

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner

v.

ISCAN2D TECHNOLOGIES, LLC,
Patent Owner

Case IPR2026-00316
U.S. Patent No. 11,664,123

**PETITION FOR *INTER PARTES* REVIEW
OF U.S. PATENT NO. 11,664,123**

Mail Stop "PATENT BOARD"
Patent Trial and Appeal Board
U.S. Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	THE '123 PATENT	2
	A. Summary	2
	B. Prosecution History	2
	C. Person of Ordinary Skill in Art (POSA)	3
III.	CLAIM CONSTRUCTION	4
IV.	FOUNDATIONS	4
V.	GROUND 1: BISHOP IN VIEW OF LEBOEUF RENDERS OBVIOUS CLAIMS 1-5, 7-15, AND 17-20.	7
	A. Bishop.....	7
	B. LeBoeuf.....	8
	C. Motivation to Combine	9
	D. Independent Claims.....	14
	1. Claim 1	14
	2. Claim 11	31
	E. Dependent Claims	36
	1. Claims 2 and 12.....	36
	2. Claims 3 and 13.....	36
	3. Claims 4 and 14.....	36
	4. Claims 5 and 15.....	37
	5. Claims 7 and 17.....	37
	6. Claims 8 and 18.....	38
	7. Claims 9 and 19.....	40
	8. Claims 10 and 20.....	40
VI.	GROUND 2: BISHOP-LEBOEUF FURTHER IN VIEW OF WILLIAMS RENDERS OBVIOUS CLAIMS 6 AND 16.	41
	1. Williams	41
	2. Claims 6 and 16.....	42

VII.	GROUND 3: BISHOP-LEBOEUF FURTHER IN VIEW OF KOVITZ RENDERS OBVIOUS CLAIMS 7-8 AND 17-18.....	43
VIII.	GROUND 4A: BROWN IN VIEW OF WEISS RENDERS OBVIOUS CLAIMS 1-5, 9-15, AND 19-20	46
A.	Brown	46
B.	Weiss	47
C.	Motivation to Combine	48
D.	Independent Claims.....	52
1.	Claim 1	52
2.	Claim 11	67
E.	Dependent Claims	70
1.	Claims 2 and 12.....	70
2.	Claim 3 and 13	71
3.	Claims 4 and 14.....	71
4.	Claims 5 and 15.....	72
5.	Claims 9 and 19.....	72
6.	Claims 10 and 20.....	72
IX.	GROUND 4B: BROWN-WEISS FURTHER IN VIEW OF ORT TEACHES CLAIMS 1-5, 9-15, AND 19-20	74
X.	GROUND 5A AND 5B: BROWN-WEISS AND BROWN-WEISS- ORT FURTHER IN VIEW OF WILLIAMS RENDERS OBVIOUS CLAIMS 6 AND 16.....	77
XI.	GROUND 6A AND 6B: BROWN-WEISS AND BROWN-WEISS- ORT FURTHER IN VIEW OF KOVITZ RENDERS OBVIOUS CLAIMS 7-8 AND 17-18.....	78
XII.	CERTIFICATION UNDER RULE 42.104(A)	80
XIII.	MANDATORY NOTICES (37 C.F.R. § 42.8(A)(1)).....	81
A.	Real Party-in-Interest (37 C.F.R. § 42.8(b)(1)):	81
B.	Related Matters (37 C.F.R. § 42.8(b)(2)).....	81
C.	Lead and Back-up Counsel (37 C.F.R. § 42.8(b)(3)).....	81
D.	Service Information (37 C.F.R. § 42.8(b)(4))	82

XIV. CONCLUSION.....	83
----------------------	----

PETITIONER'S EXHIBIT LIST

Exhibit No.	Description
1001	U.S. Patent No. 11,664,123 to McKirdy
1002	File History of U.S. Patent No. 11,664,123
1003	Declaration of Prashant Shenoy in Support of Petition for <i>Inter Partes</i> Review of U.S. Patent No. 11,664,123
1004	U.S. Patent Application Publication No. 2011/0072263 to Bishop et al. ("Bishop")
1005	U.S. Patent Application Publication No. 2008/0146892 to LeBoeuf et al. ("LeBoeuf")
1006	U.S. Patent Application Publication No. 2011/0081860 to Brown et al. ("Brown")
1007	International Patent Application Publication No. WO 2010/144626 to Weiss ("Weiss")
1008	U.S. Patent Application Publication No. 2012/0198531 to Ort et al. ("Ort")
1009	U.S. Patent Application Publication No. 2010/0012715 to Williams et al. ("Williams")
1010	U.S. Patent Application Publication No. 2008/0052243 to Narayanaswami et al. ("Narayanaswami")
1011	U.S. Patent No. 4,403,869 to Crutcher ("Crutcher")
1012	U.S. Patent No. 2,612,994 to Woodland et al. ("Woodland")
