
- Use of a known technique to improve similar devices (methods, or products) in the same way;
- Applying a known technique to a known device (method or product) ready for improvement to yield predictable results;
- Applying a technique or approach that would have been obvious to try (choosing from a finite number of identified, predictable solutions, with a reasonable expectation of success);
- Known work in one field of endeavor may prompt variations of it for use in either the same field or a different one based on design incentives or other market forces if the variations would have been predictable to a person having ordinary skill in the art; and
- Some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill to modify the prior art reference or to combine prior art reference teachings to arrive at the claimed invention.

35. I further understand that an invention may be obvious if one of ordinary skill in the art, facing a wide range of needs created by developments in the field, would have seen an obvious benefit to the solutions tried by the applicant. When there is a design need or market pressure to solve a problem and there are a finite number of identified, predictable solutions, it may be obvious to a

person of ordinary skill to try the known options. If a technique has been used to improve one device, and a person of ordinary skill in the art would recognize that it would improve similar devices in the same way, using the technique would have been obvious.

36. I further understand that a person of ordinary skill in the art is a hypothetical person who is presumed to be aware of all of the relevant art at the time of the invention. The person of ordinary skill may be able to fit together the teachings of multiple patents and/or printed publications employing ordinary creativity and the common sense that familiar items may have uses in another context or beyond their primary purposes.

37. I also understand that when considering the obviousness of a patent claim, one should consider whether a teaching, suggestion, or motivation to combine the references exists so as to avoid impermissibly applying hindsight when combining or modifying the prior art. I understand this test should not be applied rigidly, but that the test can be important to avoid such hindsight.

38. I also understand that one of ordinary skill in the art must have a reasonable expectation of success in combining or modifying prior art references.

39. I also understand that all elements of a claim must be considered in an obviousness analysis.

D. Standard of Proof

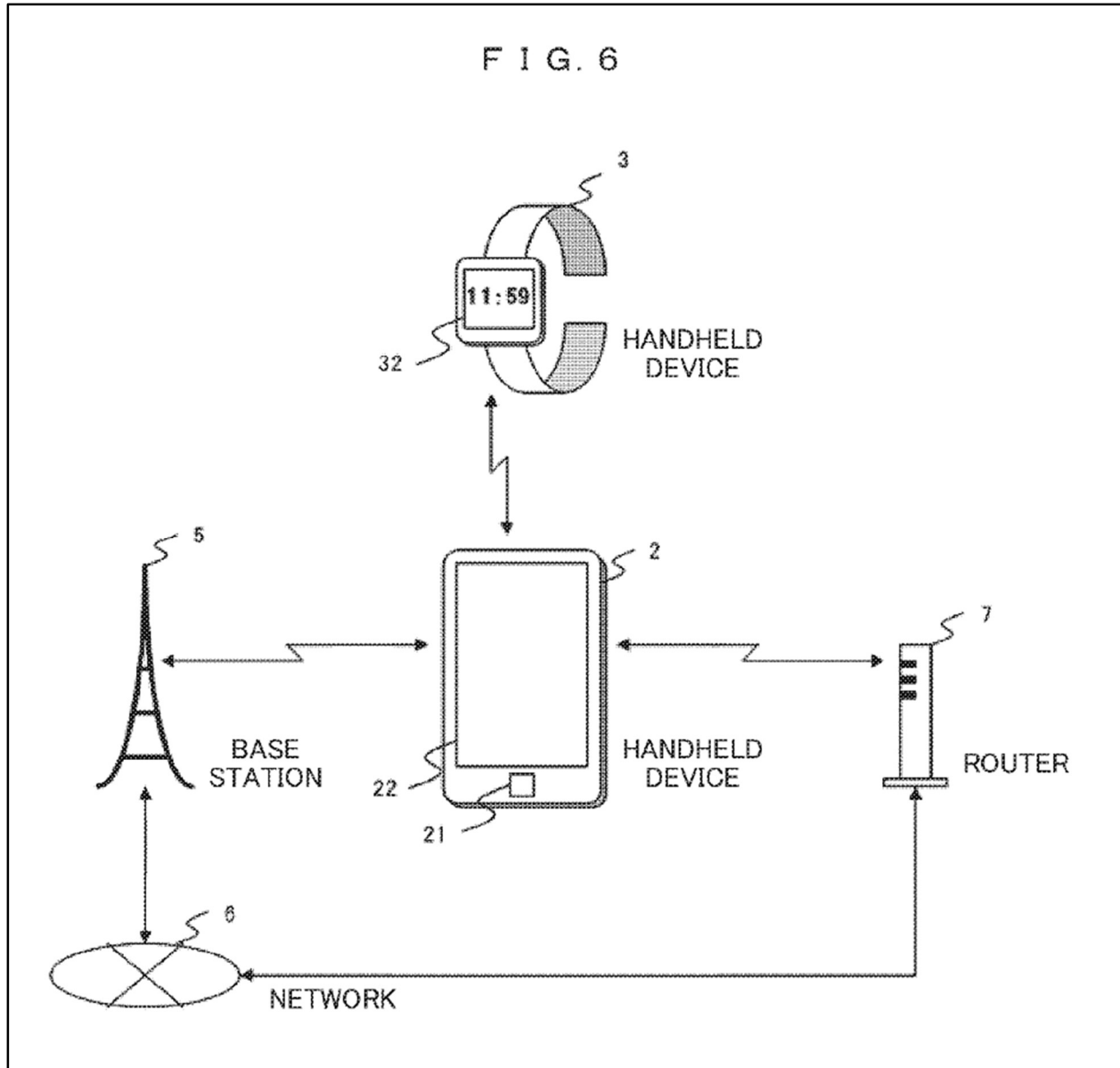
40. I understand that the standard to prove unpatentability in an *inter partes* review is by a preponderance of the evidence, which means more likely than not.

III. THE '228 PATENT

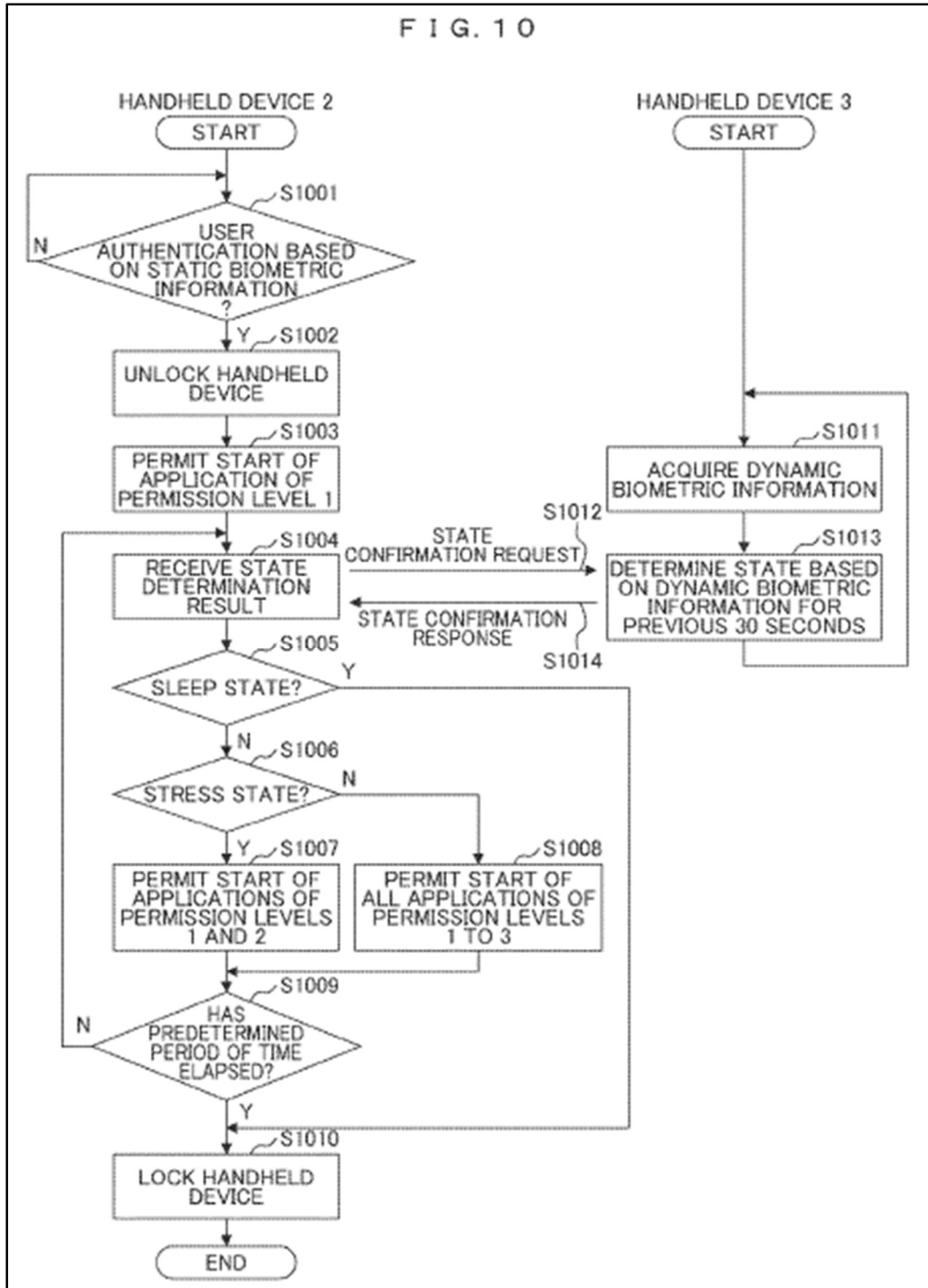
A. Summary of the '228 Patent

41. The '228 patent claims priority to U.S. Patent Application No. 15/315,735, filed on June 12, 2014. EX1001, cover page. I understand from counsel that the '228 patent's earliest possible effective filing date therefore is June 12, 2014. I understand from counsel that because the earliest effective filing date of the '228 patent is after March 16, 2013, the '228 patent is subject to the America Invents Act ("AIA").

42. The '228 patent relates to a system that, in one embodiment, includes a "handheld device 2" that is a "smart phone" in communication with a "wristwatch-type" "handheld device 3," as shown below in Figure 6. EX1001, 10:49-11:11.



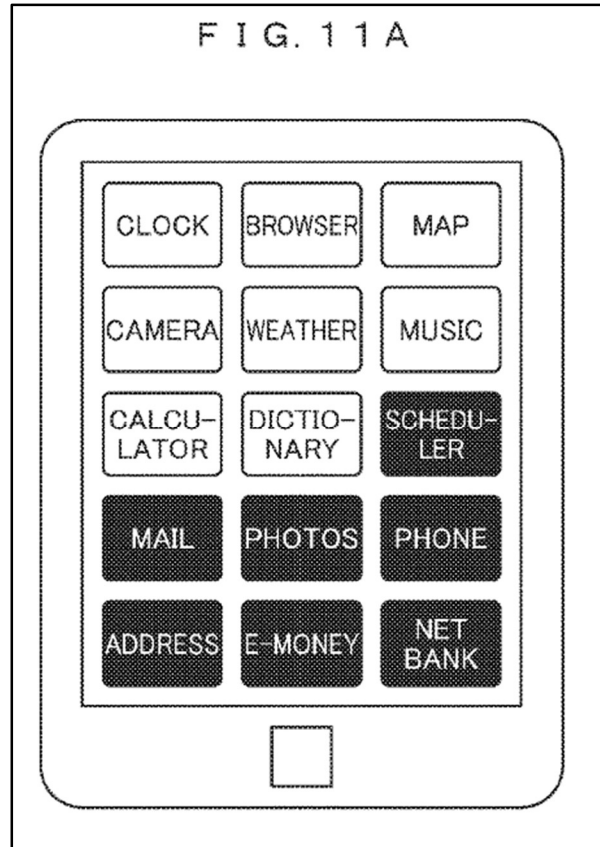
The smartphone “performs user authentication” using “static biometric information” such as a “fingerprint,” and unlocks itself. *Id.*, 13:20-31, Fig. 10 (shown below, S1001, S1002).



The wristwatch-type device measures “dynamic biometric information” from the user, such as “heart rate,” “blood pressure,” and “body temperature,” and uses this information to determine “the state of the user” (e.g., a “normal state,” “sleep

state,” or “stress state”). *Id.*, 13:47-50, 13:54-14:2, Fig. 10 (S1011, S1013). It then transmits the user state to the smartphone. *Id.*, 14:7-9, Fig. 10 (S1014).

43. If the user is sleeping, the phone locks itself. EX1001, 14:13-15, Fig. 10 (S1010). If the user is stressed, the phone permits use of applications with permission levels 1 to 2. *Id.*, 13:21-25, 8:38-43, Fig. 10 (S1007). If the user is in a normal state, the phone permits use of applications with permission levels 1 to 3. *Id.*, 13:21-25, 8:60-63, Fig. 10 (S1008). An application’s permission level relates to how large of a “problem” would be posed by it being “used by anyone else.” *Id.*, 7:22-30, 8:44-52, 8:64-9:4. The phone displays application icons in a “non-startable state” in a different color, as shown below. *Id.*, 13:32-40, 14:26-44, Figs. 11A (shown below), 11B-C.



44. Although the '228 patent specification emphasizes using the user's state to govern access to applications, the patent's independent claims are broader and recite "display[ing]" *any* "information based on a state of the user." EX1001, 20:52-55 (claim 1), 22:19-21 (claim 12). By choosing such claim language, Patent Owner erased any potential point of novelty the patent's purported invention may have had, and encompassed the prior art.

B. Overview of the '228 Patent's File History

45. The examiner of the '228 patent application rejected the claims on the basis of non-statutory double patenting in light of the application's parent, U.S. Patent No. 10,423,769. EX1002, 353-356. Patent Owner overcame the rejection

by filing a terminal disclaimer. *Id.*, 328-329. The examiner then allowed the claims, stating that the prior art of record did not disclose or render obvious the body of the independent claims. *Id.*, 12-13.

C. A Person of Ordinary Skill in the Art

46. In my opinion, a person of ordinary skill in the art (“POSITA”) at the time of the alleged invention of the ’228 patent (June 12, 2014) would have had a bachelor’s degree in computer science, electrical or computer engineering, or a comparable field of study, plus approximately two to three years of professional experience with biometrics and smart, portable consumer electronics, or other relevant industry experience. Additional education could substitute for professional experience, and significant industry experience could substitute for formal education.

47. I met and exceeded the above qualifications for a POSITA as of at least the ’228 patent’s earliest possible effective filing date (June 12, 2014).

D. Patent Owner’s Infringement Contentions

I have reviewed Patent Owner Maxell, Ltd.’s (“Patent Owner”) infringement contentions for the ’228 patent in the litigation between Patent Owner and Samsung. EX1013, pp. 73-81; EX1014.

IV. CLAIM CONSTRUCTION

48. In this section, I address the construction of certain claim terms, and I have applied those constructions in my analysis. For all other terms, I have applied

the plain and ordinary meaning as understood by a POSITA at the time of the purported invention.

A. “performs communication” (claim 1) and “performing communication” (claim 12)

49. In my opinion, the phrases “performs communication” and “performing communication” should be interpreted to include communicating within a device and to include receiving a transmission.

50. I understand from counsel that the scope of a claim term should not be interpreted in a way that excludes an embodiment disclosed in the specification, unless there is “highly persuasive” evidence to the contrary. The ’228 patent’s specification states that “communication” may be “performed” within “handheld device 1,” “between the CPU 101 and [other internal] units” using “system bus 102.” EX1001, 3:58-61, Fig. 2. I am not aware of any “highly persuasive” evidence, including in the ’228 patent and its file history, that would warrant excluding this embodiment from the claims’ scope. Thus, “performs communication”/“performing communication” includes communicating within a device. The ’228 patent also states that “communication” can be “transmission” or “reception.” *Id.*, 4:55-59, 3:45-51, 4:60-63, 11:12-15. I am not aware of any “highly persuasive” evidence that would warrant excluding these embodiments from the claims’ scope. Thus, “performs communication”/“performing communication” also includes receiving a transmission.

51. I also understand from counsel that the use of different words in a patent claim's implies different meaning. The '228 patent's claims use variations of the word "transmit," indicating that "performs communication"/"performing communication" is not synonymous with transmitting, and therefore includes reception. *Id.*, 20:24, 20:35, 21:57, 22:1.

B. "unlock" (claims 1 and 12)

52. In claims 1 and 12, "unlock" is used in context of "unlock[ing]" a device. EX1001, 20:38-42 ("a first information processing device...executes an unlock operation to unlock itself"), 22:5-6 ("executing an unlock operation to unlock the first device").

53. A POSITA would have understood that the plain meaning of "unlock[ing]" a device includes allowing the user to access additional functionality on the device. For example, the '228 patent's Figure 10 shows that, as a result of unlocking the device in step S1002, the user may start applications with certain permission levels. EX1001, Fig. 10 (S1003, S1007, S1008), 13:28-31.

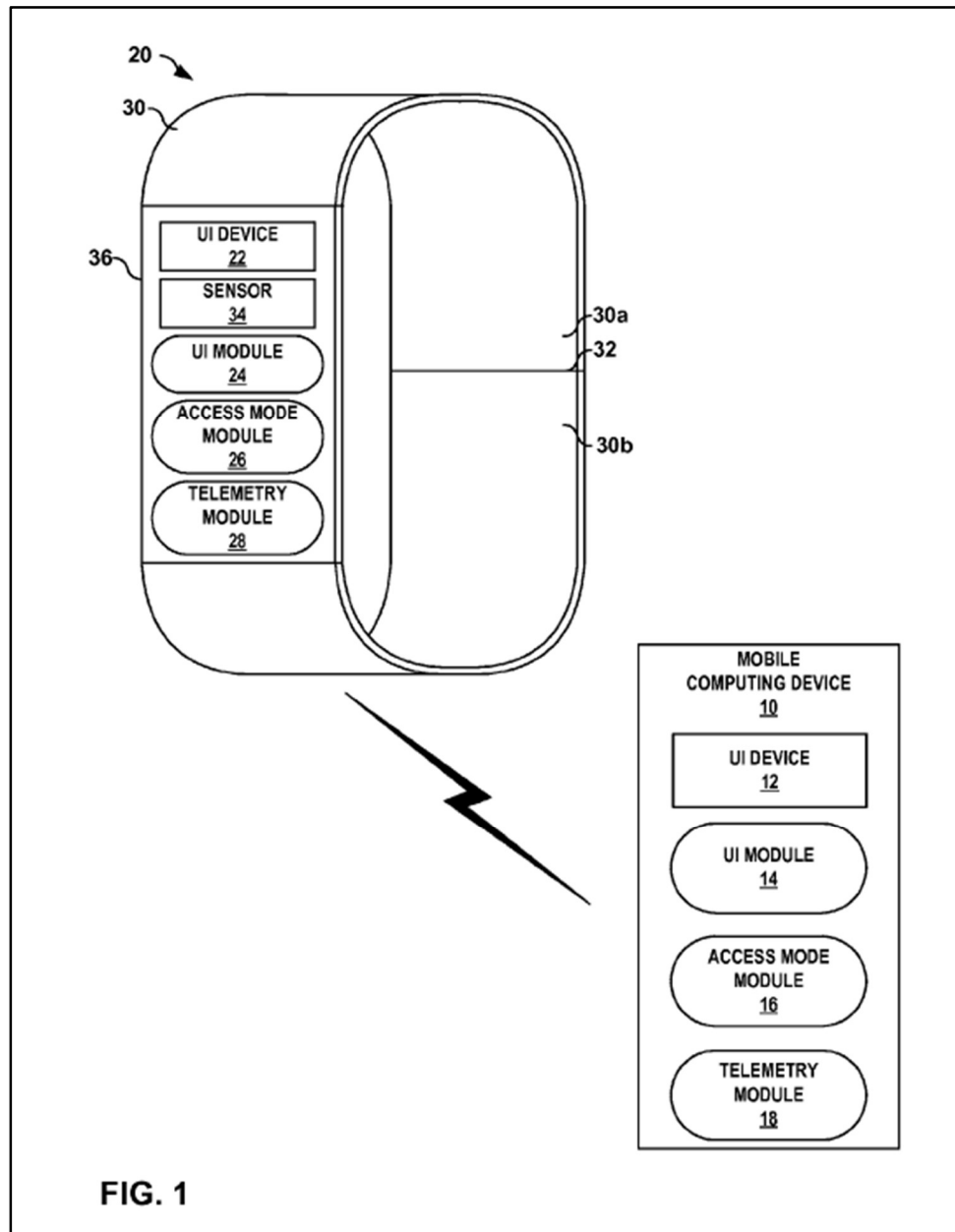
V. PRIOR ART

A. Aminzade

54. U.S. Patent No. 8,976,965 ("Aminzade") was filed on October 2, 2013. EX1004, cover page. I understand that Aminzade is prior art under at least 35 U.S.C. § 102(a)(2).

55. Aminzade discloses "a mobile computing device 10 and a wearable

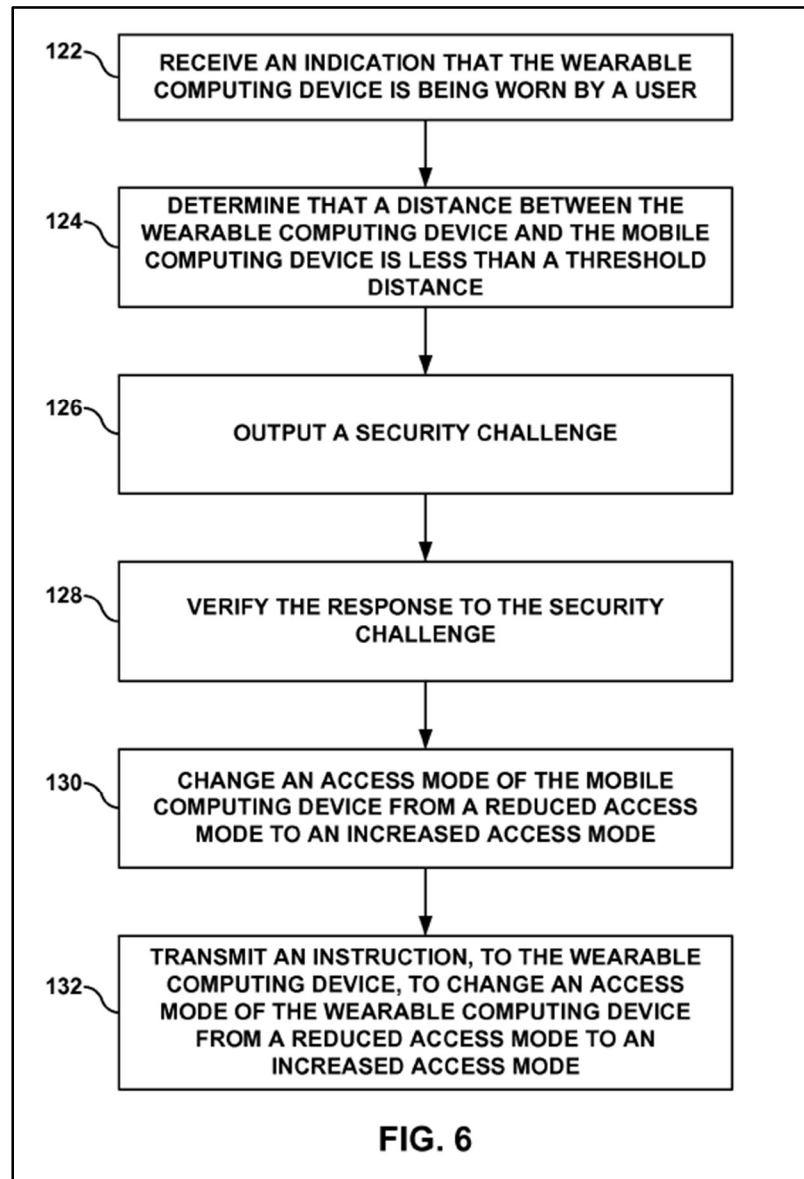
computing device 20,” shown below in Figure 1. EX1004, 4:5-12. The mobile device may be a “smart phone[]” and the wearable device may be “a smart watch.” *Id.*, 4:18-22, 4:46-48.



56. Mobile device 10 can authenticate, for example, the user’s fingerprint.

EX1004, 13:53-14:1, 8:34-46. Upon such authentication, mobile device 10

unlocks itself by changing from a “reduced access mode to an increased access mode.” *Id.*, 14:1-7, 8:47-53. It also sends an “instruction” to wearable device 20 to similarly unlock itself. *Id.*, 14:8-14, 8:54-60. Figure 6 shows these steps.



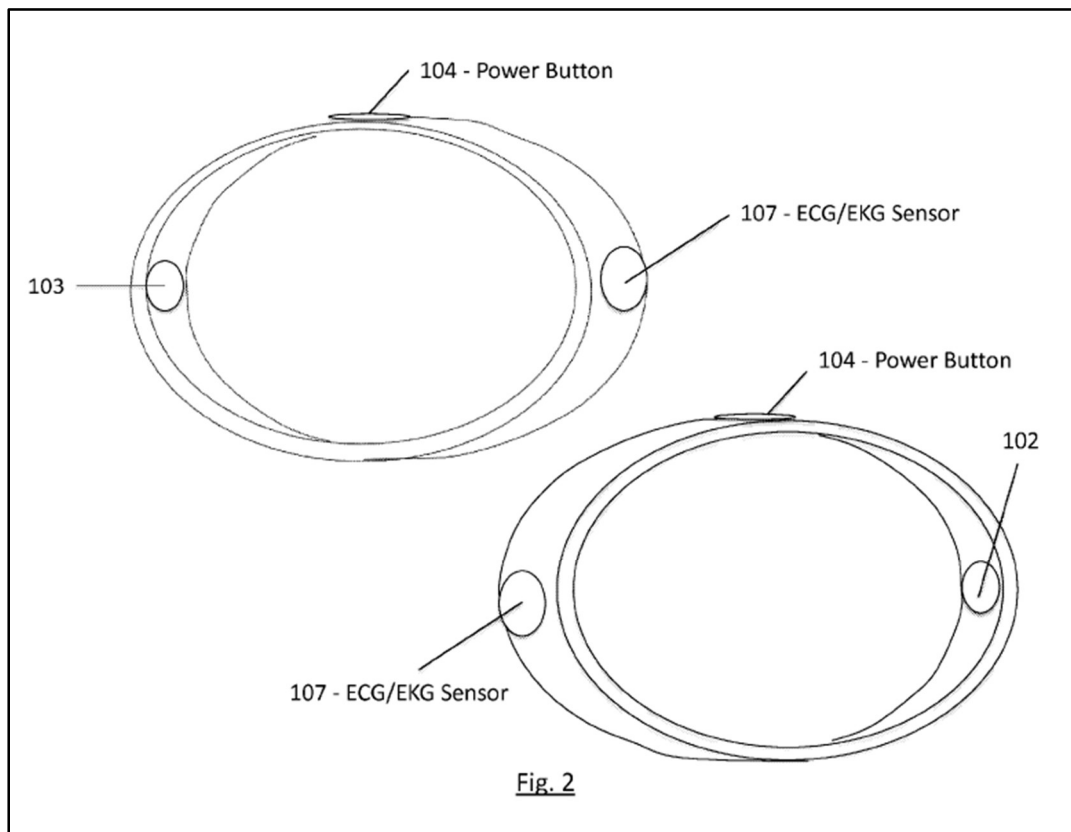
57. In my opinion, Aminzade is analogous art to the '228 patent because it relates to authenticating a user using a static biometric sensor, unlocking a handheld device, and communicating the authentication result to another device, as

described above. I understand that the USPTO did not consider Aminzade during prosecution of the '228 patent. EX1001, pp. 1-2.

B. Sowers

58. U.S. Patent Application Publication No. 2014/0343371 (“Sowers”) was filed on May 13, 2014. EX1005, cover page. I understand that Sowers is prior art under at least 35 U.S.C. § 102(a)(2).

59. Sowers discloses “health monitoring device” 101, shown below, that “is shown as a wrist band, but may be ... attachable to a watch.” EX1005, ¶15, ¶17, Fig. 2.



It includes “optical sensors 103” and “ECG/EKG sensors 107.” *Id.*, ¶15, Fig. 2.

The device uses the sensors to acquire health data, and transmits the health data to “base station 112,” which can be a “smart phone.” *Id.*, ¶¶23-25, ¶18. The smartphone analyzes the data and displays the results, which includes the “user’s risk of heart attack [and] stroke.” *Id.*, ¶¶27-28. The phone also generates a “warning or alert” if the health data indicates a “dangerous condition.” *Id.*, ¶31.

60. In my opinion, Sowers is analogous art to the ’228 patent because it relates to acquiring dynamic biometric information from a user and transmitting that information to another device, which uses that information to determine a user state and display information accordingly. I understand that the USPTO did not consider Sowers during prosecution of the ’228 patent. EX1001, pp. 1-2.

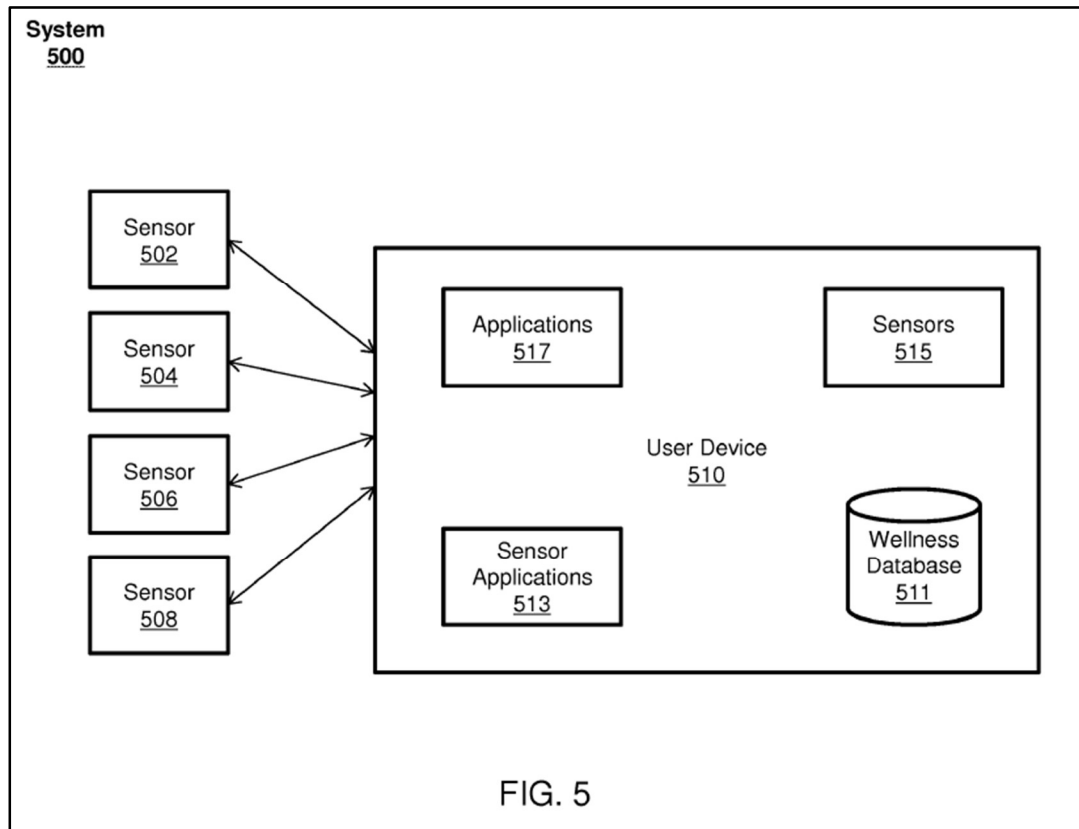
C. Soli

61. U.S. Patent Application Publication No. 2015/0347711 (“Soli”), which issued as U.S. Patent No. 10,270,898, was filed on January 16, 2015 and claims priority to a provisional application filed on May 30, 2014. EX1006, cover page. I understand that Soli is therefore prior art under at least 35 U.S.C. § 102(a)(2) and (d).

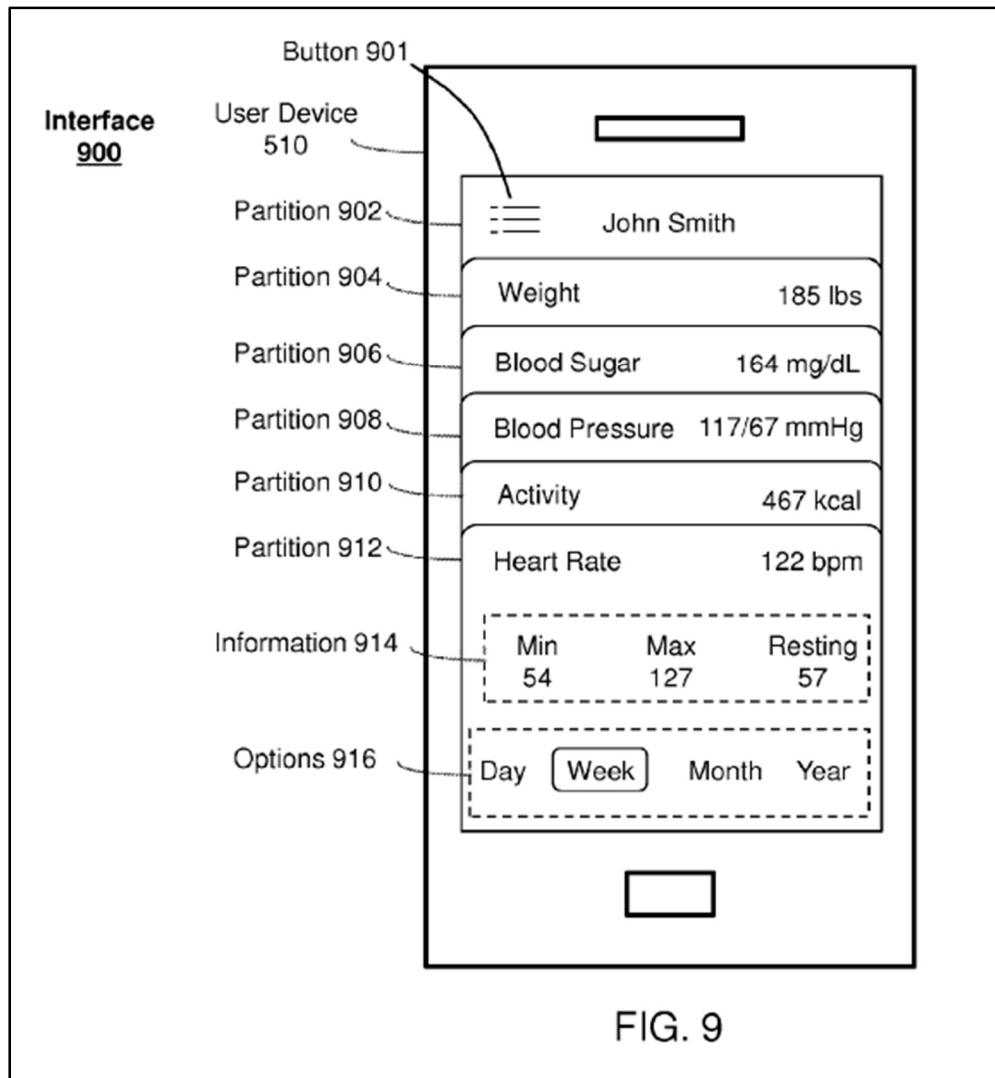
62. Soli discloses “aggregating and sharing wellness data” using “user device 510,” which can be “a mobile phone,” and “a wearable electronic device, such as a smart watch.” EX1006, ¶2, ¶225, ¶26. The smartwatch can include

sensors 502-508, such as a “photoplethysmogram, galvanic skin response sensor, [and a] temperature sensor,” to measure the user’s “wellness data.” *Id.*, ¶226, Fig.

5.



User device 510 receives the wellness data from the sensors, aggregates it with additional data from other sources, and displays the aggregated data. *Id.*, ¶226, ¶¶228-229, ¶¶251-252. Figure 9 shows such a display that is expandable into the interfaces of Figures 10-14:



Id., ¶¶252-258.

63. In my opinion, Soli is analogous art to the '228 patent because it relates to acquiring dynamic biometric information from a user and transmitting that information to another device, which uses that information to determine a user state and display information accordingly, as described above. I understand that the USPTO did not consider Soli during prosecution of the '228 patent. EX1001, pp. 1-2.

1. Soli Is Entitled to Its Provisional's Filing Date.

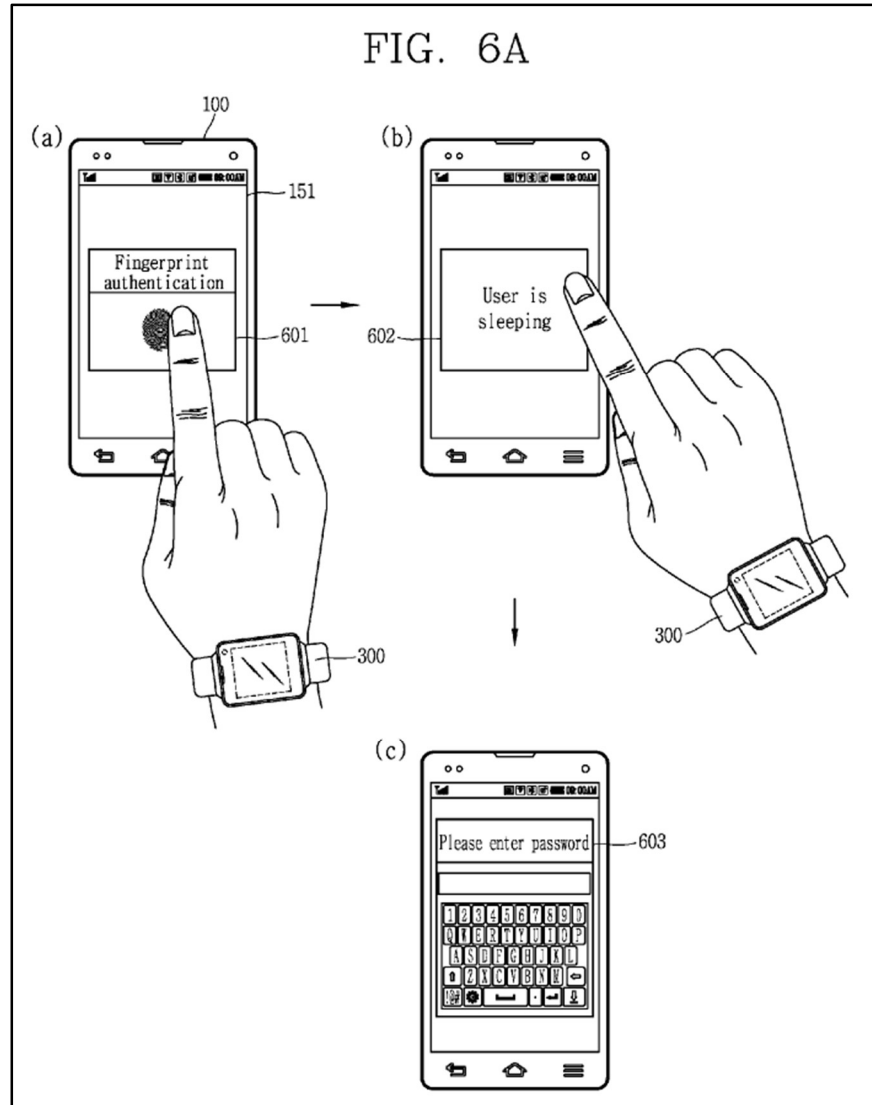
64. I understand from counsel that for the purpose of qualifying as prior art under the AIA, a patent that claims the benefit of an earlier provisional application will be deemed prior art as of the provisional application's filing date if the provisional application supports the subject matter relied upon.

65. I understand that Soli is prior art by virtue of its claim of priority to provisional application no. 62/006,032 (EX1007). EX1006, cover page. Soli's provisional application provides written description support for the cited portions of Soli, as established below using parallel citations to the provisional application.

D. Hong

66. U.S. Patent Application Publication No. 2015/0278498 ("Hong") was filed on August 25, 2014, and claims priority to a foreign application filed on March 28, 2014. EX1008, cover page. I understand that Hong is prior art under at least 35 U.S.C. § 102(a)(2) and (d).

67. Hong discloses "mobile terminals," including a smartphone and a "smart watch." EX1008, ¶51, ¶80, Figs. 1, 2B-D. The smartwatch determines whether the user is "sleeping" or in an "abnormal" "psychological state." *Id.*, ¶236. If so, the phone may request additional authentication for increased security, as shown below in Figure 6A. *Id.*, ¶¶236-237.



68. In my opinion, Hong is analogous art to the '228 patent because it relates to determining that the user is in a state matching a predetermined criteria and limiting the operation of the smartphone by seeking additional authentication from the user, as described above. *See* EX1001, 21:42-48 (claim 10). I understand that the USPTO did not consider Hong during prosecution of the '228 patent. *Id.*, pp. 1-2.

1. Hong Is Entitled to the Foreign Application's Filing Date.

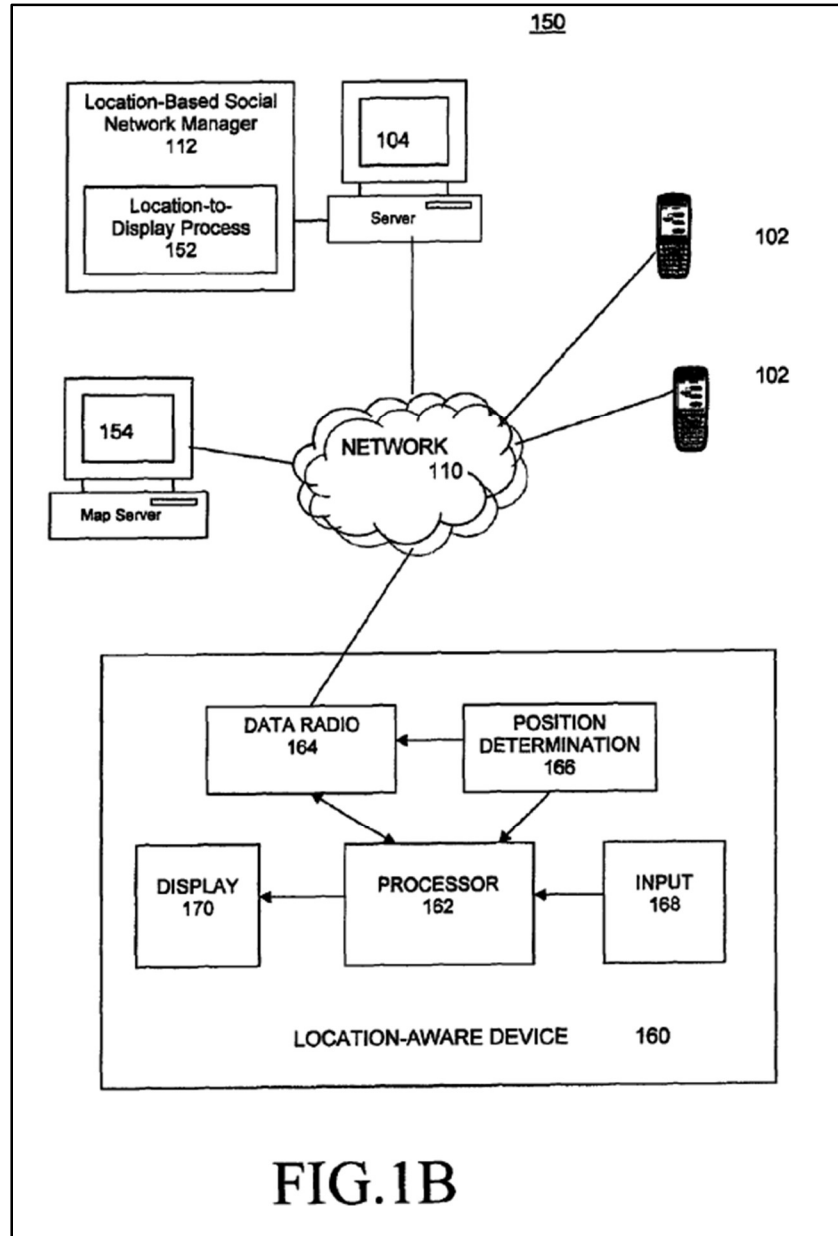
69. I understand from counsel that for the purpose of qualifying as prior art under the AIA, a patent that claims the benefit of an earlier filed foreign patent application will be deemed prior art as of the foreign application's filing date if the foreign application supports the subject matter relied upon.

70. I understand that Hong is prior art by virtue of its claim of priority to Korean Patent Application No. 10-2014-0037156. That application provides written description support for the cited portions of Hong, as established below using parallel citations to a certified translation of that foreign application (EX1009).

E. Altman

71. U.S. Patent No. 8,099,109 ("Altman") was filed on October 31, 2007, was published on June 5, 2008, and was issued on January 17, 2012. EX1010, cover page. I understand that Altman is prior art under at least 35 U.S.C. § 102(a)(1).

72. Altman discloses "a location-aware mobile device 160" that transmits its location to server 104, as shown below. EX1010, 6:16-37, Fig. 1B.



The device's location can be used to, for example, show that a friend is nearby or show location-based ads and coupons. *Id.*, 16:28-49, 21:48-61, Figs. 9, 15A-B. A user can turn his or her location sharing capabilities on and off. *Id.*, 10:61-65.

73. In my opinion, Altman is analogous art to the '228 patent because it relates to a device automatically transmitting its position information to a server

with a predetermined address, as described above. *See* EX1001, 21:26-35 (claim

8). I understand that the USPTO did not consider Altman during prosecution of the '228 patent. *Id.*, pp. 1-2.

VI. GROUND 1: CLAIMS 1-2, 4-7, 12-13, AND 15-18 ARE OBVIOUS IN LIGHT OF AMINZADE AND SOWERS

74. As set forth in greater detail below, in my opinion, claims 1-2, 4-7, 12-13, and 15-18 are obvious in light of Aminzade and Sowers.

A. Claim 1

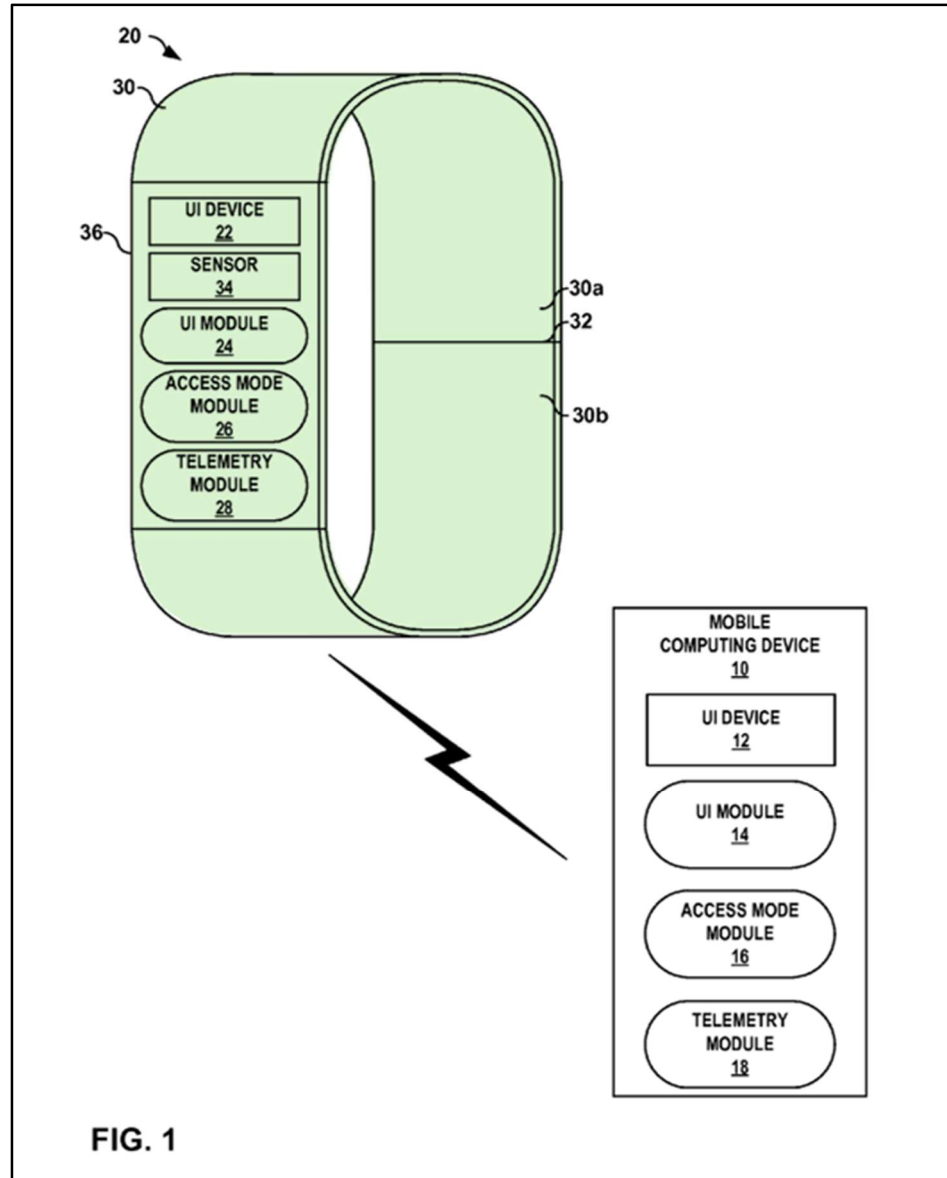
75. Aminzade combined with Sowers discloses and renders obvious claim 1.

2. [1.pre] (“A system, comprising:”)

76. Aminzade discloses this preamble. Aminzade discloses a “system including a mobile computing device 10 and a wearable computing device 20.” EX1004, 4:5-12, 4:18-22 (mobile device 10 may be a “smart phone[]”), 4:46-48 (wearable device 20 may be “a smart watch”), Fig. 1, Abstract.

3. [1.a] (“a first information processing device including:”)

77. Aminzade discloses this limitation. Aminzade discloses that wearable device 20 may be “a smart watch” (*a first information processing device*), shown below. EX1004, 4:46-48, 4:23-45, 5:35-6:23, Fig. 3, 14:35-18:31.

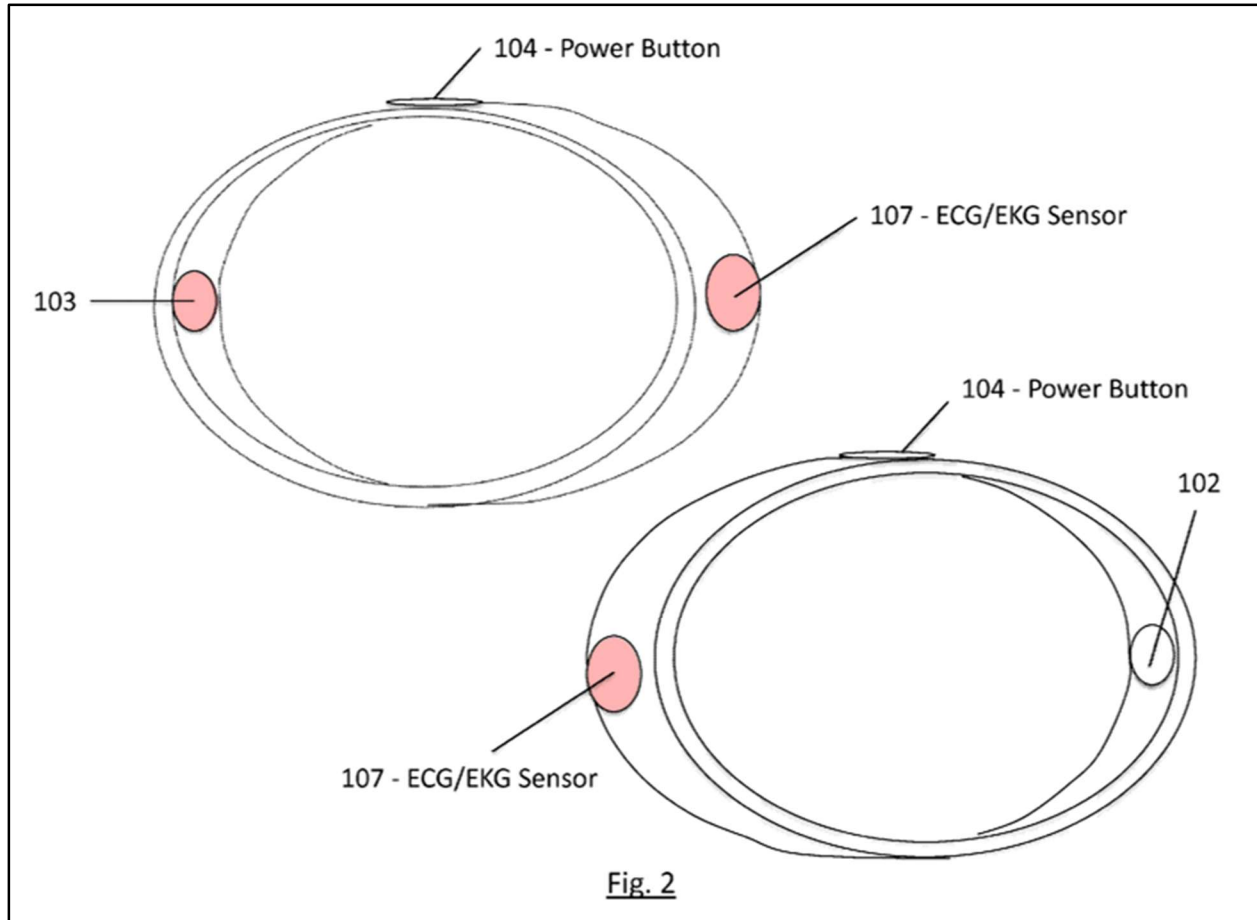


78. Wearable device 20 *process[es] information* such as an unlock instruction from mobile device 10. *See limitation 1.b.iii.*

4. [1.a.i] (“a dynamic biometric information acquisition sensor that acquires dynamic biometric information from a body of a user; and”)

79. Aminzade combined with Sowers discloses this limitation. Sowers discloses a “health monitoring device ... 101,” that is “attachable to a watch.”

EX1005, ¶15, ¶7, Figs. 1-2. Device 101 “monitor[s] ... heart rate, temperature, EKG measurements and blood characteristics” such as “the user’s concentration of oxy- and deoxy-hemoglobin,” and “data based on the user’s sweat” (each *dynamic biometric information from a body of user*). *Id.*, ¶15, ¶17 (“body temperature”), ¶¶23-24, ¶8. To do so, device 101 includes “one or more optical sensors 103” and “two ECG/EKG sensors 107” (each *a dynamic biometric information acquisition sensor*), annotated below. *Id.*, ¶15, ¶23, ¶¶7-8, Figs. 1-2.



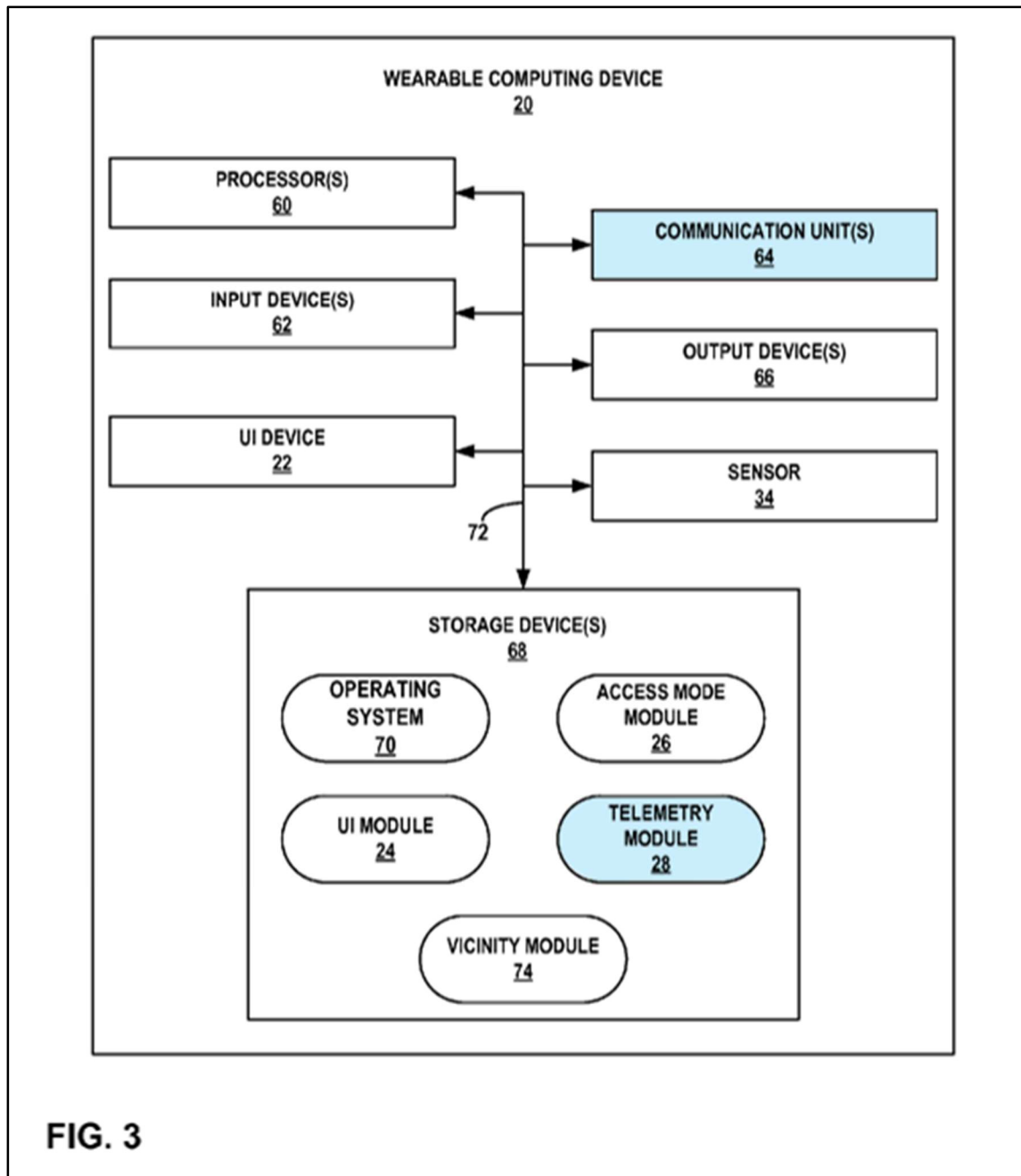
80. The sensors *acquire* these health characteristics “[w]hen the device [101] is worn by a user” (*from a body of a user*). EX1005, ¶¶23-24. Specifically,

optical sensor 103 uses light emitted onto the user's skin to "gather data from the user's blood characteristics." *Id.*, ¶8, ¶23. It also "collects data based on the user's sweat." *Id.*, ¶17, ¶24. The ECG/EGK sensors "measure the heart's electrical activity" by "measuring voltage changes on the surface of the skin" when "the user applies his thumbs to both ECG/EKG sensors 107." *Id.*, ¶4, ¶24, ¶8.

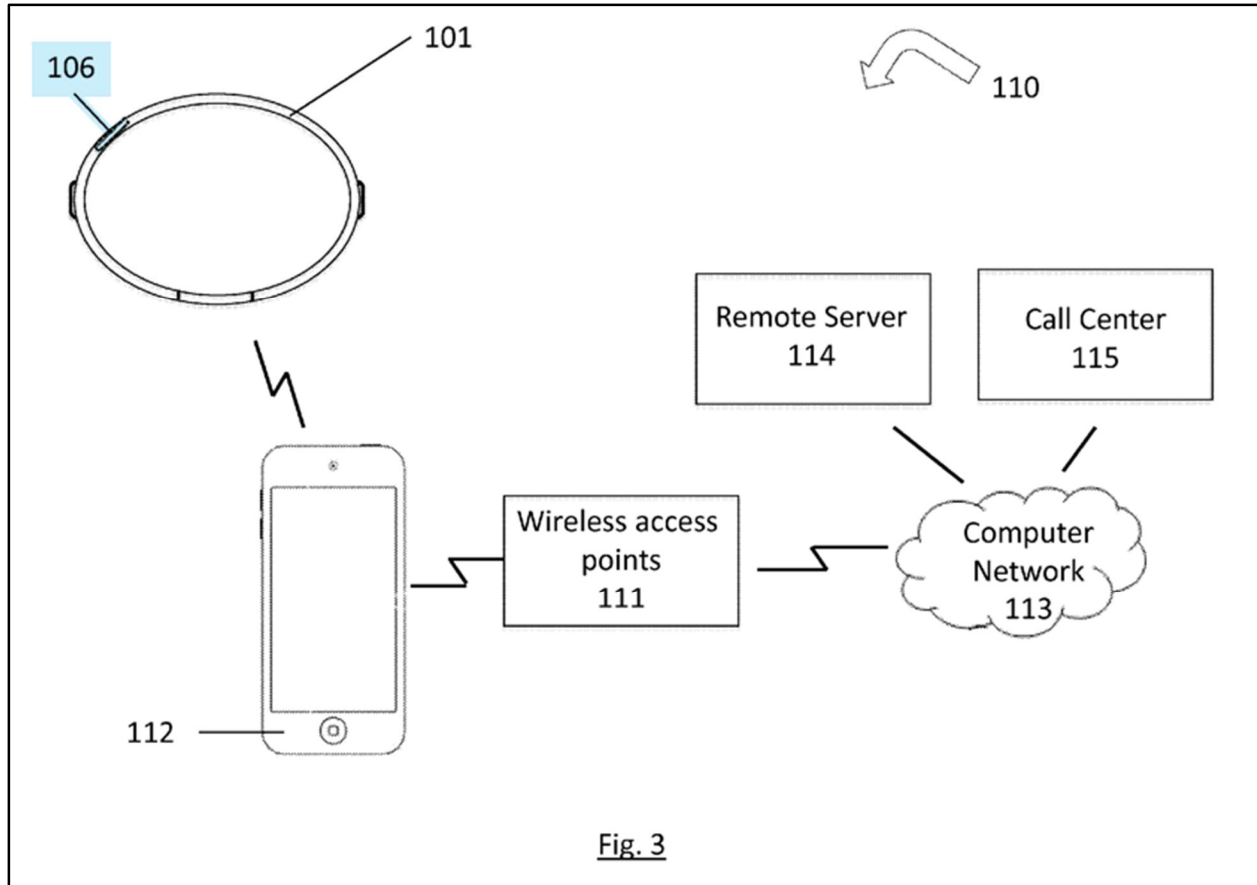
81. In my opinion, it also would have been obvious to a POSITA to combine this functionality of Sowers with Aminzade for the reasons in Section VI.M.

5. [1.a.ii] ("a first communication interface that transmits the acquired dynamic biometric information; and")

82. Aminzade combined with Sowers discloses this limitation. Aminzade's wearable device 20 (*a first information processing device*) includes "telemetry module 28" and "communication unit 64" (each *a first communication interface*) "to communicate with external devices via ... wireless networks." EX1004, 6:15-23, 15:34-37, Fig. 3 (shown below). Communication unit 64 may be a "network interface[]" and "can be controlled by telemetry module 28." *Id.*, 15:37-47. Telemetry module 28 combined with communication unit 64 also is a *first communication interface* for the same reasons as each individually.



83. Sowers's device 101 *acquire[s] dynamic biometric information*. See limitation 1.a.i. Device 101 also includes “wireless transmitting device 106”/“wireless communication device 106” (also *a first communication interface*), shown below in Figure 3. EX1005, ¶19, ¶15.



Transmitting device 106 “communicate[s] wirelessly with the base station 112,” which can be a “smart phone 112.” *Id.*, ¶¶19, 18, Fig. 3. The wearable device “transmits the health data to [the] smartphone.” *Id.*, Abstract, ¶25 (“The data collected by the [sensors] is then sent to the base station 112.”), ¶26 (“base station 112 receives [health] data from the device 101 via the wireless communication device 106”), ¶20 (“via ... transmitting device 106”), Fig. 3. Thus, device 101’s transmitting device 106 *transmits the acquired dynamic biometric information* to smartphone 112.

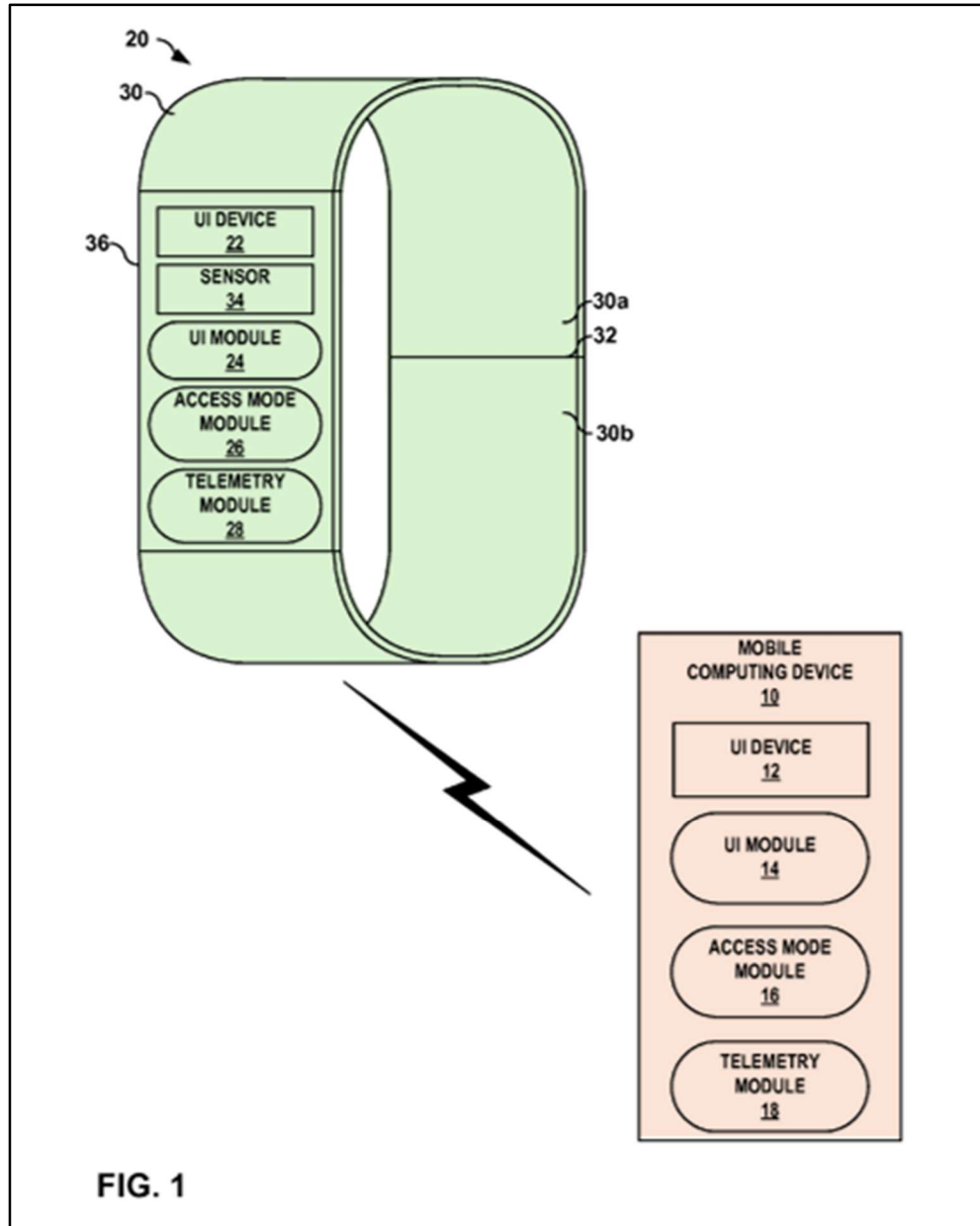
84. In my opinion, it also would have been obvious to a POSITA to

combine this functionality of Sowers with Aminzade for the reasons in Section

VI.M.

6. [1.b] (“a second information processing device including:”)

85. Aminzade discloses this limitation. Aminzade discloses that mobile device 10 may be a “smart phone[]” (*a second information processing device*), annotated orange below. EX1004, 4:18-22, 4:5-12, 4:49-5:35, Fig. 2, 9:48-14:34 (describing Figure 2).

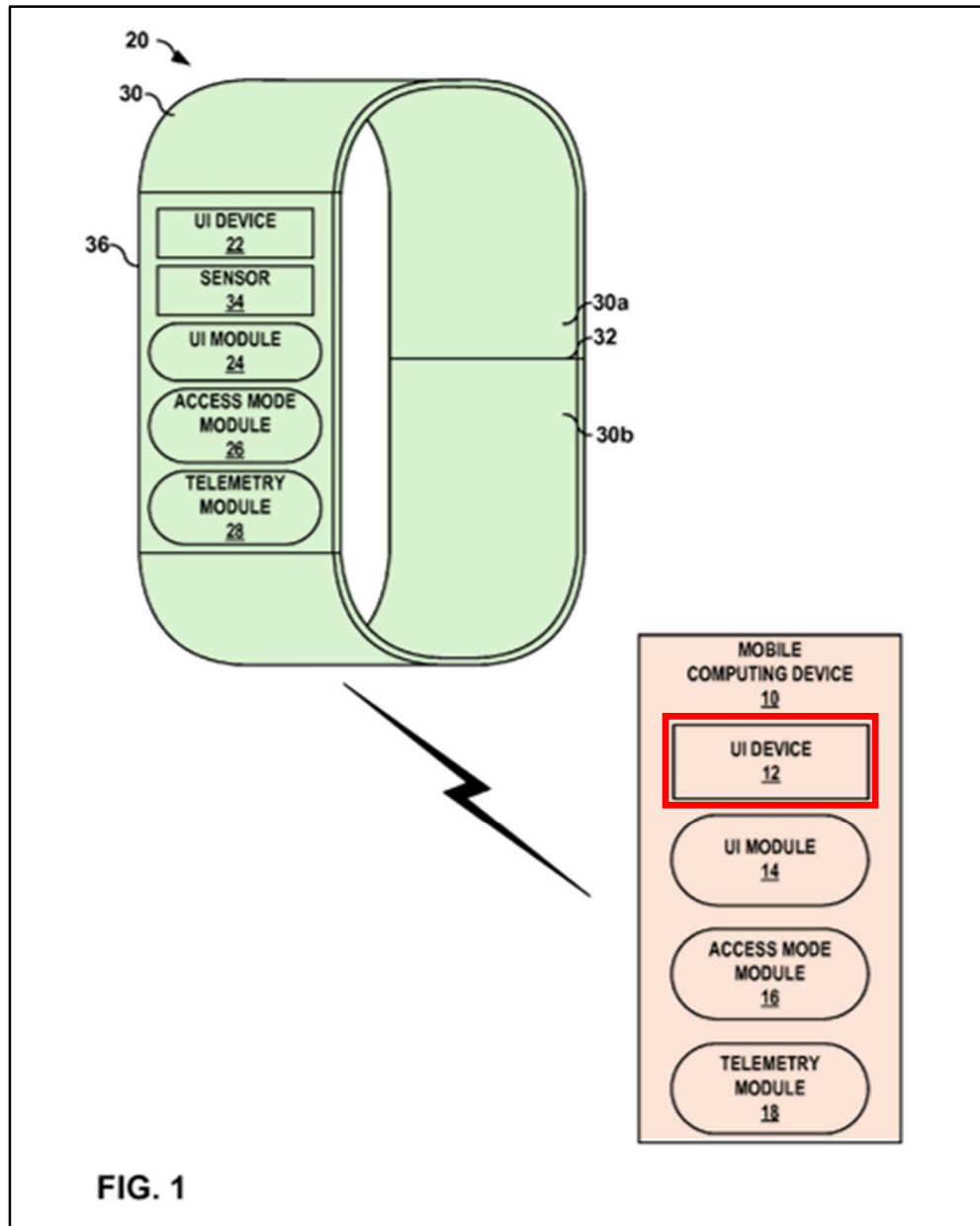


Mobile device 10 *process[es] information* such as the user's fingerprint. See limitation 1.b.iii.

7. **[1.b.i] (“a static biometric information acquisition sensor that acquires static biometric information;”)**

86. Aminzade discloses this limitation. Aminzade discloses that mobile device 10 (the *second information processing device*) includes “UI device 12,”

annotated below.



UI device 12 “prompts a user of mobile computing device 10 to input a security challenge response, such as ... biometric data (e.g., fingerprint, voice, image, or the like), etc.” (*acquires static biometric information*). EX1004, 13:58-63, Fig. 6 (step 126), 21:38-42, 8:34-43. The '228 patent confirms that fingerprint data and

image (facial) data each are *static biometric information*. EX1001, 5:56-60, 6:15-17, 7:15-21, 16:46-50, 21:4-7.

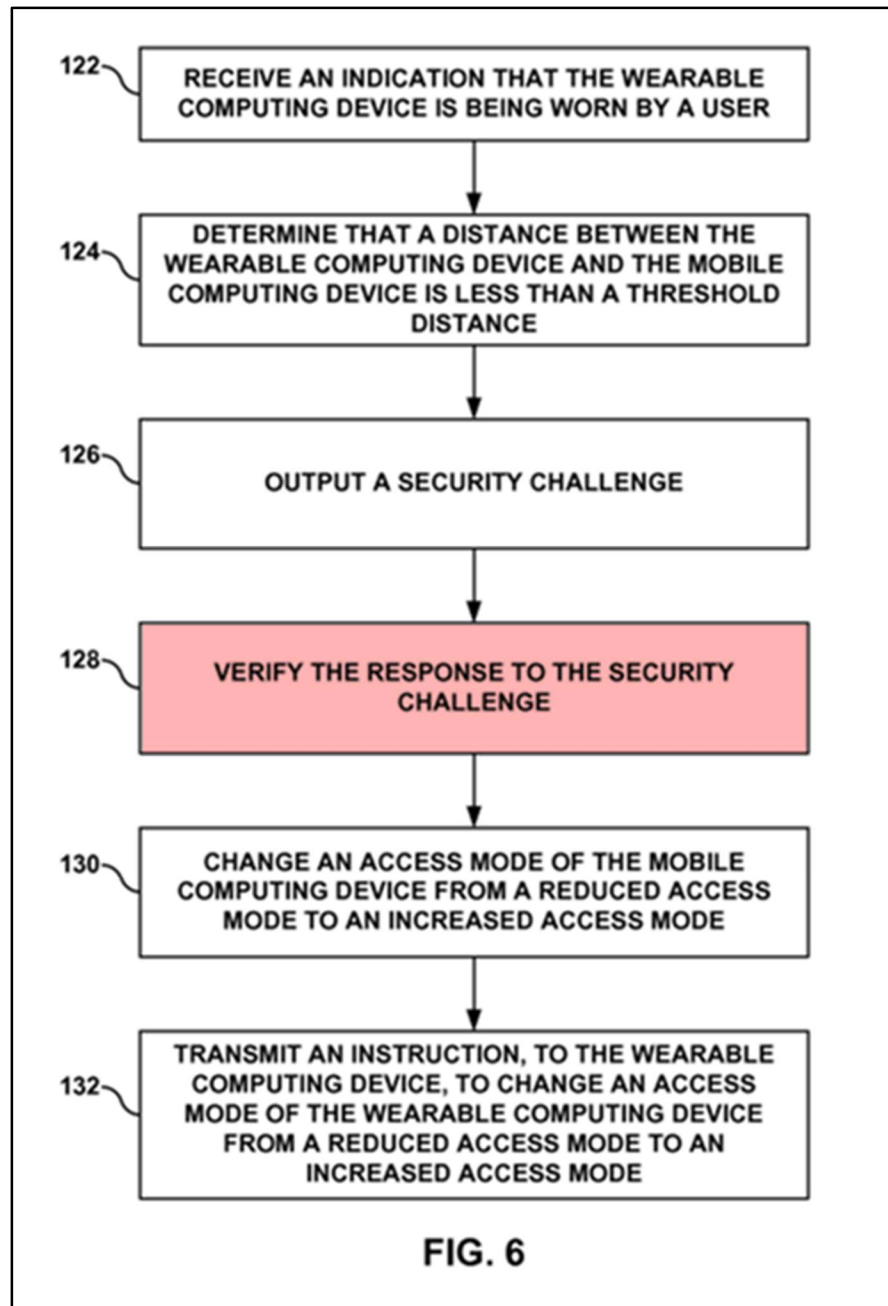
87. UI device 12 is *a static biometric information acquisition sensor* because it acquires and senses static biometric information such as user fingerprint data or image (facial) data, as described above. EX1004, 11:17-27. A POSITA also would have understood that mobile device 10 necessarily (inherently) includes *a static biometric information acquisition sensor* to receive the user's fingerprint or image data. UI device 12 combined with "UI module 14" also is *a static biometric information acquisition sensor* for the same reasons. *Id.*, 13:58-63 (the "user interface screen [is] output at UI device 12 by UI module 14").

8. [1.b.ii] ("a processor that performs user authentication based on the acquired static biometric information and obtains an authentication result;")

88. Aminzade discloses this limitation. Aminzade discloses *acquired static biometric information* in the form of a "fingerprint, voice, image, or the like." *See* Ground 1, limitation 1.b.i.

89. User Authentication. Aminzade discloses that mobile device 10 includes "access mode module 16" (also referred to as "access control module 16"). EX1004, 7:26-28, 13:63-14:6, Fig. 2. Access mode module 16 "output[s] [the] security challenge" referenced above for limitation 1.b.i. *Id.*, 13:53-63, 8:34-43. It also "receiv[es] the input security challenge response" (*acquired static*

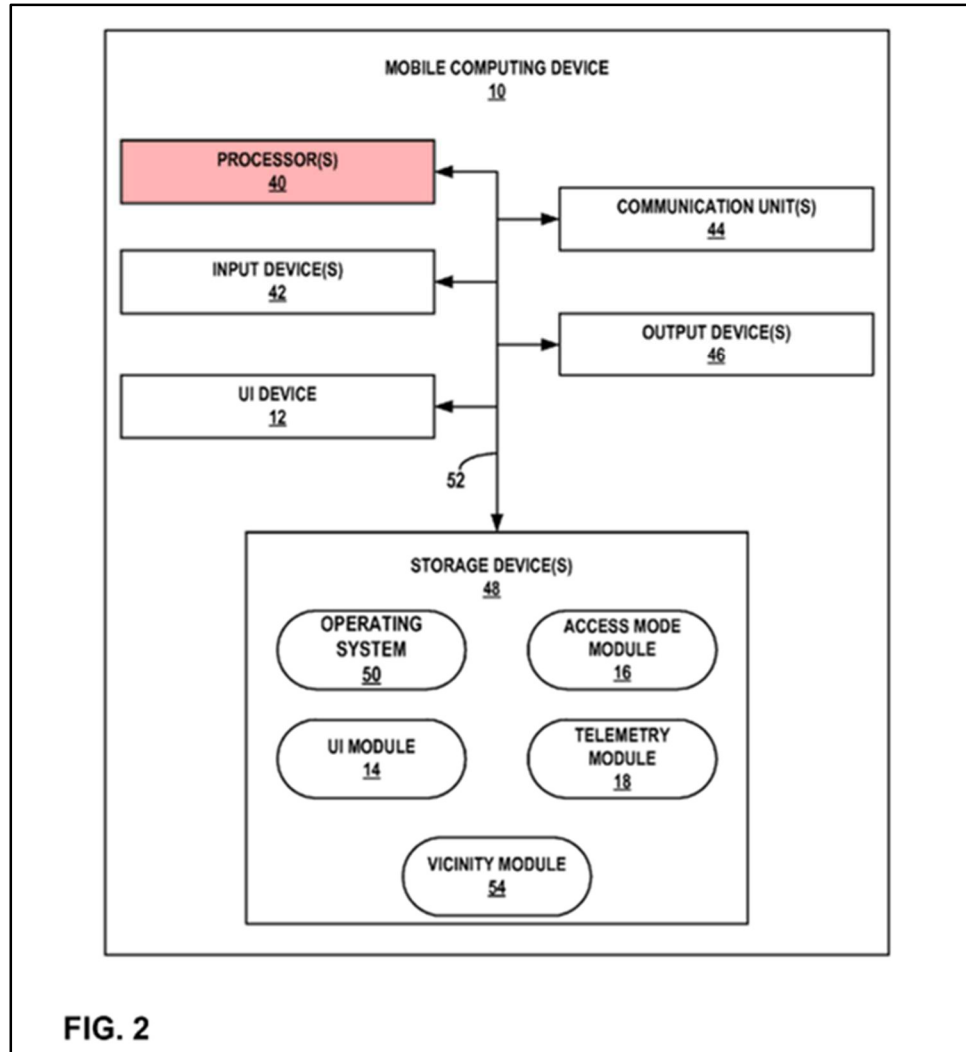
biometric information such as fingerprint information) and “verif[ies] the security challenge response against a stored security challenge response” (*performs user authentication based on the acquired static biometric information*). *Id.*, 13:63-14:1, 8:43-46, 19:35-39. This *authentication* is reflected in step 128 of Figure 6, shown below.



90. Upon verification (*an authentication result*), access control module 16 changes the mobile device's access mode "from the reduced access mode to an increased access mode." EX1004, Fig. 6 (step 130), 21:56-61, 7:6-12, 14:1-7; *see also id.*, 1:29-30 ("upon confirming a match" (*an authentication result*)), 8:67

(“the ... verification” (*an authentication result*)). In my opinion, a POSITA also would have understood that this functionality of Aminzade implicitly and inherently (necessarily) includes determining that the *acquired static biometric information* (e.g., a fingerprint) matches (*an authentication result*) the stored security challenge response.

91. A Processor. Aminzade’s mobile device 10 includes “processors 40” (collectively and individually *a processor in the first information device*) shown below. EX1004, 10:8-18.



Processors 40 execute the user authentication described above. For example, “access mode module 16 can ... [be] executable by ... one or more processors 40.” *Id.*, 11:53-56, 21:61-63 (“the technique of FIG. 6 is performed by one or more processors 40 of mobile computing device 10”), 21:38-51 (processors 40 can implement Figure 5 [sic, 6], including “verifying the response to the security

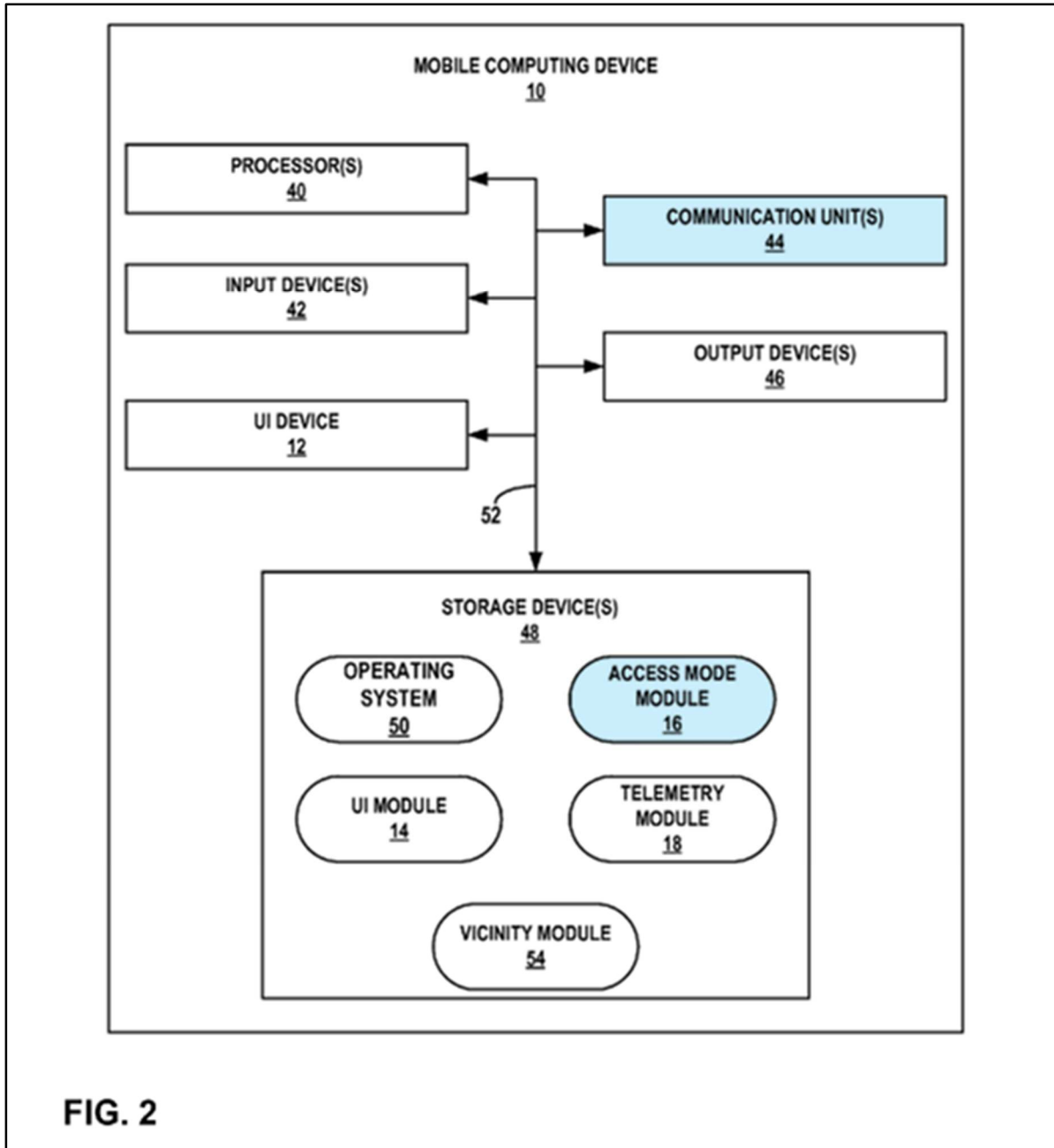
challenge”).¹ Also, access mode module 16 “can be implemented as [an] application.” In my opinion, a POSITA would have understood that such an application would execute on processors 40. *Id.*, 6:60-67.

9. [1.b.iii] (“a second communication interface that performs communication relating to the authentication result with the first communication interface and receives the dynamic biometric information transmitted from the first communication interface; and”)

92. Aminzade combined with Sowers discloses this limitation.

93. A Second Communication Interface. Aminzade’s mobile device 10 includes “telemetry module 18” and “communication unit 44” (each *a second communication interface*) “to communicate with external devices via ... wireless networks.” EX1004, 5:27-35, 10:46-50. Communication unit 44 may be a “network interface[]” and “may be controlled by telemetry module 18.” *Id.*, 10:50-60. Telemetry module 18 combined with communication units 44 also is a *second communication interface* for the same reasons as each individually.

¹ Although this passage refers to the “technique of Fig. 5,” this appears to be a typographical error because it refers to numbered elements of Figure 6.

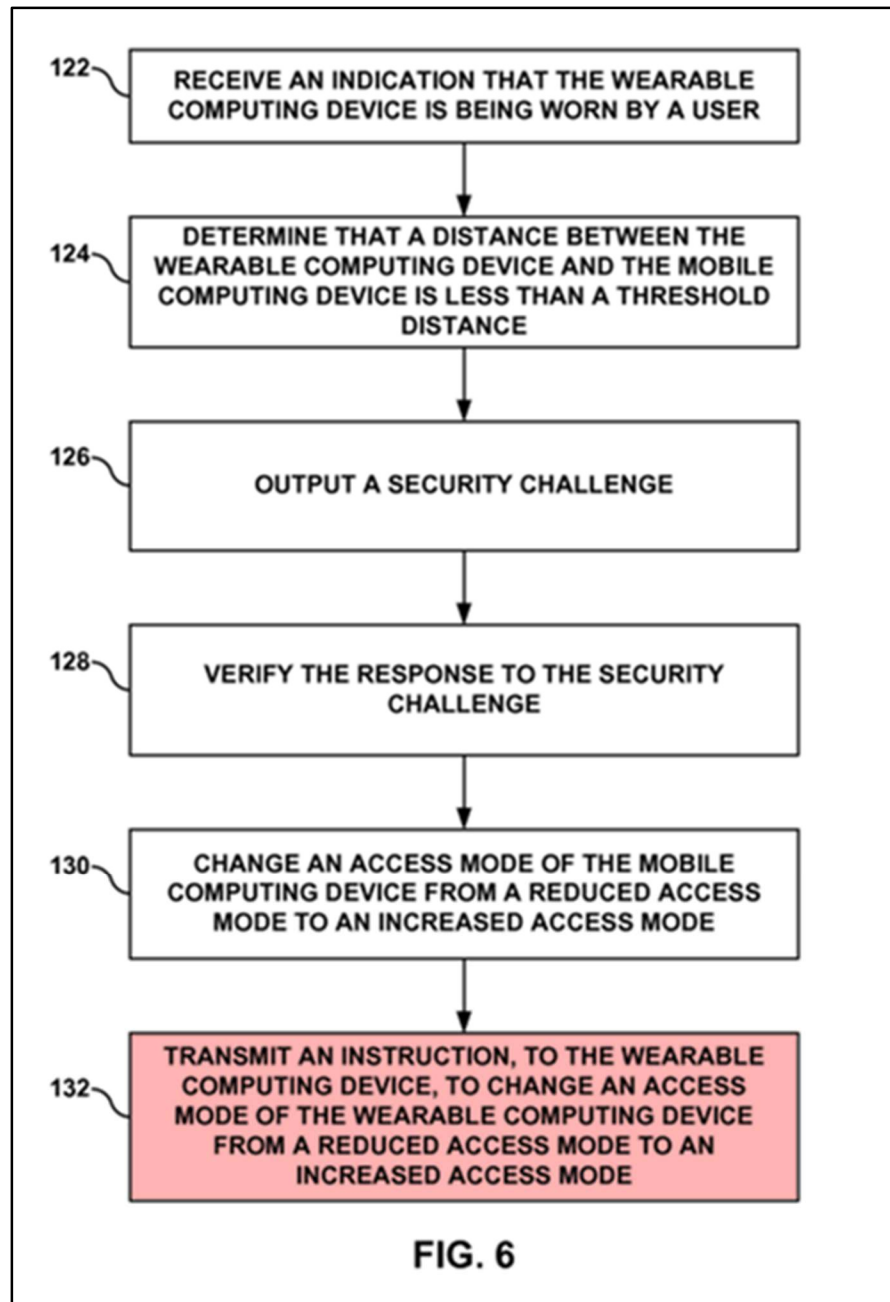


94. Telemetry module 18 communicates with the telemetry module 28 (a *first communication interface*) of wearable device 20, and vice versa. EX1004, 7:50-58 (“a wireless communication signal generated by telemetry module 18 and received by telemetry module 28, and [vice versa]”), 5:32-35, 6:21-23, 7:43-50,

Fig. 1.

95. Communication Relating to the Authentication Result. As described for limitation 1.b.ii, Aminzade discloses verification (*the authentication result*) that the user's security challenge response (*e.g.*, a fingerprint) matches a stored security challenge response.

96. Upon such verification, mobile device 10 transmits to wearable device 20 "an instruction to change an access mode ... from a reduced access mode to an increased access mode" (*performs communication relating to the authentication result*). EX1004, 21:52-61, 14:1-14 (same), 8:46-60, Fig. 6 (step 132, highlighted below).



“[T]elemetry module 18, using communications units 44” (each *a second communication interface*) transmits the “instruction to change [the] access mode” to the wearable device 20. *Id.*, 14:1-14. Such communication is received by telemetry module 28 and communication unit 64 (each *first communication*

interface) on the wearable device 20, as described above. *Id.*, 7:50-58, 15:43-47.

It also would have been obvious to a POSITA to have telemetry module 28 and communication unit 64 receive the instruction from telemetry module 18 and communications units 44 as a matter of symmetry, and in light of Aminzade's disclosures that they are used for wireless communication between the two devices, described above.

97. Receiving the Dynamic Biometric Information. Aminzade's wearable device 20 includes *a first communication interface*. See limitation 1.a.ii.

98. As also described for limitation 1.a.ii, Sowers's device 101 *transmit[s] dynamic biometric information* from its "wireless transmitting device 106" (also a *first communication interface*) to smartphone 112. Smartphone 112 includes "a transceiver capable of communicating using a wireless protocol" (also a *second communication interface*). EX1005, ¶18. In my opinion, a POSITA would have understood that smartphone 112's wireless transceiver *receives the dynamic biometric information transmitted from* device 101 and its "wireless transmitting device 106," especially because Sowers discloses no other component for wireless communication in smartphone 112. *Id.*, ¶26 (base station/smartphone 112 "receive[s] [health] data" from wireless communication device 106).

99. In my opinion, it would have been obvious to a POSITA to combine this functionality of Sowers with Aminzade for the reasons in Section VI.M.

10. [1.b.iv] (“a display screen,”)

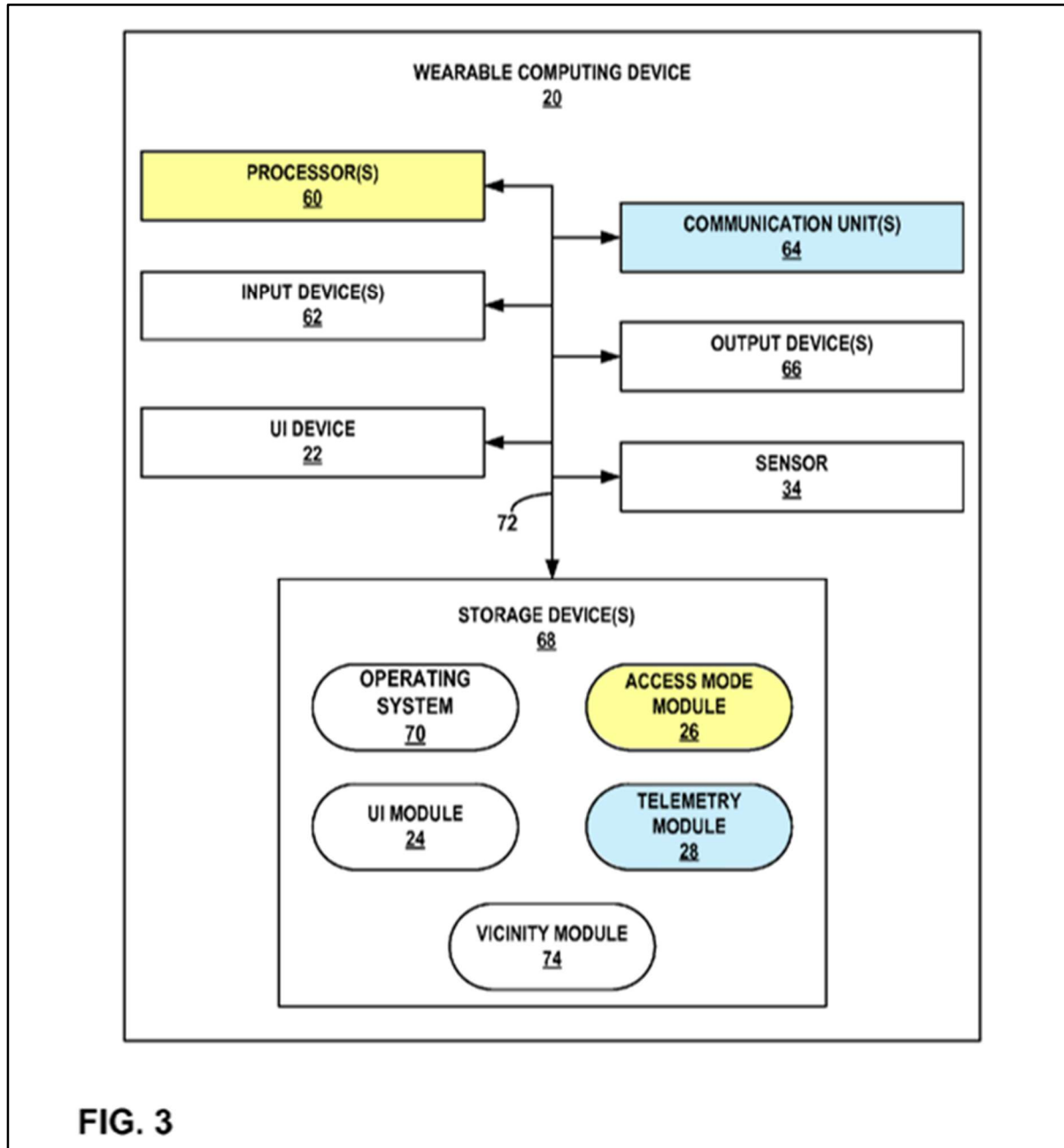
100. Aminzade discloses this limitation. Aminzade’s mobile device 10 (*second information processing device*) includes a “at least one UI device 12” that can “include a display” (*a display screen*) for displaying “a graphical user interface (GUI).” EX1004, 4:49-64, Fig. 1.

11. [1.c] (“wherein the first information processing device: performs communication relating to the authentication result between the first communication interface and the second communication interface and executes an unlock operation to unlock itself in response to the communication relating to the authentication result,”)

101. Aminzade discloses this limitation. As described for limitation 1.a, Aminzade discloses that wearable device 20 may be “a smart watch” (*a first information processing device*).

102. Communication Relating to the Authentication Result. As described for limitation 1.b.iii, Aminzade discloses that, as a result of verification of the user’s security challenge response (*e.g.*, a fingerprint), mobile device 10 transmits to the telemetry module 28 and communication unit 64 (*first communication interfaces*) of wearable device 20 an “instruction” to increase the wearable device’s access mode. Because the instruction is received at the *first communication interface* from the mobile device’s *second communication interface*, as described for limitation 1.b.iii, it is *between* the two interfaces. Wearable device 20 includes “access mode module 26” that executes on processor 60, both shown below, and

“control[s]” the device’s access mode, including changing it to an “increased access mode.” EX1004, 14:46-51, 7:6-19, 17:17-21, Fig. 3.



In Figure 3, components 60, 64, and 68 are coupled “physically, communicatively, and/or operatively) using communication channels 72 for inter-component

communications,” and components 26 and 28 “may also communicate information with one another.” *Id.*, 14:51-61. A POSITA would have understood that Aminzade implicitly and necessarily (inherently) discloses that communication unit 64 and telemetry module 28 *perform communication* of the instruction (which *relat[es] to the authentication result*) to access mode module 26 and processor 60 on which it executes, such as being communicated via channel 72. Otherwise, access mode module 26 and processor 60 could not give effect to the instruction, contrary to Aminzade’s disclosure of increasing the access mode, described below. *See also* § IV.A (“performs communication” includes communication within a device).

103. In addition, the receipt of the instruction (which *relat[es] to the authentication result*) by telemetry module 28 and communication unit 64 (*first communication interfaces*) also *performs communication*. *See* § IV.A (“performs communication” includes receiving data). And because that *communication* is received at the *first communication interface* from the *second communication interface*, it is *between* the interfaces. *See* Ground 1, limitation 1.b.iii.

104. An Unlock Operation. Aminzade also discloses that, in “increased access mode,” “the computing environment ... permit[s] the user to access a larger or complete set of functionality provided by the device” “without having to respond to another security challenge each time the user wants to interact with the

device” (*unlock* the device). EX1004, 7:16-19, 3:35-38, 3:63-4:4; § IV.B (construing “unlock”).

105. Aminzade also discloses that “access mode module 26” in wearable device 20 “control[s]” the device’s access mode and can “control” the device to be an “increased access mode” (*executes an unlock operation to unlock itself*). EX1004, 7:6-19, 17:17-21, Fig. 3. Similarly, Aminzade discloses that “[t]he technique of FIG. 5 may be performed by one or more processors of ... wearable computing device 20,” and the same for Figure 4. *Id.*, 20:5-8, 18:38-42. Each of Figures 4 and 5 includes changing the wearable device’s access mode to “an increased access mode.” *Id.*, Fig. 4 (step 90), Fig. 5 (step 110). Aminzade therefore discloses that such an increase in the access mode is performed by the wearable device’s processors (*executes an unlock operation to unlock itself*).

106. Likewise, the “instruction” to change to “increased access mode” referenced above is transmitted “to one or more processors 60 of wearable computing device 20,” which, in my opinion, a POSITA would have understood to mean the processors 60 carry out the instruction (*execute[] an unlock operation to unlock itself*). EX1004, 21:56-61. A POSITA would have understood that the disclosed “instruction” to the wearable device 20 to change its access mode “to an increased access mode” necessarily (inherently) results in the wearable device 20 changing its access mode accordingly (*executes an unlock operation to unlock*

itself in response to the communication relating to the authentication result).

Otherwise, the instruction would have no effect. The *unlock[ing]* occurs in response to the wearable device 20 receiving the instruction (*the communication relating to the authentication result*), as described above.

12. [1.d] (“acquires the dynamic biometric information from the dynamic biometric information acquisition sensor after unlocking, and”)

107. Aminzade combined with Sowers discloses and renders obvious this limitation.

108. Acquiring Information from the Sensors. Sowers’s wearable device includes “optical sensors 103” and “ECG/EKG sensors 107” (each *a dynamic biometric information acquisition sensor*). See limitation 1.a.i.

109. Sowers also discloses transmitting the sensor’s health data (*the dynamic biometric information*) from the wearable device’s “wireless communication device 106” to smartphone 112. See limitation 1.a.ii. In my opinion, a POSITA would have understood that doing so implicitly and necessarily (inherently) requires *acquir[ing]* the health data (*dynamic biometric information*) from the sensors in order to transmit it. For example, “wireless communication device 106” necessarily (inherently) would first acquire the data from the sensors to transmit it, as Sowers discloses. Sowers also discloses “stor[ing]” the health data before transmission, which a POSITA would have understood requires first

acquir[ing] that health data. EX1005, ¶25. The health data from the sensors is “digitized into a time-dependent optical waveform” before being transmit, which also necessarily (inherently) requires first *acquir[ing]* it from the sensors. *Id.*, ¶25, ¶8.

110. After Unlocking. Aminzade discloses *unlocking* its wearable device 20. *See* limitation 1.c.

111. Sowers discloses “continuous monitoring of [a user’s] health information” via “[d]ata measured continuously through the day.” EX1005, ¶34, ¶6 (“continuous monitoring”). A POSITA would understand that this “health information” includes the health data acquired from “optical sensors 103” and “ECG/EKG sensors 107” because those are Sowers’s enumerated sensors. Sowers’s wearable device 101 continuously transmits the acquired health information to smartphone 112 when in range, and stores the data when not in range. *Id.*, ¶25 (“device 101 continues to detect and store data” and “automatically transmits all the stored data to the base station 112” when “in close enough proximity”); *see also* limitation 1.a.ii. Because the storing and transmission of such health data requires first *acquir[ing]* it, as established above, Sowers discloses *acquir[ing]* it continuously through the day. It also would have been obvious to a POSITA acquire the sensor health data “continuously through the

day” to achieve a “relatively comprehensive data set” and “to monitor trends in the data that may indicate a medical condition.” *Id.*, ¶34.

112. In my opinion, it would have been obvious to a POSITA to combine this functionality of Sowers with Aminzade for the reasons in Section VI.M.

113. Upon combining Sowers with Aminzade as set forth above, wearable device 20 still would *acquire* the health data from the sensors (*dynamic biometric information*) “continuously through the day.” EX1005, ¶34. This would include doing so *after unlocking* because the word “after” refers to chronology, not causality. In my opinion, it also would have been obvious to a POSITA to keep doing so *after unlocking* for the reasons above and in Section VI.M.

13. [1.e] (“maintains the unlocked state during a condition that the dynamic biometric information can be acquired,”)

114. Aminzade combined with Sowers discloses this limitation. As described for limitation 1.d, Sowers’s wearable device 101 *acquires dynamic biometric information* from its sensors of its “continuously through the day,” including when worn “in close enough proximity” to smartphone 112 to wirelessly transmit the sensor data to the smartphone (*a condition that the dynamic biometric information can be acquired*). *See also* EX1005, ¶25 (proximity transmission), ¶26 (wirelessly), ¶8 (sensors operating when “worn by a user”), ¶23 (same).

115. Aminzade discloses unlocking wearable device 20 after authenticating the user’s fingerprint. *See* limitation 1.c. The wearable device “remain[s] in the

increased access mode[]” (*maintains the unlocked state*) “while the wearable computing device is worn by the user and” is “within a threshold distance of” the “mobile computing device” that allows for wireless communication between the two (*during the condition* described above). EX1004, 3:39-43, 3:57-4:3, 3:14-17 (“threshold distance [that allows] wireless communication coupling between the devices”), 7:43-67 (same).

116. In my opinion, it would have been obvious to a POSITA to combine this functionality of Sowers with Aminzade for the reasons in Section VI.M.

- 14. [1.f] (“wherein the second information processing device receives the dynamic biometric information via communication between the first communication interface and the second communication interface and the display screen displays information based on a state of the user that is determined using the received dynamic biometric information.”)**

117. Aminzade combined with Sowers discloses this limitation. Aminzade combined with Sowers discloses *a second communication interface of the second information processing device that receives the dynamic biometric information from the first communication interface, i.e., via communication between the first communication interface and the second communication interface. See limitation 1.b.iii.*

118. Displaying Information Based on a State of the User. Sowers discloses that its base station/smartphone 112 “analyzes” the data received from

the dynamic biometric sensors along with other data to “generate[] health information” (a *determin[ation]* using the received dynamic biometric information). EX1005, ¶¶26-27. The “health information” includes “the user’s risk of heart attack,” “the user’s risk of stroke,” and “the user’s blood alcohol content” (each *information based on a state of the user that is determined using the received dynamic biometric information*), among other health information based on the user’s state. *Id.*, ¶27, ¶10. “The health information generated ... may be viewed on a visual display of the base station 112.” *Id.*, ¶28 (a *display screen* that *displays the information*), Abstract (“review [the] health information on the base station’s display”).

119. Also, smartphone 112 “may generate a warning or alert if the user’s health information reflects a dangerous condition or a statistically significant aberration ... based on an analysis of one or more data parameters using any type of algorithm” (also *information based on a state of the user that is determined using the received dynamic biometric information*). EX1005, ¶31, ¶30. The “health information” includes the “health information collected by the device 101,” which includes the *dynamic biometric information* identified for limitation 1.a.i, such as heart rate and body temperature.

120. In my opinion, it would have been obvious to a POSITA to *display* such a warning or alert on the *display screen*. Motivation to do so arises from a

desire to maximize the chances that the user sees the warning or alert. More motivation arises from Aminzade's disclosure of displaying the "health information," such as risk of heart attack or stroke, described above. *See also* EX1005, ¶29 (view health data on the display), ¶20 (monitor health data on the display). Motivation also arises from Aminzade's disclosure of an increased access mode on its mobile device 10, described for limitation 1.b.ii, which would have led a POSITA to allow a user access Sowers's health information via the *display screen*.

121. Aminzade also discloses a *display screen* of its mobile device 10 (*second information processing device*). *See* limitation 1.b.iv.

122. In my opinion, it would have been obvious to a POSITA to combine this functionality of Sowers with Aminzade for the reasons in Section VI.M.

B. Claim 2 ("The system according to claim 1, wherein the first communication interface and the second communication interface are Bluetooth interfaces and communication between the first communication interface and the second communication interface is Bluetooth wireless communication.")

123. Aminzade discloses this limitation. *See* limitation 1.a.ii (*first communication interface*), limitation 1.b.iii (*communication between it and a second communication interface*). Aminzade also discloses that such communication can be via "Bluetooth" (*Bluetooth wireless communication*). EX1004, 6:38-44, 5:27-35, 6:15-23, 7:48-50, 10:54-56, 15:41-43, 22:34-41.

Accordingly, in my opinion, a POSITA would have understood that Aminzade implicitly and necessarily (inherently) discloses that the *first* and *second communication interfaces* can be Bluetooth interfaces because otherwise the disclosed “Bluetooth” communication would not be possible.

- C. **Claim 4 (“The system according to claim 1, wherein the dynamic biometric information is one of heart rate, pulse, blood pressure, body temperature, amount of sweating, or brain wave and the static biometric information is one of finger print information, facial recognition information, retina information, vein information, or iris information.”).**

124. Aminzade combined with Sowers discloses and renders obvious this limitation. Aminzade discloses that *the static biometric information* can be a “fingerprint” (*finger print information*) or an “image,” which a POSITA would have understood to refer to *facial recognition information*. See limitation 1.b.i.

125. Sowers discloses that *the dynamic biometric information* can be “heart rate” (*heart rate*). See limitation 1.a.i; EX1005, ¶4, ¶15. My analysis of claim 1 above explains how Sowers discloses the “dynamic biometric information” limitations of claim 1 when *the dynamic biometric information* is the user’s *heart rate*. The analysis explains how the *heart rate* information is acquired, transmitted, received, and used (potentially along with additional information) to determine a state of the user, as recited by claim 1. Regarding limitation 1.f, Sowers discloses determining “if the user’s health information reflects a dangerous condition or a statistically significant aberration” (*a state of the user*) where the

“health information” includes the “heart rate” (*using the received dynamic biometric information*). See limitation 1.f. In my opinion, it also would have been obvious to a POSITA to base such a determination at least in part on the user’s “heart rate” because it is a key “health characteristic” collected by device 101. EX1005, ¶15. Because the preamble of claim 1 uses the transition phrase “comprising,” claim 4 does not prohibit acquiring, transmitting, receiving, or using additional data along with the *heart rate* information.

126. Sowers also discloses that *the dynamic biometric information* can be “temperature”/“body temperature” (*body temperature*). EX1005, ¶15, ¶17. The analysis in the paragraph above regarding “heart rate” also applies equally to “body temperature.”

127. In my opinion, it would have been obvious to a POSITA to combine this functionality of Sowers with Aminzade for the reasons in Section VI.M.

D. Claim 5 (“The system according to claim 1, wherein the first information processing device is a wearable device that acquires the dynamic biometric information at least by being physically in contact with the body.”)

128. Aminzade combined with Sowers discloses this limitation. Aminzade’s wearable device 20 (*a first information processing device*) is a “wearable ... device.” See limitation 1.a.

129. Sowers’s device 101 *acquires dynamic biometric information* when “worn by a user” (*by being physically in contact with the body*), as also described

for limitation 1.a.i.

130. In my opinion, it would have been obvious to a POSITA to combine this functionality of Sowers with Aminzade for the reasons in Section VI.M.

E. Claim 6 (“The system according to claim 1, wherein the first information processing device is a smartwatch and the second information processing device is a smartphone or tablet.”)

131. Aminzade discloses this limitation. Aminzade’s wearable device 20 (*a first information processing device*) may be “a smart watch.” See limitation 1.a.i. Aminzade’s mobile device 10 (*a second information processing device*) may be a “smart phone[]” or “tablet.” EX1004, 4:18-22; *see also* limitation 1.b.

F. Claim 7 (“The system according to claim 1, wherein the first information processing device continuously acquires the dynamic biometric information after being unlocked and the second information processing device receives the dynamic biometric information transmitted from the first communication device continuously or based on starting of an application on the second information processing device.”)

132. Aminzade combined with Sowers discloses this limitation. Aminzade combined with Sowers discloses the *first information processing device* “continuous[ly]” *acquir[ing] the dynamic biometric information after being unlocked*. See limitation 1.d.

133. Aminzade combined Sowers also discloses *the second information processing device receiv[ing] the dynamic biometric information transmitted from the first communication device* “continuously” when Sower’s device 101 is

sufficiently close to the base station/smartphone 112. *See* limitations 1.d and 1.f; EX1005, ¶25 (device 101 “automatically” transmits information to base station 112 when “in close proximity”), ¶34 (“continuous monitoring”), ¶6 (same).

134. In my opinion, it would have been obvious to a POSITA to combine this functionality of Sowers with Aminzade for the reasons in Section VI.M.

G. Claim 12

135. In my opinion, Aminzade combined with Sowers discloses and renders obvious claim 12. It would have been obvious to a POSITA to combine the cited functionality of Sowers with Aminzade for the reasons in Section VI.M.

1. [12.pre] (“A method, comprising:”)

136. Aminzade combined with Sowers discloses and renders obvious the method below.

2. [12.a] (“acquiring dynamic biometric information from a body of a user by a dynamic biometric information acquisition sensor of a first device;”)

137. Aminzade combined with Sowers discloses this limitation. *See* limitations 1.a and 1.a.i.

3. [12.b] (“transmitting the acquired dynamic biometric information through a first communication interface of the first device to a second device;”)

138. Aminzade combined with Sowers discloses this limitation. *See* limitations 1.a.ii and 1.b.iii.

4. **[12.c] (“acquiring static biometric information by a static biometric information acquisition sensor of the second device;”)**

139. Aminzade discloses this limitation. *See* limitations 1.b and 1.b.i.

5. **[12.d] (“performing user authentication to obtain an authentication result based on the acquired static biometric information;”)**

140. Aminzade discloses this limitation. *See* limitation 1.b.ii.

6. **[12.e] (“performing communication with a second communication interface relating to the authentication result with the first communication interface and receiving the dynamic biometric information transmitted from the first communication interface;”)**

141. Aminzade combined with Sowers discloses this limitation. *See* limitation 1.b.iii.

7. **[12.f] (“performing communication relating to the authentication result between the first communication interface and the second communication interface and executing an unlock operation to unlock the first device in response to the communication relating to the authentication result;”)**

142. Aminzade discloses this limitation. *See* limitation 1.c. In addition, Aminzade’s mobile device 20’s transmission of the “instruction” described for limitation 1.c also satisfies the “*performing communication ...*” portion of this limitation for the reasons set forth for limitation 1.c.

8. [12.g] (“acquiring the dynamic biometric information from the dynamic biometric information acquisition sensor of the first device after unlocking, and”)

143. Aminzade combined with Sowers discloses and renders obvious this limitation. *See* limitation 1.d.

9. [12.h] (“maintaining the unlocked state during a condition that the dynamic biometric information can be acquired;”)

144. Aminzade combined with Sowers discloses this limitation. *See* limitation 1.e.

10. [12.i] (“receiving the dynamic biometric information by the second device via communication between the first communication interface and the second communication interface; and”)

145. Aminzade combined with Sowers discloses this limitation. *See* limitation 1.f.

11. [12.j] (“displaying on a display screen information based on a state of the user that is determined using the received dynamic biometric information.”)

146. Aminzade combined with Sowers discloses this limitation. *See* limitations 1.b.iv and 1.f.

- H. Claim 13 (“The method according to claim 12, wherein the first communication interface and the second communication interface are Bluetooth interfaces and the communication performed between the first communication interface and the second communication interface is Bluetooth wireless communication.”)

147. Aminzade discloses this limitation. *See* claim 2.

- I. Claim 15 (“The method according to claim 12, wherein the acquiring of dynamic biometric information acquires one of heart rate, pulse, blood pressure, body temperature, amount of sweating, or brain wave and the static biometric information is one of finger print information, facial recognition information, retina information, vein information, or iris information.”)**

148. Aminzade combined with Sowers discloses and renders obvious this limitation. *See* claim 4.

- J. Claim 16 (“The method according to claim 12, wherein the acquiring of dynamic biometric information by the acquisition sensor of the first device acquires the dynamic biometric information with a wearable device at least by being physically in contact with the body.”)**

149. Aminzade combined with Sowers discloses this limitation. *See* limitation 1.a.i and claim 5.

- K. Claim 17 (“The method according to claim 12, wherein the dynamic biometric information is acquired by a smartwatch as the first device and the dynamic biometric information acquired by a smartphone or tablet as the second device.”)**

150. Aminzade combined with Sowers discloses this limitation. *See* claim 6 (*smartwatch, smartphone, and tablet*), limitation 1.a.i (*first device acquire[s] the dynamic biometric information*), limitation 1.b.iii (*second device acquire[s] the dynamic biometric information from the first device*), limitation 1.f (*same*).

- L. Claim 18 (“The method according to claim 12, wherein the dynamic biometric information is continuously acquired by the first device after being unlocked and the second device receives the dynamic biometric information transmitted from the first device continuously or based on starting of an application on the second device.”)**

151. Aminzade combined with Sowers discloses this limitation. *See* claim 7.

M. Combining Sowers with Aminzade

152. In my opinion, it would have been obvious to a POSITA to combine the functionality from Sowers cited above with Aminzade.

153. For example, a POSITA could have added Sowers’s acquisition of the dynamic biometric information from the user to Aminzade by including Sowers’s sensors 103 and 107 in Aminzade’s wearable device 20. *See* limitation 1.a.i. A POSITA could have readily done so because Sowers’s sensors already are embodied in a device “shown as a wrist band” and Aminzade’s wearable device 20 may be “a smart watch” with wristband 30. *See* limitations 1.a, 1.a.i. A POSITA could have added Sowers’s acquisition of such dynamic biometric information from its sensors to Aminzade for the same reasons, and simply by reading such data from the sensors. *See* limitation 1.d.

154. A POSITA also could have added Sowers’s transmission of dynamic biometric information to Aminzade by implementing Sowers’s wireless communication circuitry (*e.g.*, component 106) in Aminzade’s wearable device 20

and using it to transmit such data. *See* limitations 1.a.ii, 1.b.iii. A POSITA could have readily done so because Aminzade's wearable device 20 already includes wireless communication circuitry (telemetry module 28 and communication unit 64). *Id.*

155. A POSITA further could have added Sowers's "continuous" acquisition of dynamic biometric information from its sensors to Aminzade by, for example, continuously "detect[ing] and stor[ing] data" from the sensors, and transmitting the data to Aminzade's smartphone when "in close enough proximity," as Sowers teaches. *See* limitations 1.d and 1.e. A POSITA could have readily done so because Aminzade's wearable device 20 already is continuously operating to determine the distance between it and mobile device 10 using wireless communication. EX1004, 7:50-53, 9:40-47, 16:48-58, 23:16-34 (reduce access mode when the distance between the two exceeds a threshold), Fig. 7, 24:60-25:19 (increase access mode when the distance between the two is less than the threshold), Fig. 8.

156. A POSITA also could have added Sowers's display of health information, and a display of Sowers's warning or alert described for limitation 1.f, to Aminzade by displaying such information on Aminzade's mobile device 10. A POSITA could have readily done so because mobile device 10 already includes a display for displaying content such as a GUI. *See* limitation 1.b.iv. Aminzade also

discloses that its mobile device 10 includes “applications,” and a POSITA could have implemented this Sowers functionality as an application, as Sowers discloses. EX1004, 10:34-37, 15:19-23; EX1005, ¶20, ¶¶26-28.

157. In each case of incorporating Sowers’s functionality into Aminzade, doing so would have been within the skill and knowledge of a POSITA, would have led to predictable results, would have created a reasonable expectation of success, would have been compatible with Aminzade, and would have been a mere design choice. The predictability, expected success, and compatibility are further confirmed by similarities between Aminzade and Sowers. For example, both involve a smartphone that wirelessly communicates with a wrist-wearable device that includes sensors, where the smartphone uses data from the wearable device’s sensors. *See* limitations 1.a, 1.a.i, 1.a.ii, 1.b, 1.b.iii; EX1004, 16:59-17:9 (wearable device sensors can detect that the device is being worn), 9:40-47 (mobile device in increased access mode when the wearable device is being worn). More specifically, the devices of Sowers and Aminzade each can communicate via wireless protocols like Wi-Fi and Bluetooth. EX1005, ¶19; EX1004 5:27-35, 6:15-23. And both sets of devices communicate with each other when they are “sufficiently close”/“in close proximity.” EX1004, 12:64-13:9; EX1005, ¶25. Moreover, Sowers’s wearable device 101 uses a general-purpose processor (“any type of device capable of processing electronic instructions ...”), which matches

the general-purpose processors 60 of Aminzade's wearable device. EX1005, ¶16; EX1004, 14:62-15:2. Sowers's system also "can be used with any number of different systems and is not specifically limited to the operating environment shown [in Sowers]." EX1005, ¶18. Furthermore, the cited Sowers functionality could be added to the existing Aminzade functionality without modifying or impacting that functionality.

158. Motivation to add the cited Sowers functionality to Aminzade first arises from Sowers's teaching of limiting access to a user's health data, in part for HIPAA compliance. EX1005, ¶21, ¶29 (password requirement). In my opinion, this teaching would have led a POSITA to seek increased security for the user's health data, which is provided by the Aminzade system entering reduced access mode for both devices if the user is no longer wearing the wearable device or the wearable device is too far away from the mobile device. EX1004, 9:40-47.

159. More motivation arises from Sowers's disclosure of the desirability to continuously monitor a user's health and provide notice of potential health problems. EX1005, ¶5. This would have motivated a POSITA to add the cited Sowers functionality to Aminzade, which does not disclose such functionality. *See* limitation 1.f (Sower's warnings and display of health information).

160. Additional motivation arises from Aminzade's disclosure of "increased" access on its mobile device 10 after user authentication, described for

limitation 1.b.ii, which would have led a POSITA to provide access to Sowers's health information by displaying it on Aminzade's mobile device 10 after user authentication.

161. Further motivation arises from Sower's disclosure that its system provides a user with "low-cost, comprehensive, continuous monitoring of his health information," which would have led a POSITA to implement it on the similar Aminzade system that does not disclose such benefit. EX1005, ¶7. Similar motivation arises from Sowers's disclosure of warning of "risk of heart attack," "risk of stroke," and "blood alcohol content," which a POSITA would have understood are desirable to know. EX1005, ¶27; *see* limitation 1.f (citing same).

162. Similar motivation arises from Soli, described in Ground 2, and its teaching of the desirability for users to "monitor and track their wellness data," as described at the end of Ground 2. EX1006, ¶3. This also would have led a POSITA to implement Sower's health monitoring in Aminzade, including the functionality cited above.

163. More motivation arises from Aminzade, which does not elaborate on any specific application (*e.g.*, messaging, health monitoring) on its wearable device. In my opinion, this would have led a POSITA to implement such an application, where Sowers's health monitoring was a known and natural choice. Likewise, Aminzade does not elaborate on controlling access to specific data (*e.g.*,

health data) from its wearable device, which again would have led a POSITA to implement and control access to Sowers's health monitoring on Aminzade's wearable device as a known and natural choice.

164. Incorporating the cited Sowers functionality in Aminzade therefore would have applied a known technique (Sowers's functionality) to known devices (Aminzade's devices) that were ready for improvement (the cited health monitoring) to yield predictable results. Doing so also would have used a known technique (the cited Sowers's functionality) to improve the similar devices of Aminzade (its smartphone and wearable device) in the same way (to provide health monitoring).

* * *

165. If Patent Owner argues that the portions of Aminzade or Sowers cited above relate to different, incompatible embodiments (which they do not), it would have been obvious to a POSITA to combine such embodiments into a single system at least because such embodiments are described in the same prior art reference, are fully compatible with each other, and could be combined with minimal effort to achieve predictable results.

166. If Patent Owner argues that Aminzade or Sowers does not disclose any limitation of the challenged claims, such limitation would have nonetheless been obvious to a POSITA in light of Aminzade and Sowers. Practicing any

limitation of the challenged claims in light of Aminzade and Sowers would have been within the knowledge and skill of a POSITA, would have required minimal effort, would have yielded predictable results, would have been fully compatible with Aminzade, and would have been a mere design choice. Motivation to do so arises from at least common sense and the disclosures of Aminzade and Sowers set forth above.

VII. GROUND 2: CLAIMS 1-2, 4-7, 12-13, 15-18 ARE OBVIOUS IN LIGHT OF AMINZADE AND SOLI

167. In my opinion, claims 1-2, 4-7, 12-13, 15-18 are obvious in light of Aminzade and Soli.

A. Claim 1

Aminzade combined with Soli discloses and renders obvious claim 1.

1. [1.pre] (“A system, comprising:”)

168. Aminzade discloses this preamble. *See* Ground 1, claim 1, preamble.

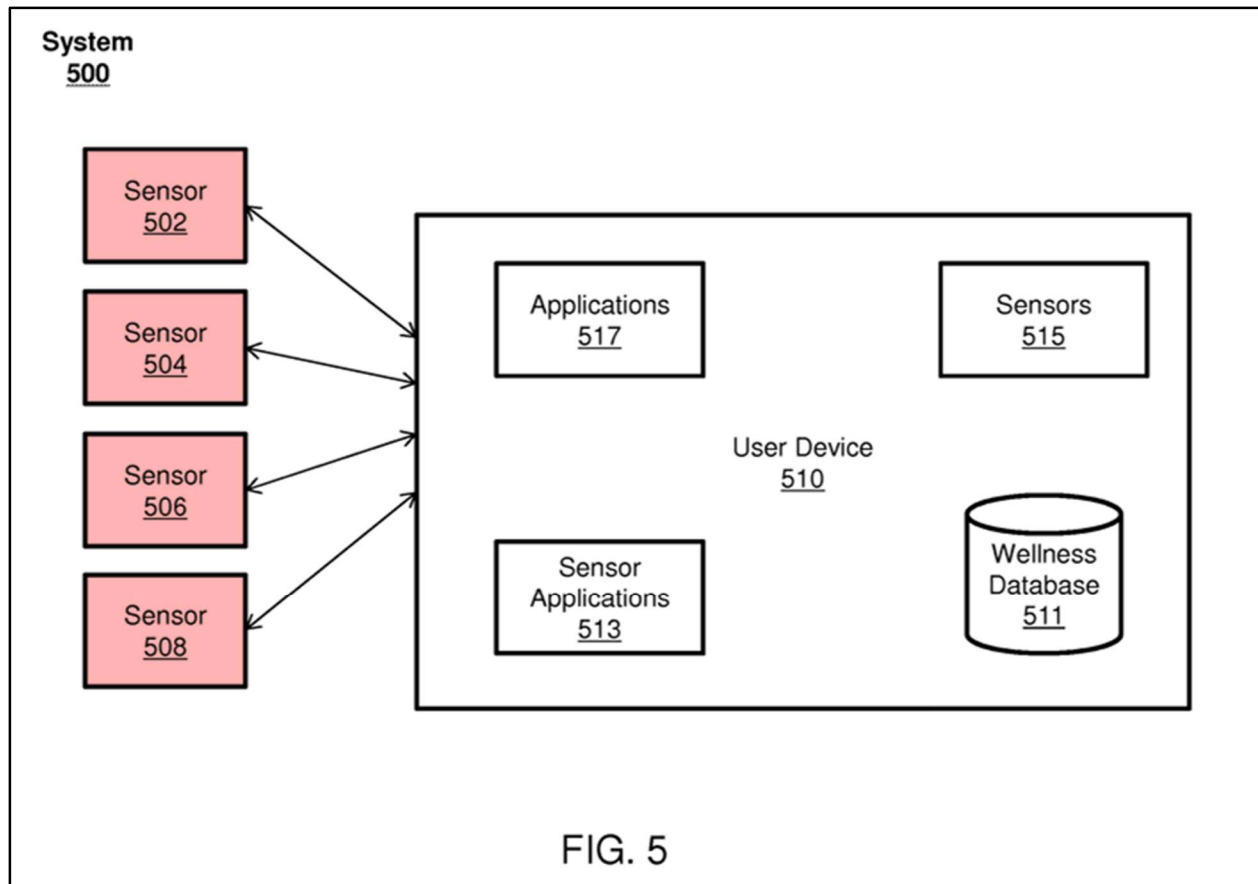
2. [1.a] (“a first information processing device including:”)

169. Aminzade discloses this limitation. *See* Ground 1, limitation 1.a.

3. [1.a.i] (“a dynamic biometric information acquisition sensor that acquires dynamic biometric information from a body of a user; and”)

170. Aminzade combined with Soli discloses this limitation.

171. Soli discloses “sensors 502, 504, 506, and 508,” annotated below, that can be “biometric sensor[s].” EX1006, ¶226, Fig. 5; EX1007, ¶141, Fig. 5.



Certain instances of the sensors “can be included within a wearable electronic device, such as a smart watch.” EX1006, ¶226; EX1007, ¶141. Those sensors include a “photoplethysmogram,² galvanic skin response sensor,³ [and a] temperature sensor” (each *a dynamic biometric information acquisition sensor that*

² A POSITA would have understood that a photoplethysmogram (“PPG”) detects heart rate and blood pressure. EX1011 (Yuen), ¶45.

³ A POSITA would have understood that a galvanic skin response sensor measures sweat levels. EX1012 (Tran), ¶225.

acquires dynamic biometric information from a body of a user). EX1006, ¶226; EX1007, ¶141. *Acquired dynamic biometric information* from such sensors includes “Heart Rate,” “Blood Pressure,” “Body Temperature,” and “Galvanic Skin Response.” EX1006, ¶325, ¶258 (“heart rate measurement”), Figs. 9, 12, 27; EX1007, ¶240, ¶173, Figs. 9, 12, 27.

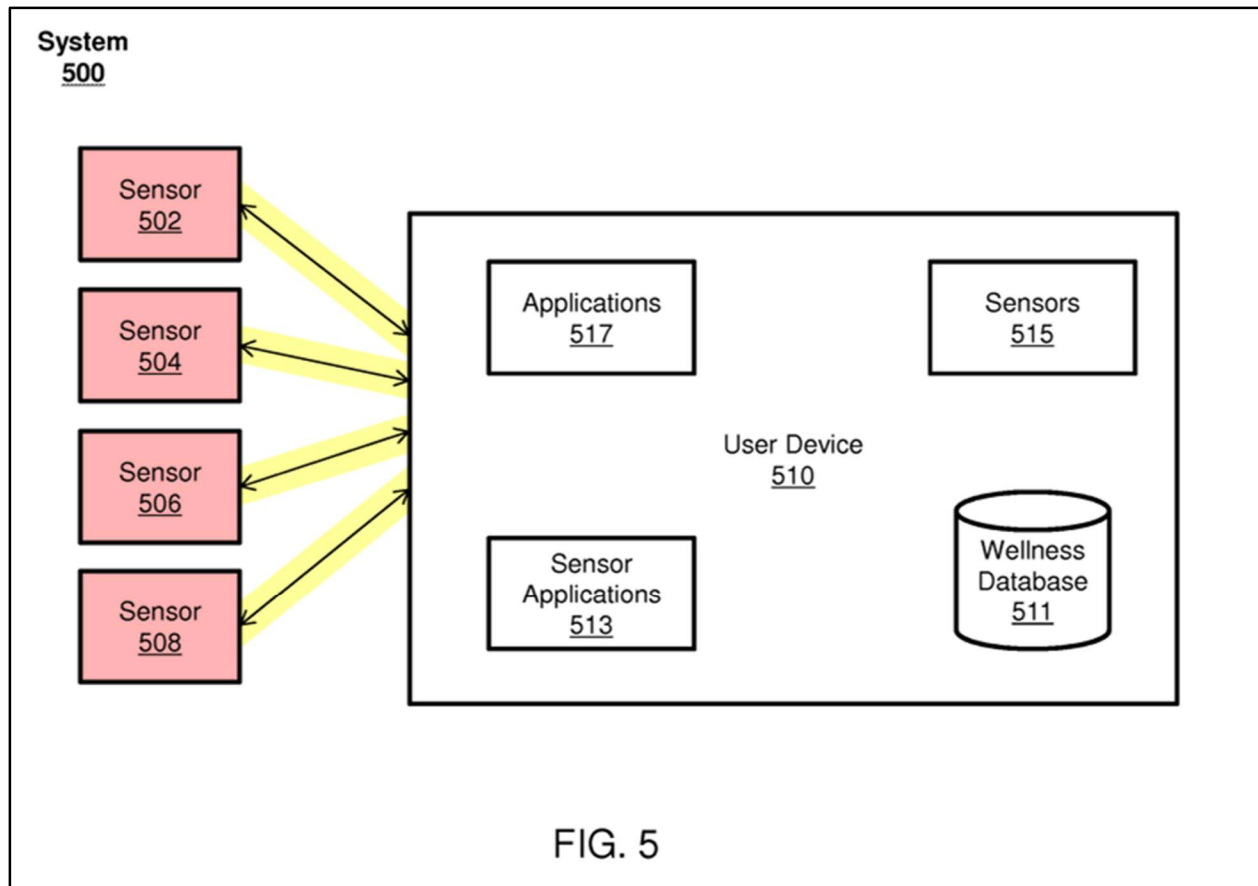
172. In my opinion, it would have been obvious to a POSITA to combine this functionality of Soli with Aminzade for the reasons in Section VII.M.

4. [1.a.ii] (“a first communication interface that transmits the acquired dynamic biometric information; and”)

173. Aminzade combined with Soli discloses this limitation.

174. Aminzade’s wearable device 20 (*a first information processing device*) includes *a first communication interface*. See Ground 1, limitation 1.a.ii.

175. Soli’s sensors 502-508 in a smartwatch *acquire[] dynamic biometric information*. See Ground 2, limitation 1.a.i. Soli’s “user device 510,” which may be “a smart phone,” “receive[s] wellness ... data from sensors 502, 504, 506, and 508.” EX1006, ¶226, ¶228 (“allow user device 510 to receive the wellness ... data;” “device 510 can be a smart phone”), ¶229 (“receive[s] ... wellness ... data from the sensors”), Fig. 5; EX1007, ¶141, ¶¶143-144, Fig. 5. Figure 5 illustrates such transmission with arrows from the sensors to user device 510, as highlighted below. EX1006, Fig. 5; EX1007, Fig. 5.



Soli's Figures 9-14 show user interfaces of user device 510 that include data from the sensors, confirming that the data was transmit to that device. EX1006, ¶¶251-252; EX1007, ¶¶166-167.

176. In my opinion, a POSITA would have understood that Soli implicitly and necessarily (inherently) discloses that the smartwatch containing sensors 502-508 also includes a *first communication interface*, which *transmits* the sensors' *acquired dynamic biometric information* to user device 510. Otherwise, user device 510 would not be able to receive the wellness data from the sensors as Soli discloses.

177. In my opinion, it would have been obvious to a POSITA to combine this functionality of Soli with Aminzade for the reasons in Section VII.M.

5. [1.b] (“a second information processing device including:”)

178. Aminzade discloses this limitation. *See* Ground 1, limitation 1.b.

6. [1.b.i] (“a static biometric information acquisition sensor that acquires static biometric information;”)

179. Aminzade discloses this limitation. *See* Ground 1, limitation 1.b.i.

7. [1.b.ii] (“a processor that performs user authentication based on the acquired static biometric information and obtains an authentication result;”)

180. Aminzade discloses this limitation. *See* Ground 1, limitation 1.b.ii.

8. [1.b.iii] (“a second communication interface that performs communication relating to the authentication result with the first communication interface and receives the dynamic biometric information transmitted from the first communication interface; and”)

181. Aminzade combined with Soli discloses and renders obvious this limitation.

182. Aminzade’s mobile device 10 includes *a second communication interface that performs communication relating to the authentication result with the first communication interface* of its wearable device 20. *See* Ground 1, limitation 1.b.iii.

183. Receiving the Dynamic Biometric Information. Aminzade’s wearable device 20 includes *a first communication interface*. *See* Ground 1, limitation 1.a.ii.

184. As described for Ground 2, limitation 1.a.ii, Soli's user device 510 (e.g., a smartphone) can be "identical" to the device of Figure 1A, showing a "portable multifunction device 100." EX1006, ¶225, ¶82; EX1007, ¶140, ¶45. Device 100 (and therefore user device 510) includes "RF (radio frequency) circuitry 108" (also *a second communication interface*) for "wireless communication" with "other communications devices." EX1006, ¶88, ¶107 ("data received by RF circuitry 108"), Fig. 1A; EX1007, ¶52, ¶68, Fig. 1A.

185. Soli's user device 510 *receives the dynamic biometric information transmitted from a first communication interface*. See Ground 2, limitation 1.a.ii. Soli's user device 510 can be the device of Figure 1A, as established above. In that case, in my opinion, a POSITA would have understood that RF circuitry 108 (a *second communication interface*) would *receive[] the dynamic biometric information transmitted from the smartwatch containing wellness sensors 502-508 and its first communication interface*, because Soli discloses that circuitry as the circuitry that receives wireless data, as described above. See also Ground 2, limitation 1.a.ii (Soli's *first communication interface*).

186. It also would have been obvious to a POSITA to use RF circuitry 108 in user device 510 to receive wellness data from the smartwatch containing sensors 502-508. A POSITA could have done so using, for example, the disclosed "Bluetooth" protocol or other disclosed wireless protocols. EX1006, ¶88; EX1007,

¶52. Motivation to do so arises from 1) Soli's disclosure that the RF circuitry can be used to wirelessly communicate with other devices, described above; 2) Sowers's disclosure of transmitting dynamic biometric sensor data wirelessly, described in Ground 1, limitation 1.a.ii; 3) Aminzade's disclosure of wireless communication between a smartphone and wearable device, described in Ground 1, limitation 1.b.iii; and 4) avoiding having such communication be wired, for purposes of usability, which a POSITA would have known.

187. In my opinion, it would have been obvious to a POSITA to combine this functionality of Soli with Aminzade for the reasons in Section VII.M.

9. [1.b.iv] ("a display screen,")

188. Aminzade discloses this limitation. *See* Ground 1, limitation 1.b.iv.

10. [1.c] ("wherein the first information processing device: performs communication relating to the authentication result between the first communication interface and the second communication interface and executes an unlock operation to unlock itself in response to the communication relating to the authentication result,")

189. Aminzade discloses this limitation. *See* Ground 1, limitation 1.c.

11. [1.d] ("acquires the dynamic biometric information from the dynamic biometric information acquisition sensor after unlocking, and")

190. Aminzade combined with Soli discloses and renders obvious this limitation.

191. Acquiring Information from the Sensors. Soli discloses that

smartwatch sensors 502-508 can be *dynamic biometric information acquisition sensor[s]*. See Ground 2, limitation 1.a.i. Soli also discloses transmitting the “wellness data” obtained from the sensors (*the dynamic biometric information*) to user device 510. See Ground 2, limitation 1.a.ii. In my opinion, a POSITA would have understood that doing so implicitly and necessarily (inherently) requires first *acquir[ing]* the wellness data from the sensors in order to transmit it. It also would have been obvious to a POSITA to do so by, for example, having Soli’s RF circuitry *acquire[]* the wellness data for purposes of wirelessly transmitting it to user device 510. See Ground 2, limitation 1.b.iii (Soli’s RF circuitry). Motivation to do so arises at least from Soli’s disclosure that user device 510 receives the wellness data from the sensors, which would motivate a POSITA to have the sensors’ device (the smartwatch) *acquire[]* the data to transmit it. See Ground 2, limitation 1.a.ii.

192. After Unlocking. Aminzade discloses *unlocking* its wearable device 20. See Ground 1, limitation 1.c.

193. Soli discloses that sensors 502-508 “can be used to measure wellness ... data continuously, intermittently, periodically, or at any other desired frequency or interval of time.” EX1006, ¶227, ¶236; EX1007, ¶142, ¶151. Similarly, system 500 (of Figure 5) “can be configured to measure, generate, receive, [and] store wellness ... data continuously, intermittently, periodically, or at any other desired

frequency or interval of time.” EX1006, ¶283; EX1007, ¶198. Such receipt and storage of wellness data in system 500 includes user device 510 “receiv[ing]” the wellness data, as described for limitation 1.a.ii in Ground 2. It also includes user device 510 “stor[ing]” the wellness data in its “wellness database 511.” EX1006, ¶¶228-229, Fig. 5; EX1007, ¶¶143-144, Fig. 5. The receipt and storage of such wellness data (*dynamic biometric information*) on user device 510 first requires the smartwatch containing sensors 502-508 to *acquire* the wellness data to transmit it to user device 510, as described above. Because Soli discloses such receipt and storage “continuously, intermittently, and periodically,” as described above, it also discloses *acquir[ing]* the wellness data continuously, intermittently, and periodically.

194. It would have been obvious to a POSITA to combine each of these functionalities of Soli with Aminzade for the reasons in Section VII.M.

195. Upon doing so, the smartwatch containing sensors 502-508 still would *acquire* the wellness data (*dynamic biometric information*) from the sensors “continuously, intermittently, and periodically.” EX1006, ¶283; EX1007, ¶198. Each of those frequencies would include doing so *after unlocking* because the word “after” refers to chronology, not causality. It also would have been obvious to a POSITA to keep doing so *after unlocking* for the reasons in Section VII.M.

12. [1.e] (“maintains the unlocked state during a condition that the dynamic biometric information can be acquired,”)

196. Aminzade combined with Soli discloses this limitation.

197. Soli discloses *acquiring dynamic biometric information* from sensors 502-508 “continuously, intermittently, and periodically,” and the smartwatch containing those sensors transmitting that information to user device 510. *See* Ground 2, limitations 1.a.ii and 1.b.iii. Soli discloses and renders obvious such transmission being wireless, such as via Bluetooth. *See* Ground 2, limitation 1.b.iii. The smartwatch containing sensors 502-508 being worn and being sufficiently close to user device 510 to support wireless transmission (*e.g.*, via Bluetooth) therefore is *a condition that the dynamic biometric information can be acquired*.

198. Aminzade discloses unlocking wearable device 20 after authenticating the user’s fingerprint and then *maintain[ing] the unlocked state during the condition that* the wearable device is worn by the user and close enough to the mobile device 10 for wireless communication between the two (*during the condition* described above). *See* Ground 1, limitation 1.e.

199. In my opinion, it would have been obvious to a POSITA to combine this functionality of Soli with Aminzade for the reasons in Section VII.M.

13. [1.f] (“wherein the second information processing device receives the dynamic biometric information via communication between the first communication interface and the second communication interface and the display screen displays information based on a state of the user that is determined using the received dynamic biometric information.”)

200. Aminzade combined with Soli discloses this limitation.

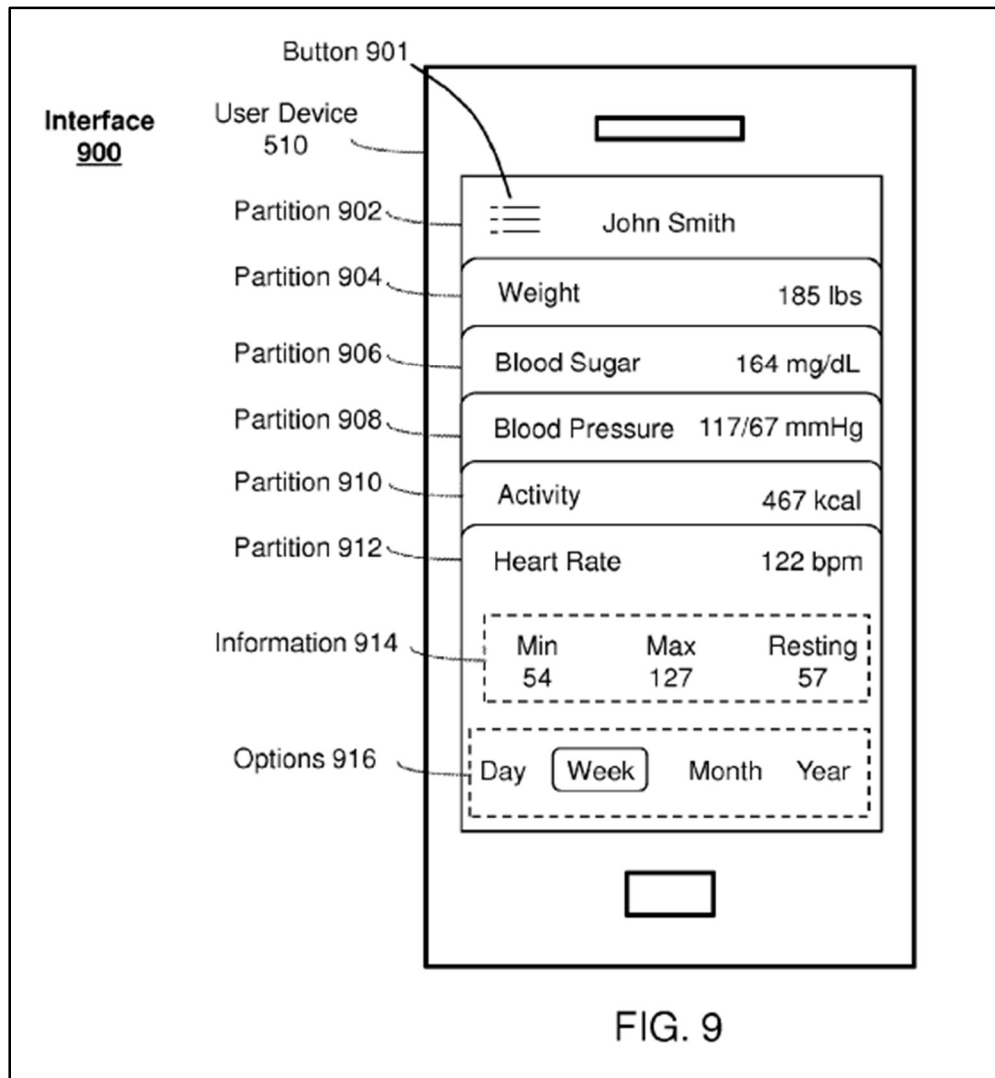
201. Aminzade combined with Soli discloses *a second communication interface of the second information processing device that receives the dynamic biometric information from the first communication interface, i.e., via communication between the first communication interface and the second communication interface. See Ground 2, limitation 1.b.iii.*

202. Displaying Information Based on a State of the User. Soli discloses that its user device 510 receives wellness data (*received dynamic biometric information*) from sensors 502-508 in a “smart watch,” such as a “photoplethysmogram, galvanic skin response sensor, [and] temperature sensor.” *See Ground 2, limitations 1.a.i, 1.a.ii, and 1.b.iii.* User device 510 can receive additional data from “separate devices” (*i.e., separate from the smartwatch*), such as a “scale, blood glucose monitor, [and] SpO2 sensor,”⁴ each of which can be

⁴ A POSITA would have understood that an SpO2 sensor measures blood oxygen saturation. EX1011 (Yuen), ¶57 (“oxygen saturation (SpO2)”).

“separate devices.” EX1006, ¶226; EX1007, ¶141. Additional data also can be received from applications on device 510, such as a “healthcare provider” app. EX1006, ¶230; EX1007, ¶145.

203. Soli’s user device 510 can “aggregate” the wellness data from the smartwatch (*received dynamic biometric information*) with such additional data to create a superset of data about the user’s state (*determine a state of the user using the received dynamic biometric information*). EX1006, ¶¶251-252, ¶226, Figs. 34-35 (“Source List” with multiple devices), ¶339, ¶341; EX1007, ¶¶166-167, ¶141, Figs. 34-45, ¶254, ¶256. For example, Soli’s Figure 9, shown below, shows “interface 900” of user device 510 that is expandable into the interfaces of Figures 10-14. EX1006, ¶¶252-258, ¶¶263-267; EX1007, ¶¶167-173, ¶¶178-182. The interfaces of Figures 9-14 collectively are *information based on [the] state of the user that the display screen displays*.



The displayed *user state* in these figures includes data from the smartwatch sensors (*received dynamic biometric information*), such as “heart rate” data and “blood pressure” data, which a POSITA would have understood comes from the photoplethysmogram (“PPG”). EX1006, Figs. 12, 14, ¶265, ¶267; EX1007, Figs. 12, 14, ¶180, ¶182. In my opinion, it also would have been obvious to a POSITA to obtain such data from the PPG because the PPG is used to measure such data. See Ground 2, limitation 1.a.i. The displayed *user state* also includes data from

“separate devices,” such as “weight,” which would come from the “scale,” and “blood sugar,” which would come from the “blood glucose monitor,” for example. EX1006, Figs. 10-11, ¶¶263-264; EX1007, Figs. 10-11, ¶¶178-179.

204. Similarly, Soli’s user device 510 *display[s]* “interface 2700” that includes wellness data from the smartwatch sensors (*received dynamic biometric information*), such as “Heart Rate,” “Blood Pressure,” and “Body Temperature.” EX1006, ¶325, Fig. 27; EX1007, ¶240, Fig. 27. That interface also includes data from the “separate devices” described above, such as “Oxygen Saturation” and “Blood Glucose” (sugar), along with additional aggregated data about the user’s state, such as “Respiratory Rate,” “Blood Alcohol Content,” “Body Fat Percentage,” and so on. EX1006, ¶325, Fig. 27; EX1007, ¶240, Fig. 27. Interface 2700 therefore also is *display[ed] information based on [the] state of the user that is determined using the received dynamic biometric information*.

205. Aminzade’s mobile device 10 (*second information processing device*) also includes a *display screen*. See Ground 1, limitation 1.b.iv.

206. In my opinion, it would have been obvious to a POSITA to combine this functionality of Soli with Aminzade for the reasons in Section VII.M.

- B. Claim 2 (“The system according to claim 1, wherein the first communication interface and the second communication interface are Bluetooth interfaces and communication between the first communication interface and the second communication interface is Bluetooth wireless communication.”)**

207. Aminzade discloses this limitation. *See* Ground 1, claim 2.

- C. Claim 4 (“The system according to claim 1, wherein the dynamic biometric information is one of heart rate, pulse, blood pressure, body temperature, amount of sweating, or brain wave and the static biometric information is one of finger print information, facial recognition information, retina information, vein information, or iris information.”).**

208. Aminzade combined with Soli discloses this limitation.

209. Aminzade discloses that *the static biometric information* can be a “fingerprint” (*finger print information*) or “image,” which a POSITA would have understood to refer to *facial recognition information*. *See* Ground 1, limitation 1.b.i.

210. Soli discloses that *the dynamic biometric information* can be “temperature” (*body temperature*). *See* Ground 2, limitation 1.a.i. The analysis of claim 1 above explains how Soli discloses the “dynamic biometric information” limitations of claim 1 when *the dynamic biometric information* is the user’s *body temperature*. *See* Ground 2, claim 1. The analysis explains how the *body temperature* information is acquired, transmitted, received, and used (potentially along with additional information) to determine a state of the user, as recited by claim 1. *Id.* Regarding limitation 1.f, Soli discloses *determin[ing] a state of the*

user by aggregating “Body Temperature” (*using the received dynamic biometric information*) with other wellness data and displaying such information in interface 2700. *See* Ground 2, limitation 1.f; EX1006, ¶325, Fig. 27; EX1007, ¶240, Fig. 27. Because the preamble of claim 1 uses the transition phrase “comprising,” claim 4 does not prohibit acquiring, transmitting, receiving, or using additional data along with the *body temperature* information.

211. Soli also discloses that *the dynamic biometric information* can be from a “galvanic skin response sensor,” which data would be an *amount of sweating*. *See* Ground 2, limitation 1.a.i. The analysis in the paragraph above regarding body temperature also applies equally to *amount of sweating*. *See also* EX1006, ¶325 (interface 2700 can include “Galvanic Skin Response”), Fig. 27; EX1007, ¶240, Fig. 27.

212. Soli also discloses that *the dynamic biometric information* can be “heart rate” (*heart rate*). *See* Ground 2, limitation 1.a.i; *see also* EX1006, ¶258 (“heart rate measurement [of] 122 bpm”), Fig. 9; EX1007, ¶173, Fig. 9. The analysis above regarding body temperature also applies equally to *heart rate*. *See also* EX1006, ¶325 (interface 2700 can include “Heart Rate”), Fig. 27; EX1007, ¶240, Fig. 27.

213. In my opinion, it would have been obvious to a POSITA to combine this functionality of Soli with Aminzade for the reasons in Section VII.M.

D. Claim 5 (“The system according to claim 1, wherein the first information processing device is a wearable device that acquires the dynamic biometric information at least by being physically in contact with the body.”)

214. Aminzade combined with Soli discloses this limitation. Aminzade’s wearable device 20 (*a first information processing device*) is a “wearable ... device.” *See* Ground 1, limitation 1.a.

215. Soli discloses *dynamic biometric information acquire[d]* from sensors 502-508 in a “wearable electronic device, such as a smart watch” (also *a wearable device*). *See* Ground 2, limitation 1.a.i. A POSITA would have understood that such sensors (the “photoplethysmogram, galvanic skin response sensor, [and] temperature sensor”) operate by *being physically in contact with the body* based on the data they measure, such as blood pressure, sweat levels, and temperature. *See* Ground 2, limitation 1.a.i.

216. In my opinion, it would have been obvious to a POSITA to combine this functionality of Soli with Aminzade for the reasons in Section VII.M.

E. Claim 6 (“The system according to claim 1, wherein the first information processing device is a smartwatch and the second information processing device is a smartphone or tablet.”)

217. Aminzade discloses this limitation. *See* Ground 1, claim 6.

- F. Claim 7 (“The system according to claim 1, wherein the first information processing device continuously acquires the dynamic biometric information after being unlocked and the second information processing device receives the dynamic biometric information transmitted from the first communication device continuously or based on starting of an application on the second information processing device.”)**

218. Aminzade combined with Soli discloses this limitation.

219. Aminzade combined with Soli discloses the *first information processing device* “continuous[ly]” *acquir[ing] the dynamic biometric information after being unlocked*. See Ground 2, limitation 1.d.

220. Aminzade combined with Soli also discloses that *the second information processing device receiv[ing] the dynamic biometric information transmitted from the first communication device* “continuously.” See Ground 2, limitations 1.d, 1.f. For example, Soli’s system 500” (of Figure 5) “can ... receive [and] store ... wellness ... data continuously,” which a POSITA would understand implicitly and necessarily (inherently) discloses that user device 510 *receives* the wellness data (the *dynamic biometric information*) “continuously” because it is the only device in system 500 that receives data from sensors 502-508, and it stores such data in wellness database 511. EX1006, Fig. 5, ¶¶225-226; EX1007, Fig. 5, ¶¶140-141.

221. In my opinion, it would have been obvious to a POSITA to combine this functionality of Soli with Aminzade for the reasons in Section VII.M.

G. Claim 12

222. Aminzade combined with Soli discloses and renders obvious claim 12. In my opinion, it would have been obvious to a POSITA to combine the cited functionality of Soli with Aminzade for the reasons in Section VII.M.

2. [12.pre] (“A method, comprising:”)

223. Aminzade combined with Soli discloses and renders obvious the method below, as established below.

3. [12.a] (“acquiring dynamic biometric information from a body of a user by a dynamic biometric information acquisition sensor of a first device;”)

224. Aminzade combined with Soli discloses this limitation. *See* Ground 2, limitations 1.a, 1.a.i.

4. [12.b] (“transmitting the acquired dynamic biometric information through a first communication interface of the first device to a second device;”)

225. Aminzade combined with Soli discloses this limitation. *See* Ground 2, limitations 1.a.ii and 1.b.iii.

5. [12.c] (“acquiring static biometric information by a static biometric information acquisition sensor of the second device;”)

226. Aminzade discloses this limitation. *See* Ground 1, limitations 1.b and 1.b.i.

6. **[12.d] (“performing user authentication to obtain an authentication result based on the acquired static biometric information;”)**

227. Aminzade discloses this limitation. *See* Ground 1, limitation 1.b.ii.

7. **[12.e] (“performing communication with a second communication interface relating to the authentication result with the first communication interface and receiving the dynamic biometric information transmitted from the first communication interface;”)**

228. Aminzade combined with Soli discloses and renders obvious this limitation. *See* Ground 2, limitation 1.b.iii.

8. **[12.f] (“performing communication relating to the authentication result between the first communication interface and the second communication interface and executing an unlock operation to unlock the first device in response to the communication relating to the authentication result;”)**

229. Aminzade discloses this limitation. *See* Ground 1, limitation 12.f.

9. **[12.g] (“acquiring the dynamic biometric information from the dynamic biometric information acquisition sensor of the first device after unlocking, and”)**

230. Aminzade combined with Soli discloses and renders obvious this limitation. *See* Ground 2, limitation 1.d.

10. **[12.h] (“maintaining the unlocked state during a condition that the dynamic biometric information can be acquired;”)**

231. Aminzade combined with Soli discloses this limitation. *See* Ground 2, limitation 1.e.

11. **[12.i] (“receiving the dynamic biometric information by the second device via communication between the first communication interface and the second communication interface; and”)**

232. Aminzade combined with Soli discloses this limitation. *See* Ground 2, limitation 1.f.

12. **[12.j] (“displaying on a display screen information based on a state of the user that is determined using the received dynamic biometric information.”)**

233. Aminzade combined with Soli discloses this limitation. *See* Ground 2, limitations 1.b.iv and 1.f.

- H. **Claim 13 (“The method according to claim 12, wherein the first communication interface and the second communication interface are Bluetooth interfaces and the communication performed between the first communication interface and the second communication interface is Bluetooth wireless communication.”)**

234. Aminzade discloses this limitation. *See* Ground 1, claim 2.

- I. **Claim 15 (“The method according to claim 12, wherein the acquiring of dynamic biometric information acquires one of heart rate, pulse, blood pressure, body temperature, amount of sweating, or brain wave and the static biometric information is one of finger print information, facial recognition information, retina information, vein information, or iris information.”)**

235. Aminzade combined with Soli discloses this limitation. *See* Ground 2, claim 4.

- J. Claim 16 (“The method according to claim 12, wherein the acquiring of dynamic biometric information by the acquisition sensor of the first device acquires the dynamic biometric information with a wearable device at least by being physically in contact with the body.”)**

236. Aminzade combined with Soli discloses this limitation. *See* Ground 2, limitation 1.a.i and claim 5.

- K. Claim 17 (“The method according to claim 12, wherein the dynamic biometric information is acquired by a smartwatch as the first device and the dynamic biometric information acquired by a smartphone or tablet as the second device.”)**

237. Aminzade combined with Soli discloses this limitation. *See* Ground 1, claim 6 (*smartwatch, smartphone, and tablet*), Ground 2, limitation 1.a.i (*first device acquire[s] the dynamic biometric information*), Ground 2, limitation 1.b.iii (*second device acquire[s] the dynamic biometric information from the first device*), Ground 2, limitation 1.f (same).

- L. Claim 18 (“The method according to claim 12, wherein the dynamic biometric information is continuously acquired by the first device after being unlocked and the second device receives the dynamic biometric information transmitted from the first device continuously or based on starting of an application on the second device.”)**

238. Aminzade combined with Soli discloses this limitation. *See* Ground 2, claim 7.

- M. Combining Soli with Aminzade**

239. In my opinion, it would have been obvious to a POSITA to combine the functionality from Soli cited above with Aminzade.

240. A POSITA could have added Soli's acquisition of the dynamic biometric information to Aminzade by including Soli's smartwatch sensors (the PPG, galvanic skin response sensor, and temperature sensor) in Aminzade's wearable device 20. *See* Ground 2, limitation 1.a.i. A POSITA could have readily done so because these Soli sensors already are in a "smart watch" and Aminzade's wearable device 20 may be "a smart watch." *See* Ground 2, limitations 1.a, 1.a.i. A POSITA could have added Soli's acquisition of such dynamic biometric information from the sensors to Aminzade for the same reasons, and simply by reading such data from the sensors. *See* Ground 2, limitation 1.d.

241. A POSITA also could have added Soli's transmission of dynamic biometric information to Aminzade by implementing the communication interface of Soli's smartwatch in Aminzade's wearable device 20 and using it to transmit such data. *See* Ground 2, limitations 1.a.ii and 1.b.iii. A POSITA, in my opinion, could have readily done so because Aminzade's wearable device 20 already includes wireless communication circuitry (telemetry module 28 and communication unit 64). *Id.*

242. A POSITA further could have added Soli's "continuous[], intermittent[], [or] periodic[]" acquisition of dynamic biometric information from its sensors to Aminzade by, for example, "receiv[ing], [and] stor[ing] wellness ... data" from the sensors with such frequency, and transmitting the data to

Aminzade's smartphone wirelessly, as Soli teaches. *See* Ground 2, limitations 1.d and 1.e; EX1006, ¶88; EX1007, ¶52. A POSITA could have readily done so because Aminzade's wearable device 20 already is continuously operating to determine the distance between it and mobile device 10 using wireless communication. *See* § VI.M (combining Sowers with Aminzade).

243. A POSITA also could have included Soli's display of aggregated health information described for limitation 1.f in Ground 2 by displaying such information on Aminzade's mobile device 10. A POSITA could have readily done so because mobile device 10 already includes a display for displaying content such as a GUI. *See* Ground 1, limitation 1.b.iv. Aminzade also discloses that its mobile device 10 includes "applications," and a POSITA could have implemented this Soli functionality as one or more applications, as Soli discloses. EX1004, 10:34-37, 15:19-23; EX1006, ¶¶228-229 (user device 510 can include "applications 513" to "receive" and "store wellness ... data"), Fig. 5, ¶230 (additional sources of wellness data can be apps on the mobile device, such as a "healthcare provider" app), ¶442; EX1007, ¶¶143-144, Fig. 5, ¶145, ¶357.

244. In each case of incorporating Soli's functionality into Aminzade, doing so would have been within the skill and knowledge of a POSITA, would have led to predictable results, would have created a reasonable expectation of success, would have been compatible with Aminzade, and would have been a mere

design choice. The predictability, expected success, and compatibility are further confirmed by similarities between Aminzade and Soli. For example, both involve a smartphone that wirelessly communicates with a wrist-wearable device that includes sensors, where the smartphone uses data from the wearable device's sensors. *See* Ground 2, limitations 1.a, 1.a.i, 1.a.ii, 1.b, and 1.b.iii; EX1004, 16:59-17:9, 9:40-47. More specifically, the devices of Soli and Aminzade each can communicate via wireless protocols like Wi-Fi and Bluetooth. EX1006, ¶88; EX1007, ¶52; EX1004, 5:27-35, 6:15-23. Soli's sensors 502-508 can be in "a smart watch," and Aminzade's wearable device 20 can be a "smart watch." EX1006, ¶226; EX1007, ¶141; EX1004, 4:46-48. Furthermore, the cited Soli functionality could be added to the existing Aminzade functionality without modifying or impacting that functionality.

245. Motivation to add the cited Soli functionality to Aminzade first arises from Soli's disclosure of the desirability for users to "monitor and track their wellness data," given that "[over 100 million] Americans currently suffer from at least one chronic condition." EX1006, ¶3; EX1007, ¶3. This would have led a POSITA to implement Soli health monitoring in Aminzade, including the Soli functionality cited above.

246. Similar motivation arises from Sowers and its disclosure of the desirability to provide for health monitoring, described at the end of Ground 1. *See*

§ VI.M.

247. Further motivation arises from Soli's disclosure of "transmitting ... wellness data ... to the user authorized to access the set of wellness data."

EX1006, ¶7; EX1007, ¶7. This would have motivated a POSITA to transmit the dynamic biometric data from Soli's wearable device to Aminzade's mobile device 10, which authorizes the user to use the mobile device via fingerprint authentication, for example. *See* Ground 1, limitation 1.b.ii.

248. Additional motivation arises from Aminzade's disclosure of "increased" access on its mobile device 10 after user authentication, described in Ground 1 for limitation 1.b.ii, which would have led a POSITA to provide access to Soli's health information by displaying it on Aminzade's mobile device 10 after user authentication.

249. More motivation arises from Aminzade, which does not elaborate on any specific application (e.g., messaging, health monitoring) on its wearable device. This would have led a POSITA to implement such an application, where Soli's health monitoring was a known and natural choice. Likewise, Aminzade does not elaborate on controlling access to specific data (e.g., health data) from its wearable device, which again would have led a POSITA to implement and control access to Soli's health monitoring on Aminzade's wearable device as a known and natural choice.

250. Incorporating the cited Soli functionality in Aminzade therefore would have applied a known technique (Soli's cited functionality) to known devices (Aminzade's devices) that were ready for improvement (the cited health monitoring) to yield predictable results. Doing so also would have used a known technique (the cited Soli functionality) to improve the similar devices of Aminzade (its smartphone and wearable device) in the same way (to provide health monitoring).

* * *

251. If Patent Owner argues that the portions of Aminzade or Soli cited above relate to different, incompatible embodiments (which they do not), it would have been obvious to a POSITA to combine such embodiments into a single system at least because such embodiments are described in the same prior art reference, are fully compatible with each other, and could be combined with minimal effort to achieve predictable results.

252. If Patent Owner argues that Aminzade or Soli does not disclose any limitation of the challenged claims, such limitation would have nonetheless been obvious to a POSITA in light of Aminzade and Soli. Practicing any limitation of the challenged claims in light of Aminzade and Soli would have been within the knowledge and skill of a POSITA, would have required minimal effort, would have yielded predictable results, would have been fully compatible with Aminzade,

and would have been a mere design choice. Motivation to do so arises from at least common sense and the disclosures of Aminzade and Soli set forth above.

VIII. GROUND 3: CLAIMS 3, 10-11, 14, 21-22 ARE OBVIOUS IN LIGHT OF AMINZADE, SOWERS, AND HONG

253. As set forth above, Aminzade combined with Sowers discloses and renders obvious claims 1 and 12. *See* Ground 1. Claim 1 is the independent claim on which claims 3 and 10-11 depend (either directly or indirectly), and claim 12 is the independent claim on which claims 14 and 21-22 depend (either directly or indirectly).

- A. Claim 3 (“The system according to claim 1, wherein the first communication interface and the second communication interface are Wi-Fi interfaces and communication between the first communication interface and the second communication interface includes establishing a Wi-Fi Direct connection.”)**

254. Aminzade combined with Sowers and Hong discloses this limitation. Aminzade discloses *the first communication interface, the second communication interface, and communication between them*. *See* Ground 1, limitations 1.a.ii and 1.b.iii.

255. Hong discloses that a “[s]uitable technology for implementing ... short-range communication” between two devices such as a smartphone and a smartwatch is “Wi-Fi Direct.” EX1008, ¶79 (“short-range communication module 114” of Figure 2A implements “Wi-Fi Direct”), ¶59 (Figure 2A is a block diagram of the “mobile terminal”), ¶51 (the “mobile terminal” may be a “smart phone”),

¶80 (or a “smart watch”); EX1009, ¶66, ¶46, ¶38, ¶67.

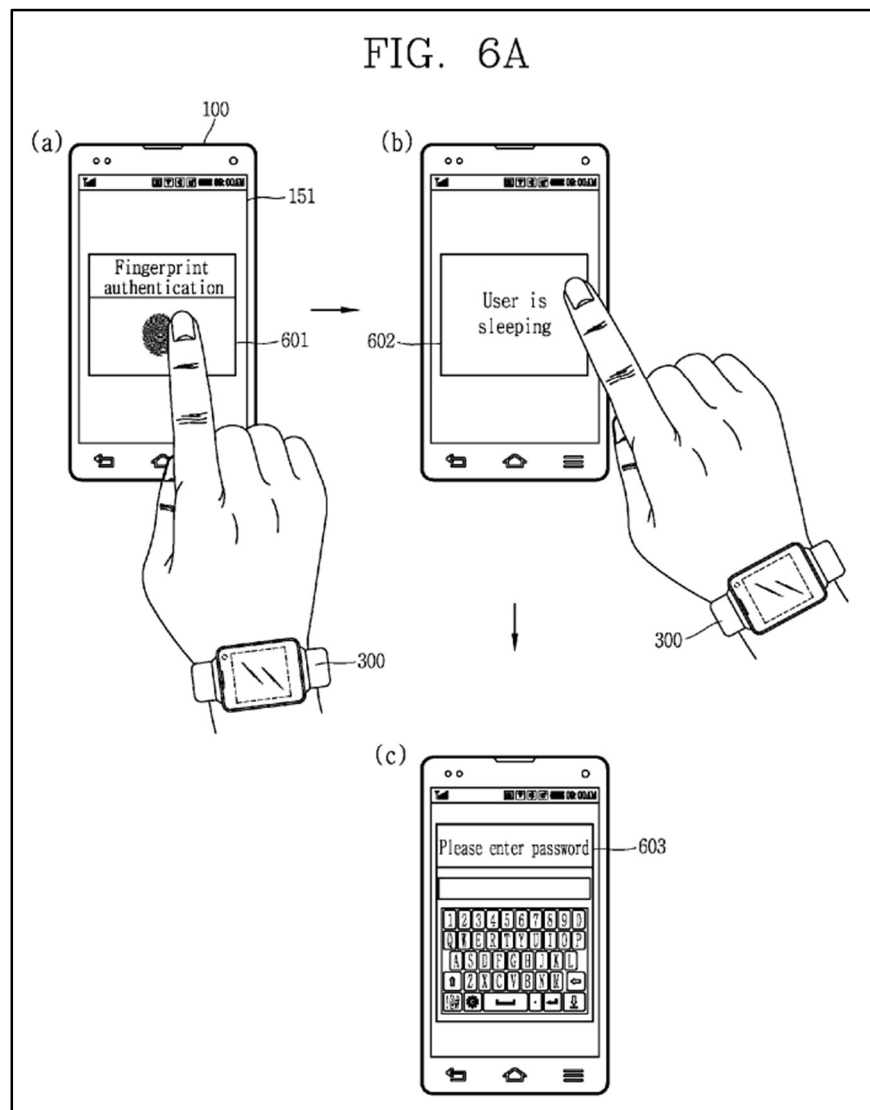
256. In my opinion, it would have been obvious to a POSITA to combine this functionality of Hong with Aminzade for the reasons in Section VIII.G.

B. Claim 10 (“The system according to claim 1, wherein upon determining that the user is in a state matching predetermined criteria, the second information processing device limits an operation of the second information processing device by displaying a screen seeking confirmation from the user that the user intended to execute the operation.”)

257. Aminzade combined with Sowers and Hong discloses this limitation. Aminzade discloses mobile device 10 (*a second information processing device*). See Ground 1, limitation 1.b.

258. Hong discloses a “smart watch” that communicates with “mobile terminal” that may be a “smart phone” (also *a second information processing device*). EX1008, ¶80 (“smart watch”), ¶160 (“watch type mobile terminal”), Fig. 2D, ¶51 (“smart phone”), Figs. 2B, 1 (showing both); EX1009, ¶67, ¶147, Fig. 2D, ¶38, Figs. 2B, 1. Upon the user providing input such as “a touch” for user authentication (*an operation of the second information processing device*), the smartphone’s “controller 180” determines whether the user is “sleeping” or “in a psychological state satisfying a predetermined abnormal condition” (each *determining that the user is in a state matching predetermined criteria*). EX1008, ¶¶236-237 (“sleeping” state), Fig. 6A, ¶30 (“sleeping or ... abnormal condition”), ¶208 (upon “an information input” (*an operation*), detect “sleeping, or ... coercive,

intimidated, stress state”); EX1009, ¶¶223-224, Fig. 6A, ¶27, ¶195. If the user is in such a state, the smartphone *displays a screen* requesting additional authentication, such as a password, as shown below. EX1008, ¶¶236-237 (“another authentication method with an increased security level”), ¶30 (“an input corresponding to another authentication method to be additionally requested”), ¶208 (“another authentication method”), Fig. 6A; EX1009, ¶¶223-224, ¶27, ¶195.



In my opinion, a POSITA would have understood such a request for additional authentication *seek[s] confirmation from the user that the user intended to execute the operation* because if the user performs the additional authentication (*e.g.*, the password authentication of Figure 6A), it indicates that the user intended to authenticate himself or herself via the original authentication method (*e.g.*, the fingerprint authentication of Figure 6A). The request for additional authentication also *limits* the user's original request for authentication via fingerprint (*limits that operation*) by not authenticating the user unless the user provides a password.

259. It would have been obvious to a POSITA to combine this functionality of Hong with Aminzade for the reasons in Section VIII.G.

C. Claim 11 (“The system according to claim 10, wherein the operation is executed on the second information processing device after the user provides confirmation in response to displaying of the screen.”)

260. Aminzade combined with Sowers and Hong discloses and renders obvious this limitation. Aminzade discloses mobile device 10 (*a second information processing device*). *See* Ground 1, limitation 1.b.

261. As described above for claim 10, Hong discloses a “smart phone” (*also a second information processing device*) that *display[s] [a] screen* requesting additional authentication (*e.g.*, a password) when determining that the user is in one of certain states when the user is attempting user authentication (*the operation*) (*e.g.*, via a fingerprint). The additional “user authentication [is] carried out” (*the*

operation is executed). EX1008, ¶31; EX1009, ¶28. Also, in my opinion, a POSITA would have understood that when the user provides input for the additional authentication, the smartphone authenticates the user (*the operation is executed*) because, otherwise, it would not make sense for the smartphone to seek input for that additional user authentication. It also would have been obvious to a POSITA to do so for the same reasons.

262. It would have been obvious to a POSITA to combine this functionality of Hong with Aminzade for the reasons in Section VIII.G.

D. Claim 14 (“The method according to claim 12, wherein the first communication interface and the second communication interface are Wi-Fi interfaces and the communication performed between the first communication interface and the second communication interface includes establishing a Wi-Fi Direct connection.”)

263. Aminzade combined with Sowers and Hong discloses this limitation.

See Ground 3, claim 3.

E. Claim 21 (“The method according to claim 12, wherein upon determining that the user is in a state matching predetermined criteria, the second device limits an operation of the second device by displaying on the display screen a message seeking confirmation from the user that the user intended to execute the operation.”)

264. Aminzade combined with Sowers and Hong discloses this limitation.

See Ground 3, claim 10.

F. Claim 22 (“The method according to claim 21, wherein the operation is executed on the second device after the user provides confirmation in response to the displaying of the message on the display screen.”)

265. Aminzade combined with Sowers and Hong discloses and renders obvious this limitation. *See* Ground 3, claim 11.

G. Combining Hong with Aminzade (and Sowers).

266. In my opinion, it would have been obvious to a POSITA to combine the Hong functionality cited above with Aminzade (and Aminzade combined with Sowers).

267. A POSITA could have used Wi-Fi Direct in the Aminzade system simply by choosing Wi-Fi Direct as the protocol to use for Aminzade’s “direct wireless communication connection” between its two devices on a “WiFi” network. EX1004, 7:39-50. Doing so would have been merely choosing among a number of finite, identified, predictable solutions (known Wi-Fi protocols). Motivation to do so arises from Hong’s disclosure of using “Wi-Fi Direct” for “short-range communications,” which applies to Aminzade’s wearable device and mobile device, and from Aminzade’s disclosure of using “WiFi” for “direct wireless communication.” *See* claim 3; EX1004, 7:39-50.

268. A POSITA could have added Hong’s request for additional authentication depending on the user’s state by adding the appropriate functionality from Hong’s smartwatch 300 and smartphone 100 to Aminzade’s corresponding

smartwatch and smartphone. EX1008, ¶51 (“smart phone”), ¶80 (“smart watch”), Figs. 2B-D, 3; EX1009, ¶38, ¶67, Figs. 2B-D, 3. In my opinion, a POSITA could have readily done so because, for example, Aminzade’s mobile phone already supports fingerprint and password authorization. EX1004, 8:38-43. In addition, Aminzade’s wearable device 20 can accommodate “additional components,” such as the Hong sensor(s) to detect the user’s state. *Id.*, Fig. 3, 17:10-16; EX1008, ¶196, ¶199, ¶¶208-209; EX1009, ¶183, ¶186, ¶¶195-196.

269. Motivation to do so arises from Aminzade’s disclosure of increasing security (*e.g.*, by locking a device) depending on the state of the user (*e.g.*, the user is not wearing the wearable device). EX1004, Fig. 9, 25:20-26:10. This would have led a POSITA to also increase security as warranted by other conditions, such as detecting that the user is in a “sleeping or ... stress state.” *See* claim 10. Similar motivation arises from Hong’s teaching of enhancing security using biometric data, which would have led a POSITA to do the same. EX1008, ¶18; EX1009, ¶15.

IX. GROUND 4: CLAIMS 3, 10-11, 14, 21-22 ARE OBVIOUS IN LIGHT OF AMINZADE, SOLI, AND HONG

270. Aminzade combined with Soli discloses and renders obvious claims 1 and 12. *See* Ground 2. Aminzade combined with Soli and Hong discloses and renders obvious claims 3, 10-11, 14, and 21-22 for the reasons in Ground 3 for Aminzade combined with Sowers and Hong. Those reasons apply equally to

Aminzade combined with Soli and Hong because Hong's teachings are combined with Aminzade and Soli in the same way they are combined with Aminzade and Sowers.

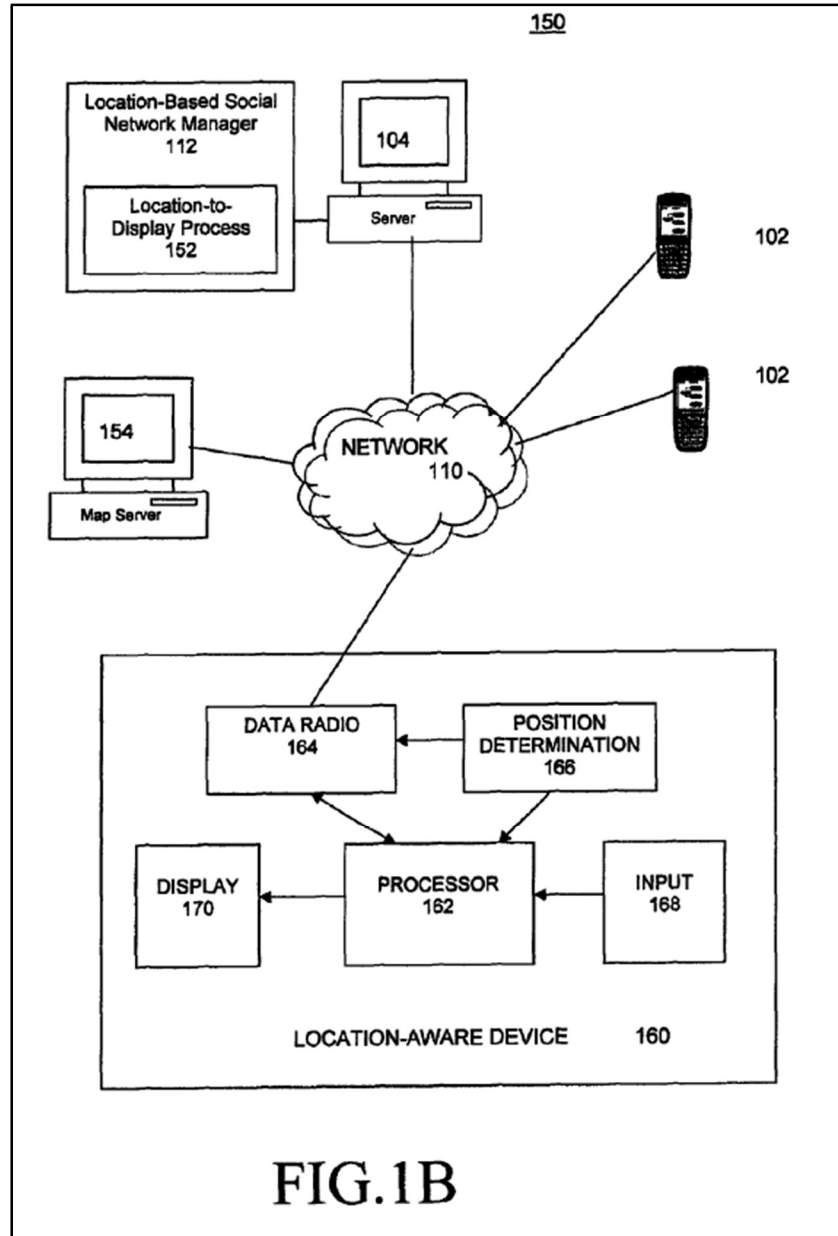
X. GROUND 5: CLAIMS 8-9 AND 19-20 ARE OBVIOUS IN LIGHT OF AMINZADE, SOWERS, AND ALTMAN

271. Aminzade combined with Sowers discloses and renders obvious claims 1 and 12, on which claims 8-9 and 19-20 respectively depend (directly or indirectly). *See* Ground 1.

- A. Claim 8 (“The system according to claim 1, wherein the second information processing device gets position information denoting a position of the second information processing device and automatically transmits the position information to a predetermined address based on reception of a user input that is determined to be a predetermined type of user input during a time period, wherein the predetermined address is not inputted by the user during the time period.”)**

272. Aminzade combined with Sowers and Altman discloses and renders obvious this limitation. Aminzade discloses mobile device 10 (*a second information processing device*). *See* Ground 1, limitation 1.b.

273. Altman discloses “a location-aware mobile device 160” that is a “mobile phone or similar mobile device” (also *a second information processing device*), shown below. EX1010, 6:16-22, Figs. 1A-1B.



Device 160 includes “position determination unit 166” that determines “[l]ocation information for the device,” such as “latitude/longitude” data (*gets position information denoting a position of the second information processing device*). *Id.*, 6:25-31, Fig. 1B. Device 160 then “transmits the location data for the device ... to server 104” (*automatically transmits the position information to a predetermined*

address). *Id.*, 6:35-37, Fig. 1B, 17:17-20. This process is an “*automatic* location updating process,” and a POSITA also would have understood it to be automatic because the passages cited above include no manual steps. *Id.*, 11:1-3, 11:8-13, 12:11-14; *see also id.*, 17:56-18:16 (the frequency transmitting location data to the server is automatically adjusted based on the user’s movement), 18:35-39, 18:49-53, Fig. 10 (step 1014).

274. In my opinion, a POSITA also would have understood that the “server” (*e.g.*, server 104) to which the mobile device sends its location information implicitly and necessarily (inherently) has a *predetermined address*, such as an IP address and/or URL, because it is “a server or workstation class computer” and is accessible to mobile device 160 via “network 110,” which may be “the Internet.” EX1010, 5:1-3, 5:6-9, 6:35-37, Figs. 1A-B. Moreover, Altman does not disclose that the user provides the address of the server (*the predetermined address is not inputted by the user during the time period* described below or otherwise). It also would have been obvious to a POSITA to give the server a *predetermined address not inputted by the user* so that mobile device 160 can automatically update its location to the server, as Altman discloses and as described above. Motivation to do so arises at least from Altman’s disclosure and a desire to increase ease of use.

275. Altman also discloses a user providing input to opt-in to location-

based features (*a user input determined to be a predetermined type of user input*).

EX1010, 10:32-36 (“consent-based features ... based upon receiving a user’s authorization”), 10:61-65 (“users ... turning on or off their location sharing capability”), 22:50-54 (“location-based coupons [for] users who have opted-in”), 23:12-17 (“‘opt-in’ coupons”), 23:49-52 (“ad ... based on user location (opt-in)”).

A user’s opt-in selection “can be implemented through means of a toggle switch ... on the mobile device or [a] web page” (also *a user input determined to be a predetermined type of user input*). *Id.*, 10:61-62. The period of time during which the user makes the opt-in selection and the system processes it is *a time period during* which the opt-in selection is *determined* to be a *predetermined type of input* (an opt-in selection), because the system then enables the location-based feature to which the user opted-in, as described above. *See also id.*, 11:8-12 (“automatic location updating ... if location sharing is enabled”).

276. It would have been obvious to a POSITA to combine this functionality of Altman with Aminzade for the reasons in Section X.E.

B. Claim 9 (“The system according to claim 8, wherein the position information is automatically transmitted in response to the user input and without requiring additional user input that explicitly requires approval of the automatic transmission of the position information during the time period.”)

277. Aminzade combined with Sowers and Altman discloses and renders obvious this limitation.

278. As described for claim 8, Altman discloses that a user can opt-in (*the user input*) to location-based features such as sharing location with friends and receiving location-based ads or coupons. *See also* EX1010, 6:44-48 (displaying location to friends), 7:56-65 (same), Figs. 2A-B. If the user opts-in to such features (*in response to the user input*), mobile device 160 *automatically transmit[s]* its location information (*the position information*) to server 104. *See* claim 8; EX1010, 11:8-12 (“*automatic* location updating ... if location sharing is enabled”). Altman does not disclose any *requir[ement]* of *additional user input* that *explicitly requires approval of the automatic transmission of the position information during the time period* of claim 8 or otherwise. And a POSITA would have understood that Altman has no such additional requirement. That is, after a user opts-in to the location-based features, there is no additional input the user must provide for approval of the location-sharing. Requiring such additional input would not make sense because the user already has opted-in, and it does not make sense to opt-in twice. Altman therefore discloses this limitation. It also would have been obvious to a POSITA to not require additional user input for approval after the user already has opted-in, for the reasons described above.

279. It would have been obvious to a POSITA to combine this functionality of Altman with Aminzade for the reasons in Section X.E.

- C. Claim 19 (“The method according to claim 12, wherein the second device gets position information denoting a position of the second device and automatically transmits the position information to a predetermined address based on reception of a user input that is determined to be a predetermined type of user input during a time period, wherein the predetermined address is not inputted by the user during the time period.”)**

280. Aminzade combined with Sowers and Altman discloses and renders obvious this limitation. *See* Ground 5, claim 8.

- D. Claim 20 (“The method according to claim 19, wherein the position information is automatically transmitted in response to the user input and without requiring additional user input that explicitly requires approval of the automatic transmission of the position information during the time period.”)**

281. Aminzade combined with Sowers and Altman discloses and renders obvious this limitation. *See* Ground 5, claim 9.

- E. Combining Altman with Aminzade (and Sowers)**

282. It would have been obvious to a POSITA to combine the Altman functionality cited above with Aminzade (and Aminzade combined with Sowers).

283. A POSITA could have done so by, for example, adding any of Altman’s disclosed location detection circuitry to Aminzade’s mobile device 10. EX1010, 7:13-26 (*e.g.*, “GPS module”). A POSITA could have readily done so because such modules were supported by even the 2007-era flip phones described in Altman. *Id.*, cover page (2007 filing date), Fig. 2A. A POSITA also could have readily added Altman’s other functionality in the form of “software instructions” to Aminzade’s mobile device. *Id.*, 5:3-5; EX1004, 10:8-10 (mobile device 10’s

processor executes instructions).

284. Motivation to do so arises from Altman's disclosure that its location-based features "greatly enhance[] the social networking capability of [mobile] devices" and "enhance the effectiveness of ad campaigns." EX1010, 1:33-67. Doing so would have led a POSITA to implement such functionality in other mobile devices, including Aminzade's mobile device 10.

285. Doing so therefore would have merely applied a known technique (Altman's cited functionality) to a known device (Aminzade's mobile device) that was ready for improvement (the cited location-based features) to yield predictable results.

XI. GROUND 6: CLAIMS 8-9 AND 19-20 ARE OBVIOUS IN LIGHT OF AMINZADE, SOLI, AND ALTMAN

286. Aminzade combined with Soli discloses and renders obvious claims 1 and 12. *See* Ground 2. Aminzade combined with Soli and Altman discloses and renders obvious claims 8-9 and 19-20 for the reasons in Ground 5 for Aminzade combined with Sowers and Altman. Those reasons apply equally to Aminzade combined with Soli and Altman because Altman's teachings are combined with Aminzade and Soli in the same way they are combined with Aminzade and Sowers.

XII. CONCLUSION

287. For these reasons, it is my opinion that the claims of the '228 patent

are unpatentable.

APPENDIX A



Seth James Nielson's Vita

(512) 387-4310

seth@crimsonvista.com

October 2024

Academic Degrees

2009	Ph.D. Computer Science , Rice University, Houston, TX
2004	M.S. Computer Science , Brigham Young University, Provo, UT
2000	B.S. Computer Science , Brigham Young University, Provo, UT

Certifications

CISSP

Current Appointments

Founder and Chief Scientist	Crimson Vista, Inc.
Director of Cybersecurity Research	Curuvar LLC
Adjunct Assistant Professor	University of Texas at Austin Law School
Senior Fellow	Robert Strauss Center for International Security and Law

Professional Advising

2019-Present	Advisory Board	Syccure Inc.
--------------	----------------	--------------

Non-profit and Community Engagement

2021-Present	Founding Director	The Crypto Done Right Foundation
2019-2021	Cyberlab Advisory Board	The SEED School of Maryland

Grants and Research Awards

Decentralizing Zero-Trust Infrastructure to Combat Advanced Persistent Threats and Malicious Insiders (Senior Personnel), NSF 2020 SBIR solicitation. Award number 2051989, Curuvar LLC.

Mitigation of Ransomware, DoD 2018.B STTR solicitation (Army), Topic: A18B-T010, Crimson Vista, \$150,000 (2019)

An Enabling Repository of Cryptographic Knowledge (Co-PI), Cisco Grant, Johns Hopkins University Information Security Institute, \$150,000 (2017-2021)

University Research Funding

Sel4 Security Appliance Capstone, funded by Crimson Vista to Brigham Young University Department of Computer Science. 2021

Academic Awards

Brown Fellowship
John and Eileen Tietze Fellowship

Professional Service

International Cryptographic Module Conference, 2018-2024 Program Committee

Subject Matter Expertise and Selected Projects

Forensic Analysis (e.g., Code/IP Theft)

Trusted images research (UT Austin, 2024)

Investigation of email transmissions, reception (Crimson Vista, 2024-)

Investigation of stolen digital documents, provenance, handling (Crimson Vista, 2023-)

Investigation of cryptocurrency transfers and fraud (Crimson Vista, 2023-)

Investigation of website content development and provenance (Crimson Vista, 2023-2024)

Investigation of server, laptop, and hard drives for indications of tampering (Crimson Vista, 2023)

Investigation of voting machine software for vulnerabilities (Crimson Vista, 2022-)

Investigation of altered/forged emails (Crimson Vista, 2022)

CLE training related to source code analysis/trade secrets (Source Code Discovery, 2021)

Investigation of IP/code theft related to MTA, spear-phishing, and email (Crimson Vista, 2019-2021)

Investigation of code theft related to housing and rental software (Crimson Vista, 2019-2022)

Investigation of code development for security vulnerabilities/intrusion (Crimson Vista, 2020)

Investigation of code theft related to digital mobile radios (Crimson Vista, 2017-2021)

Investigation of code theft related to financial trading software (Crimson Vista, 2016-2017)

Investigation of code theft related to e-commerce (Harbor Labs, 2015)

Investigation of IP theft related to domain anti-abuse (Harbor Labs, 2015)

Investigation of IP theft related to high-frequency trading (Harbor Labs, 2010-2011)

Applied Cryptography

Cryptography training modules (UT Austin, 2022-)

Analysis of compromised password hashes (Crimson Vista, 2020)

"Crypto Done Right", Cryptographic Knowledge Base Non Profit (2020-)

"Crypto Done Right", Cryptographic Knowledge Base with Cisco (Johns Hopkins, 2017-2020)

Simulated implementation of Vehicle-to-Vehicle authentication (Crimson Vista, 2018-2019)

Cryptographic protocol analysis and design for Syccure Inc. (Crimson Vista, 2017-2023)

Timing attacks on Hardware Security Modules with Diamond Key Security (Johns Hopkins, 2018)

Technical consulting for U.S. Dpt. of Justice (Antitrust Division, Transportation, Energy & Agriculture) (Crimson Vista, 2018)

Aircraft/drone anti-collision protocol security with OnBoard Security (Johns Hopkins, 2017)

Cryptographic communication library for Security First Corp (ISE, 2010-2011)

Encryption library, file system encryption, GPU for Security First Corp (ISE, 2005-2011)

Security Operations, Compliance, Oversight

SEC cybersecurity disclosures (Crimson Vista, 2024-)

GDPR, Privacy, PII analysis (Crimson Vista, 2024-)

Security analysis of Twitter cybersecurity operations/practices (Crimson Vista, 2022)

Virtual Chief Information Security Officer for IperionX (Crimson Vista, 2022-2023)

IoT Devices and IoT Security

Robotic automation system (Crimson Vista, 2024-)

Traffic lights and systems software analysis (Crimson Vista, 2023-2024)

Vulnerability and exploitation analysis of voting machine hardware (Crimson Vista, 2023-)

High-security appliance based on formal methods (Crimson Vista, BYU, 2021)

Hadoop security research (Crimson Vista, 2021-2022)

IoT data sensors for agricultural operations (Crimson Vista, 2020-2023)

Contributor, reviewer for the Institute of Assured Autonomy (Johns Hopkins, 2019)

IoT data aggregation security with Armored Things (Johns Hopkins, 2018-2019)

Automated IoT device profiling with the Physics Lab (Johns Hopkins, 2018)

Physical forensics from IoT devices (Johns Hopkins 2017)

Network Security

Bluetooth-enabled alert system security analysis (Crimson Vista, 2024)

Web security, cookies, XSS, XSRF training modules (UT Austin, 2023-)

Phishing samples analysis (Crimson Vista, 2022-2023)

WiFi transmission analysis, packet capture (Crimson Vista, 2023-2024)

Security-Focused Data Discovery Methods and Practice (Crimson Vista, 2022-2023)

Analysis of weaknesses in two-factor authentication (Crimson Vista, 2022-2023)

Analysis of bots on Twitter in terms of prevalence, stealth, and impact (Crimson Vista, 2022)

Secure distributed computing (Curuvar, 2021-2023)

Hadoop deployment and security considerations (Crimson Vista, 2021-2022)

SSO technology evaluation and test (UT Austin, Crimson Vista, 2021-2022)

Information risk assessment with respect to data breach (Crimson Vista, 2020-2021)

Data breach analysis with respect to password authentication (Crimson Vista, 2020-2021)

Network security curriculum design for Law and Policy (University of Texas at Austin, 2020-)

Network security curriculum design for undergraduates (University of Texas at Austin, 2020-2021)

Network security curriculum design (Johns Hopkins, 2013-2019)

Security analysis of financial services vendor for Fortune-100 client (Crimson Vista, 2018-2019)

Analysis of secure e-mail transmission for confidential client (Crimson Vista, 2018-2019)

Cloud storage system security evaluation for confidential client (Harbor Labs, 2015)

Secure gateway security and compliance evaluation for SecurityFirst Corp (Harbor Labs, 2015)

Gateway caching security/privacy engineering (Google, 2005)

Malware and Viruses

Ransomware training modules (UT Austin, 2022-)

Ransomware recovery research and development (Crimson Vista, 2018-2019)

Advanced malware and malware defenses analysis (Johns Hopkins, 2018)

Malware Analysis for Confidential Client (Crimson Vista, 2016)

Privacy

Investigation of biometric tracking in commercial systems (Crimson Vista, 2024-)

Investigation of location tracking in mobile devices (Crimson Vista, 2021-)

Investigation of biometric tracking/transmission in devices and systems (Crimson Vista, 2021-)

Development of an auditing tool for cookies and other web tracking (Crimson Vista, 2020, 2024)

Audit of a large hospital network for cookies and web tracking (Confidential client, 2020)

Development of a privacy curriculum for data architects (Crimson Vista, 2019)

Anonymization of threat indicators with the Applied Physics Lab (Johns Hopkins, 2017)

Analysis of anti-piracy vendor for Center for Copyright Information (Harbor Labs, 2013-2014)

Miscellaneous Security Technologies

Distributed ledger technology for secure state replication (Curuvar, 2021-2023)

Blockchain technology for sale and/or licensing of intellectual property (Crimson Vista, 2021-2022)

Blockchain technology analysis for a start-up (Crimson Vista, 2019-2020)

Analysis of cyber security norms for a confidential Fortune 100 client (Crimson Vista, 2018-2019)

Analysis of vulnerabilities in portable chemical manufacturing system (Johns Hopkins, 2018)

Open-Source Contribution and Sponsorship for The PyPy Project (Crimson Vista, 2018-2019)

Blockchain and smart contract design for confidential start-up (Crimson Vista, 2018)

Medical device system security evaluation for confidential client (Harbor Labs, 2015)

Software Engineering and Software Analysis

Automotive source code analysis (Crimson Vista, 2024-)

Medical implant source code analysis (Crimson Vista, 2024-)

Automated least-privilege compilation/language research (UT Austin 2024-)

Review of failed software project, root cause analysis, attribution (Crimson Vista, 2024-)

Review of development practices, error handling, and robustness (Crimson Vista, 2023-)

Open-source licensing analysis, build, and test (Crimson Vista, 2023-)

GitHub analysis and statistics for effort estimation (Crimson Vista, 2022)

Software theft analysis and tool design for various clients (Crimson Vista, 2018-)

Cyber insurance investigations for Clyde & Co (Crimson Vista, 2018-2019)

Distributed code coverage analysis tool for a confidential Fortune 100 client (ISE, 2011)

Software engineering for Metrowerks Inc. (2001-2003, formerly Lineo Inc.)

Code Languages: C, C++, Java, Python, Ruby, Scala, RTL/VHDL/Verilog, JavaScript, Go

Publications

Books

Seth James Nielson, *Discovering Cybersecurity: A Technical Introduction for the Absolute Beginner*. (December 2023).

Seth James Nielson, Christopher K. Monson, *Practical Cryptography in Python, Learning Correct Cryptography by Example*. (October 2019).

Refereed Publications

Joseph Kosturko, Eric Schlieber, Sean Futch, Seth James Nielson, *Cracking a Continuous Flow Reactor: A Vulnerability Assessment for Chemical Additive Manufacturing Devices*. In *Proceedings of the 2018 IEEE International Symposium on Technologies for Homeland Security*. (September 2018)

Chanyang Shin, Prerit Chandok, Ran Liu, Seth James Nielson, Timothy Leschke, *Potential Forensic Analysis of IoT Data: An Overview of Amazon Echo, Z-wave, and Home Router Data Extraction and Analysis*. In *Proceedings of the 2017 IEEE International Conference on Internet of Things (iThings)*, Exeter, UK, pp. 705-710 (June 2017).

Seth James Nielson, *PLAYGROUND: Preparing Students for the Cyber Battleground*. *Computer Science Education*, volume 26, issue 4, pp. 255-276, (January 2017).

Seth James Nielson and Charles D. Knutson, *Design Dysphasia and the Design Patterns Maintenance Cycle*. *Information & Software Technology*, volume 48, number 8, pp. 660- 675, (August 2006)

Seth James Nielson, Scott S. Crosby, and Dan S. Wallach, *A Taxonomy of Rational Attacks*. In *Proceedings of the Fourth International Workshop on Peer-to-Peer Systems (IPTPS '05)*, Ithaca, New York, (February 2005)

Seth J. Nielson and Charles D. Knutson. *OO++: Exploring the Multiparadigm Shift*. *Proceedings of the Workshop on Multiparadigm Programming with Object-Oriented Languages (MPOOL 2004)*, Oslo, Norway, (June 2004)

Rob Kunz, Seth Nielson, Mark Clement, Quinn Snell, *Effective Bandwidth for Traffic Engineering*, *Proceedings of the IEEE Workshop on High Performance Switching and Routing (HPSR 2001)*, Dallas, TX, (May 2001)

Testimony Before Government Bodies

Testimony in support of *Maryland SB 151/HB 211 Criminal Law - Crimes Involving Computers – Ransomware*. Testimony given to the Judicial Proceedings Committee of the Maryland Senate and the Judiciary Committee of the Maryland House of Delegates (January/February 2019)

Invited Talks, Panels, and Technical Training

Seth James Nielson, *Data Security: Four Approaches to a Better Defensive Posture*, 2023 Enterprise Data World, Anaheim, CA (September 2023)

[CANCELED DUE TO VENUE CHANGE] Seth James Nielson, *Maintaining Data Security and Data Privacy in the 21st Century*, 2022 Enterprise Data World, San Diego, CA (March 2022)

Seth James Nielson, *Securing Your Data Assets Against Hackers*, 2021 Enterprise Data World, Boston, MA. (April 2021)

Seth James Nielson, *The Cybersecurity of IP*, 2020 Essential Cybersecurity Law, Austin, TX (Virtual). (July 2020)

[CANCELED DUE TO COVID 19] Seth James Nielson and Ellie Daw, *Correct Cryptography in Python*, a Tutorial for Cryptography Beginners, PyCon 2020, Philadelphia, PA. (April 2020)

[CANCELED DUE TO COVID 19] Seth James Nielson, *Protecting Your Data Assets*, 2020 Enterprise Data World, Boston, MA. (March 2020)

Seth James Nielson, *Security and Privacy for Data Architects*, 2019 Data Architecture Summit, Chicago, IL (October 2019)

Seth James Nielson, *Crypto Done Right, One Year In. Lessons Learned and Next Steps*. Presented in the International Cryptographic Knowledge Base 2019 (ICMC 2019), Vancouver, Canada (May 2019)

Panel Discussion, *Hardening US Unmanned Systems Against Enemy Counter Measures*. Accepted invitation to 7th Annual DoD Unmanned Systems Summit, Alexandria, VA (April 2019).

Seth James Nielson, *A Gentle Introduction to Blockchain*. 2019 Enterprise Data World, Boston, MA (March 2019).

Seth James Nielson, *A Gentle Introduction to Blockchain*. 2018 Data Architecture Summit, Chicago, IL (October 2018).

Seth James Nielson, *Detecting Malicious Sandboxes*. Workshop on Defensive Deception and Trust in Autonomy, San Diego, CA (August 2018).

Seth James Nielson and Debra Baker, *Towards a Crowd-Sourced Cryptographic Knowledge Base*. Presented in the International Cryptographic Knowledge Base 2018 (ICMC18), Ottawa, Canada (May 2018).

Seth James Nielson, *The PyPy Sandbox*. Presented in the National Centers of Academic Excellence Tech Talk, Online (March 2018).

Theses

PhD Thesis: Designing Incentives for Peer-to-Peer Systems (defended 10/2009)

Master's Thesis: OO++ Design Patterns, GOF Revisited (defended 8/2004)

Technical Reports

Seth James Nielson and Dan S. Wallach, *The BitTorrent Anonymity Marketplace*, arXiv Technical Report 1108.2718, (August 2011)

Seth James Nielson, Caleb E. Spare, and Dan S. Wallach, *Building Better Incentives for*

Robustness in BitTorrent, arXiv Technical Report 1108.2716, (August 2011)

Seth James Nielson, Seth J. Fogarty, and Dan S. Wallach, *Attacks on Local Searching Tools*, arXiv Technical Report 1108.2704 (Originally produced in December, 2004, available on arXiv as of August 2011)

White Papers and Trade Publications

Seth James Nielson, *Techniques for Discovering Unauthorized Copying in Software*, Crimson Vista White Paper, (January 2022)

Aviel D. Rubin, Seth J. Nielson, Christopher K. Monson, *Evaluation of the MarkMonitor AntiPiracy System*, Produced for the Center for Copyright Information (December 2013)

Aviel D. Rubin, Seth J. Nielson, Sam Small, Christopher K. Monson, *Guidelines for Source Code Review in Hi-Tech Litigation*, Harbor Labs White Paper (September 2013)

Undergraduate Advising

Independent Research and Capstones (University of Texas Austin)

Charlotte White, *Automated Partitioning of Software During Compilation*, CS 370, Independent Study, Summer 2024

Nishaanth Saaketh Joopelli, *Automated Patching of Unsafe C Functions*, CS 370, Independent Study, Summer 2024

Tanuj Tekkale, *Analysis of Image Provenance Techniques*, CS 370, Independent Study, Summer 2024

Andrew Dang, *Individual Voice Recognition using Machine Learning*, CS 370, Independent Study, Summer 2023

Monique Tran, *Malware Classification with SVM*, CS 370, Independent Study, Summer 2023

Gonzalo Tamariz-Martel Sánchez, *SMART CONTRACTS: Different approaches to introduce external (off-chain) data* (June 2022)

Graduate Advising

Capstones for Masters of Science in Security Informatics (Johns Hopkins)

Weizhou Wang, Runjie Zhang, *Research on defense next-generation malware on the Windows platform* (December 2018)

Yu-Tsern Jou, Ying Liu, Menghan Bai, *Open Source HSM Side Channel Analysis* (December 2018)

Bowen Shi, Hong Ma, Mengqi Qin, *Side Channel Attack on HSM Based on Machine Learning* (December 2018)

Dylan Richmond, Matthew Shonman, Jingcheng Yang, *An Exploration of the Usability of HTTPS* (December 2018)

Steven Cheng, Venkata Aditya Bollapragada, and Antara Sargam, *Using Selective RAM Journaling to Fight Ransomware* (December 2018)

Yongqiang Fan, Haiwen Sun, *Fault Tolerance System for IoT* (December 2018)

WeiKe Chen, Harry Luo, Prashanth Venkateswaran, *IoT Discovery* (August 2018)

Joseph “Jay” Kosturko, Eric Schlieber, Sean Futch, *Cracking a Continuous Flow Reactor: A Vulnerability Assessment for Chemical Additive Manufacturing Devices* (May 2018)

Chao Lei, Wenjun Li, *Anti-Honeypot Detection in Advanced Botnet Attacks* (December 2017)

Ritvik Sachdev, Purushottam Kulkarni, Praveen Malhan, *Securing ADS-B Based Airborne Collision Avoidance Systems* (December 2017)

Ningyuan Bao, Mengying Hu, *Security-Testing-Orientated Internet of Things(IoT) Simulator* (December 2017)

Zehuan Li, Shanshan Yang, Liangjia Fu, *AIS Data De-anonymization* (December 2017)

Chanyang Shin, Prerit Chandok, Aurin Chakravarty, *Forensic Data Collection from IoT Devices* (December 2017)

Kevin Manzotti, Kashif Memon, Rahul Durgad, *Replication of CryptoDrop* (December 2016)

Harshneel More, Jingmiao Wang, Yuanqi Zhu, *Detecting XSS attacks using BRO IDS* (December 2016)

Asmaa Aljohani, Gyan Namdhari, Yue Zhu, *Feasibility, Security and Privacy Analysis of EMVCo Payment Tokenization Technology for Identity Enabled Transactions* (December 2016)

Richard Eaton, *The Emperor Has No Friends: Identifying Botnet Customers and Mapping Out Botnets on Twitter* (May 2015)

Jingru Chen, Yaning Liu, Yifan Yu, Zhiyue Zu, *Investigating the Heartbleed Vulnerability* (2015)

Kartik Thapar, *Security Techniques for Developing iOS Applications* (February 2015)

Jie Feng, Jianxiang Peng, Likai Zhang, *De-anonymizing BitCoin* (January 2014)

Teaching

University of Texas at Austin

Cybersecurity Tech/Law Policy (2020-)
Network Security and Privacy (2020-2021)

Johns Hopkins University

Advanced Network Security (2017 - 2019)
Network Security (2014 – 2019)

Rice University

Data Structures and Algorithms (Spring 2008)

Patents

Co-inventor: Nielson, S. 2021. Distributed Authentication Between Network Nodes. U.S. Patent 11,032,252 filed January 2, 2019 and issued June 8, 2021.

Co-inventor: Orsini, R. 2014. Systems and methods for security data in motion. U.S. Patent 8,745,372 filed November 24, 2010 and issued June 3, 2014.

Co-inventor: Orsini, R. 2014. Systems and methods for security data in motion. U.S. Patent 8,745,379 filed August 20, 2012 and issued June 3, 2014.

Co-inventor: O'Hare, R. 2014. Systems and methods for security data. U.S. Patent 8,677,148 filed January 27, 2012 and issued March 18, 2014.

In the News

"Johns Hopkins Researchers and OnBoard Security Team Up to Protect Drones," *Robotics Tomorrow*, 3/16/2018

"Rice University Computer Scientists Find a Flaw in Google's New Desktop Search Program." *New York Times*, 12/20/2004

Employment History

University of Texas at Austin

2020-

Adjunct Assistant Professor

Source Code Discovery, LLC.

2019-2021

Founder and Partner

Crimson Vista, Inc.

2016-Present

Founder and Chief Scientist

Johns Hopkins Applied Physics Lab

2018-2019

Senior Professional Staff (Temp/On-Call)

Johns Hopkins University

2016-2019

Director of Advanced Research Projects

2015-2019

Adjunct Associate Research Scientist

2014

Lecturer

Harbor Labs, LLC

2014-2015

Principal

2011-2014

Research Scientist

Independent Security Evaluators

2010-2011

Senior Security Analyst

2005-2009 **Security Analyst**

Google, Inc.
2005 **Summer Intern**

Metrowerks (Formerly Lineo, Inc.)
2001-2003 **Software Engineer II**

Expert Testimony

On behalf of LG Electronics in TOT Power Control v LG Electronics; C.A No. 21-1304-MN

Counsel: DLA Piper
Venue: District of Delaware
Subject Matter: Outer loop power control, source code
Reports: 1 report September 2024

On behalf of Dexcom in Dexcom v Abbott Diabetes Care; C.A. No. 22-605-KAJ

Counsel: Quinn Emanuel
Venue: District of Delaware
Subject Matter: Glucose alerts source code
Reports: 1 report September 2024

On behalf of Axonics in In the Matter of Certaom Video Processing Devices and Components
Thereof; Investigation No. 337-TA-1396

Counsel: Tensegrity
Venue: ITC
Subject Matter: Medical implant wireless transmission source code
Reports: 2 reports September 2024

On behalf of Apple in Carbyne v. Apple; Civil Action No. 1:23-cv-00324

Counsel: Ropes and Gray
Venue: West District of Texas, Austin Division
Subject Matter: Authentication, Secure Storage, Secure Processing, Access
Reports: 1 report August 2024, 1 report September 2024
Deposition: 1 deposition October 2024

On behalf of Commure in Commure v. Canopy Works; Case No. 3:24-cv-02592-AMO

Counsel: Quinn Emanuel
Venue: Norther District of California
Subject Matter: Security norms and customs related to wireless security
Reports: 1 declaration August 2024
Deposition: 1 deposition September 2024

On behalf of Samsara In the Matter of Certain Vehicle Telematics, Fleet Management, and Video-
based Safety Systems, Devices, and Components Thereof, Investigation No. 337-TA-1393

Counsel: Kirkland and Ellis
Venue: ITC
Subject Matter: Automotive tracking, safety, analysis source code

Reports: 1 report August 2024, 1 report September 2024
Deposition: 1 deposition September 2024

In support of Unified's Request for Ex Parte Reexamination of 10,601,780

Counsel: Unified Patents
Venue: PTAB
Subject Matter: Network security and data filtering
Reports: 1 declaration, August 2024

On behalf of BOKF in Dynapass v BOKF

Counsel: Fish and Richardson
Venue: Eastern District of Texas, Marshall Division
Subject Matter: Multifactor Authentication, Financial Systems
Reports: 1 report May 2024

On behalf of Samsung in Samsung v Maxell

Counsel: DLA Piper
Venue: PTAB
Subject Matter: Biometrics
Reports: 1 declaration April 2024

On behalf of Forescout Technologies in Fortinet v Forescout Technologies

Counsel: Winston & Strawn
Venue: Northern District of California
Subject Matter: Network security architecture and devices
Reports: 1 report March 2024
Deposition: 1 deposition May 2024

On behalf of Threat Modeler Software in Iriusrisk v Threat Modeler Software

Counsel: Rimon
Venue: PTAB
Subject Matter: Threat modeling
Reports: 1 declaration January 2024, 1 declaration February 2024
Deposition: 1 deposition March 2024, 1 deposition April 2024

On behalf of Motorola Solutions in Motorola Solutions v. Hytera Communications

Counsel: Kirkland and Ellis
Venue: Northern District of Illinois, Eastern Division
Subject Matter: Source code forensics
Reports: 1 declaration January 2024
Deposition: 1 deposition February 2024

In support of Unified's Request for Ex Parte Reexamination of U.S. Patent 7,586,871

Counsel: Univied Patents
Venue: PTAB
Subject Matter: Network security and data filtering
Reports: 1 declaration, February 2024

On behalf of the State of Texas in State of Texas v. Google

Counsel: Norton Rose Fulbright
Venue: District Court of Victoria County Texas
Subject Matter: Location tracking
Reports: 1 report, January 2024
Deposition: 1 deposition May 2024

In support of Unified's Request for Ex Parte Reexamination of U.S. Patent 9,264,441

Counsel: Rothwell, Figg, Ernst, and Manbeck
Venue: PTAB
Subject Matter: Network security devices and operations
Reports: 1 declaration, January 2024

On behalf of Dennis Zeedyk in the United States vs. Dennis Zeedyk (2023-Present)

Counsel: Saul Euwing
Venue: Northern District of Indiana South Bend Division
Subject Matter: Website forensics
Reports: 1 report November 2023

On behalf of OpenAI in OpenAI v Open Artificial Intelligence and Guy Ravine (2023-Present)

Counsel: Quinn Emanuel
Venue: Northern District of California
Subject Matter: Forensic investigation of website and related assets
Reports: 1 report October 2023

On behalf of Palo Alto Networks in Centripetal Networks v Palo Alto Networks (2021-Present)

Counsel: Norton Rose Fulbright and Ropes & Gray
Venue: Eastern District of Virginia
Subject Matter: Network security devices
Reports: 3 reports issued August 2023, September 2023, and October 2023
2 related declarations for EPR submitted July 2024
Deposition: 1 deposition October 2023
In Court: January 2024

On behalf of Anchor Semiconductor in Elite v. Anchor (2022-Present)

Counsel: Venable
Venue: Northern District of California
Subject Matter: Forensic investigation of alleged sabotage and data destruction
Reports: 1 report July 2023

In support of Unified Patents in Ex Parte Reexamination of U.S. Patent 9,438,614

Counsel: Unified Patents
Venue: PTAB
Subject Matter: Machine learning and intrusion detection systems
Reports: 1 declaration Apr 2023

On behalf of Trend Micro in Trend Micro v. TaaSera Licensing (2022-Present)

Counsel: Marbury Law Group
Venue: PTAB
Subject Matter: Security technologies and devices (various)

Reports: 4 declarations Apr 2023

On behalf of Salesforce in WSOU Investments v. Salesforce (2022-Present)

Counsel: Quinn Emanuel
Venue: Western District of Texas
Subject Matter: Source code related to transmission of marketing emails
Reports: 1 report March 2023
Deposition: 1 deposition August 2023

On behalf of Trend Micro in Trend Micro v. Webroot (2022-Present)

Counsel: Marbury Law Group
Venue: PTAB
Subject Matter: Security technologies and devices (various)
Reports: 5 declarations Feb-Mar 2023, 5 declarations September 2023

On behalf of Fox News in Dominion Voting Systems v. Fox News (2022-2023)

Counsel: Winston and Strawn
Venue: Superior Court of the State of Delaware
Subject Matter: Voting machine security including forensic investigation
Reports: 1 Report December 2022
Deposition: 1 deposition February 2023

On behalf of Public Storage in Estch v. Public Storage (2022-2023)

Counsel: Orrick
Venue: Eastern District of Texas
Subject Matter: VoIP, authentication, authorization
Reports: 1 Report January 2023
Deposition: 1 deposition January 2023

On behalf of Lenovo/Motorola Mobiliy in Maxell Ltd v. Lenovo/Motorola Mobility (2022-2023)

Counsel: Kirkland and Ellis
Venue: ITC
Subject Matter: Authentication
Reports: 1 Declaration November 2022
2 Reports February 2023
Deposition: 1 deposition March 2023

On behalf of Elon R Musk in Twitter Inc v. Elon R Musk (2022)

Counsel: Quinn Emanuel Urquhart & Sullivan, LLP
Venue: Court of Chancery of the State of Delaware
Subject Matter: Evaluation of Security in light of Whistleblower Report
Reports: 1 Report October 2022

On behalf of Bissell, Inc. in Bissell Inc. v. Tineco Intelligent Technology Co. Ltd., (2022)

Counsel: Quinn Emanuel Urquhart & Sullivan, LLP
Venue: ITC
Subject Matter: Forensic evaluation of source code
Reports: 1 Report submitted September 2022
Deposition: 1 deposition November 2022

In Court: December 2022

On behalf of Hakkasan USA in Hakkasan USA v Endurance American Specialty Insurance (2022)

Counsel: Quinn Emanuel Urquhart & Sullivan, LLP
Venue: District of Nevada (Clark County)
Subject Matter: Forensic evaluation of emails
Reports: 1 Report submitted May 2022
Deposition: 1 deposition July 2022

On behalf of JTC in Seimens vs JTC (2021-2022)

Counsel: Peckar and Abramson, PC
Venue: American Arbitration Association
Subject Matter: Software Engineering Efforts
Reports: 1 Report submitted in July 2021
1 Report submitted in September 2021
Deposition: 1 deposition October 2021
In Court: March 2022 (arbitration)

On behalf of Samsung in Samsung v. Proxense (2021-2022)

Counsel: Quinn Emanuel Urquhart & Sullivan, LLP
Venue: Western District of Texas (Waco)
Subject Matter: Authentication, Authorization, Device-to-device
Reports: 1 declaration submitted October 2021
Deposition: 1 deposition October 2022

On behalf of Bitglass in Netskope, Inc. v. Bitglass Inc. (2021-2022)

Counsel: Irell and Manela, LLP
Venue: PTAB Petition for Inter Partes Review
Subject Matter: Authentication, Single-Sign-On
Reports: 1 declaration submitted September 2021
1 declaration submitted March 2021

On behalf of The State of Arizona in Arizona v. Google (2021-2022)

Counsel: Ruttenberg IP Law
Venue: Superior Court of the State of Arizona (Maricopa)
Subject Matter: Privacy, Location tracking, Data collection
Reports: 1 declaration submitted August 2021

On behalf of TLC in TLC v. Koninklijke Philips N.V., US Philips Corporation (2019-2021)

Counsel: Perkins Coie LLP
Venue: PTAB Petition for Inter Partes Review
Subject Matter: Cryptographic protocols
Reports: 1 declaration submitted February 2021

On behalf of Magic Micro in Monsoon v. Magic Micro (2020-2021)

Counsel: Gutnicki, LLP
Venue: International Centre for Dispute Resolution
Subject Matter: Blockchain, file storage
Reports: 1 declaration submitted October 2020

In Court: 1 declaration submitted November 2020
In arbitration December 2020

On behalf of Juniper in Juniper Networks Inc. v. Huawei Digital Technologies Co. (2020-2021)

Counsel: Irell and Manella, LLP
Venue: PTAB Petition for Inter Partes Review
Subject Matter: Network perimeter defense against malware
Reports: 1 declaration submitted June 2020
1 declaration submitted July 2021
Deposition: 1 deposition April 2021

On behalf of DivX in Netflix v. DivX (2020-2023)

Counsel: Lowenstein & Weatherwax, LLP
Venue: PTAB Petition for Inter Partes Review
Subject Matter: Encryption of streaming media
Reports: 1 declaration submitted May 2020
1 declaration submitted December 2020
1 declaration submitted April 2021
Deposition: 1 deposition January 2021, 1 deposition February 2021

On behalf of Juniper in Juniper Networks Inc. v. Implicit LLC (2019-2020)

Counsel: Irell and Manella, LLP
Venue: PTAB Petition for Inter Partes Review
Subject Matter: Packet classification
Reports: 1 declaration submitted February 2020

On behalf of the Dealership class in Dealer Management Systems Antitrust Litigation (2019-Present)

Counsel: Milberg Phillips Grossman LLP
Venue: Case No. 18-cv-00864 (Northern District of Illinois)
Subject Matter: Cybersecurity, risk assessment, third-party access
Reports: 1 report submitted November 2019
Deposition: 1 deposition January 2020

On behalf of Symantec in the Trustees of Columbia University in the City of New York v. Symantec Corporation. (2018-2022)

Counsel: Quinn Emanuel Urquhart & Sullivan, LLP
Venue: Case No. Civil Action No. 3:13-cv-00808-JRS (Eastern District of Virginia)
Subject Matter: Deception technologies, Honeypots
Reports: 1 report submitted October 2019
Deposition: 1 deposition January 2020

On behalf of Proofpoint in Proofpoint Inc. v. Vade Secure (2019-2021)

Counsel: Quinn Emanuel Urquhart & Sullivan, LLP
Venue: Case No. 3:19-cv-04238 (Northern District of California)
Subject Matter: Cloud-based email, malware detection, AI
Reports: 1 report submitted September 2019, 1 report submitted December 2019
1 report submitted February 2021, 1 report submitted April 2021
Deposition: 1 deposition April 2021

In Court: Expert testimony August 2021

On behalf of Bitdefender in Finjan Inc. v. BitDefender Inc. (2018-2021)

Counsel: Susman Godfrey LLP
Venue: Case No. 4:17-cv-4790-HSG (Northern District of California)
Subject Matter: Web threat detection, malware, gateways
Reports: 1 report submitted July 2019, 1 report submitted August 2019
Deposition: 1 deposition October 2019

On behalf of HTC in Koninklijke Philips N.V., US Philips Corporation v. HTC Corp., HTC America Inc. (2019-2020)

Counsel: Perkins Coie LLP
Venue: Case No. 4:18-cv-01887-HSG (Northern District of California)
Subject Matter: Cryptographic protocols
Reports: 1 report submitted May 2019, 1 report submitted June 2019
Deposition: 1 deposition August 2019

On behalf of Juniper in Juniper Networks Inc. v. Finjan Inc. (2018-2019)

Counsel: Irell and Manella, LLP
Venue: PTAB Petition for Inter Partes Review
Subject Matter: Malware, firewall/gateway, network security
Reports: 4 declarations submitted October 2018
Deposition: 1 deposition June 2019

On behalf of Redbox in Disney Enterprises, Inc., LucasFilm Ltd, LLC, and MVL Film Finance LLC v. Redbox Automated Retail, LLC. (2018)

Counsel: Robins Kaplan LLP
Venue: Case No. 2:17-cv-08655-DDP (AGRx) (Central District of California, Western Division)
Subject Matter: DRM, cloud security, media streaming
Reports: 1 declaration submitted May 2018

On behalf of Trend Micro in Trend Micro, Inc. v. Security Profiling, LLC (2017-2018)

Counsel: The Marbury Law Group, PLLC
Venue: Inter Partes Review Case No. IPR2017-02191 and IPR2017-02192
Subject Matter: Automated security patches
Reports: 2 declarations submitted September 2017
Deposition: 1 deposition June 2018

On behalf of TeleSign in Twilio Inc. v. TeleSign Corporation (2016-2021, multiple cases)

Counsel: Shook, Hardy & Bacon LLP
Venue: Inter Partes Review Case No. IPR2016-01688, IPR2016-00360, IPR2017-01976 IPR2017-01977, IPR2017-01978
Case No. 5:16-cv-6925-LHK (Nor. District of California, San Jose Div.)
Subject Matter: Telecommunications security
Reports: 1 declaration submitted August 2016, May 2017, and July 2017
Deposition: 1 deposition November 2016, 1 deposition July 2017, 1 deposition August 2017

On behalf of Blue Coat in Finjan Inc. v. Blue Coat Systems LLC (2017-2018)

Counsel: Originally Wilson, Sonsini, Goodrich and Rosati PC; later Morrison & Foerster LLP
Venue: Case No. 15-cv-03295-BLF-SVK (Nor. District of California, San Div.)
Subject Matter: Firewalls, gateway, security devices, malware
Reports: 1 report submitted April 2017
Deposition: 1 deposition April 2017
In Court: Tech tutorial February 2017, expert testimony November 2017

On behalf of Sedosoft in Sedosoft Inc. v Mark Burchett LTD and NFSx9 LLC (2016)

Counsel: McInnes and McLane LLP
Venue: Case No. Civil Action No. 1:15-cv-10244-RGS (District of Massachusetts)
Subject Matter: Code theft
Reports: 1 report submitted May 2016 and August 2016

On behalf of USAA in Asghari-Kamrani, et al. v. United Services Automobile Association, Inc.

Counsel: Fish and Richardson PC
Venue: Inter Partes Review Case No. IPR2015-01842, and CBM2016-00063, CBM2016-00064
Subject Matter: Applied cryptography, authentication
Reports: 1 report submitted September 2015, 1 report submitted April 2016
Deposition: 1 deposition March 2017

On behalf of WTS Paradigm in WTS PARADIGM, LLC v EDGEAQ, LLC (2015-2016)

Counsel: Quarles & Brady LLP
Venue: Case No. 3:15-CV-330 (Western District of Wisconsin)
Subject Matter: Software-assisted product configuration, presentation, and ordering
Reports: 1 report submitted March 2016
Deposition: 1 deposition April 2016

On behalf of Mr Leon Stambler in Mr. Leon Stambler v Mastercard IPR (2015-2016)

Counsel: Flachsbart & Greenspoon, LLC
Venue: CBM2015-00044
Subject Matter: Authentication, authentication codes
Reports: 1 declaration submitted October 2015
Deposition: 1 deposition December 2015

On behalf of Trusteer/IBM in Trusted Knight Corporation v. International Business Machines Corporation and Trusteer, Inc. (2015)

Counsel: Quinn Emanuel Urquhart & Sullivan LLP
Venue: C.A. No. 14-1063 LPS-CJB (District of Delaware)
Subject Matter: Key logging, protections against
Reports: 1 declaration submitted July 2015

On behalf of Sensus in Sensus USA, Inc. v. Certified Measurement, LLC (2015)

Counsel: Feldman Gale PA
Venue: Inter Partes Review Case No. IPR2015-01262, IPR2015-01311, IPR2015-01439, IPR2015-01454
Case number 3:14-cv-01069 (District of Connecticut)

Subject Matter: Applied cryptography, certification of data
Reports: 1 declaration submitted June 2015, 4 declarations submitted July 2015

On behalf of Chad Eichenberger in Chad Eichenberger v. ESPN (2015)

Counsel: Edelson PC
Venue: Case No. 2:14-cv-00463 (Western District of Washington)
Subject Matter: Consumer privacy
Reports: 1 declaration submitted January 2015

On behalf of Optimum Content Protection in Microsoft Corporation v. Optimum Content Protection LLC. (2014)

Counsel: Sidley Austin LLP
Venue: Inter Partes Review No. IPR2015-00048
Subject Matter: DRM, data streaming, protection
Reports: 1 declaration submitted October 2014

On behalf of Fortinet in Fortinet v. Sophos (2014-2015, multiple cases)

Counsel: Quinn Emanuel Urquhart & Sullivan LLP
Venue: Inter Partes Review No. IPR2015-00618
Case No. 3:13-cv-05831-EMC (DMR) (Nor. District of California, SF div.)
Case No. 1:14-cv-00100-GMS (District of Delaware)
Subject Matter: Antivirus, anti-malware
Reports: 2 declarations submitted September 2014, 1 submitted September 2015
1 report submitted October 2015, November 2015
Deposition: 1 deposition October 2014, 1 deposition October 2015
In Court: Tech tutorial December 2015

On behalf of Afiliis in Afiliis PLC v Architelos Inc and Alexa Raad (2015)

Counsel: Haynes Boone LLP
Venue: Case No. 1:15-cv-00014-LMB-JFA (Eastern District of Virginia)
Subject Matter: Domain name system anti-abuse
Reports: 1 report submitted April 2015, May 2015
Deposition: 1 deposition June 2015
In Court: Expert testimony August 2015

On behalf of Telit in M2M v. Motorola, Telit (2015-2016)

Counsel: Pearl Cohen Zedek Latzer Baratz LLP
Venue: Case No. 12-033-RGA (District of Delaware)
Subject Matter: Authentication
Reports: 1 declaration submitted May 2014,
1 report submitted July 2014, August 2014
Deposition: 1 deposition June 2015

On behalf of Rmail/Rpost in Rmail Limited, v. Amazon.com, Inc., and Paypal and Rmail Limited, Rpost Communications Limited, and Rpost Holdings Inc., v. DocuSign, Inc. (2013-2014)

Counsel: Hudnell Law Group PC
Venue: Case No. 2:10-CV-258-JRG (Lead Case)
Case No. 2:11-CV-299-JRG (Member Case) (E.D. Texas)
Subject Matter: Email security

Reports: 2 reports April 2013, 1 declaration June 2013
Depositions 1 deposition May 2013 (2 days)

On behalf of Via Vadis in Via Vadis v. Skype (2012-2014)

Counsel: WTP Law
Venue: Via Vadis v. Skype, Case No. 11-507 (RGA) (District of Delaware)
Subject Matter: P2P communications
Reports: 1 affidavit December 2012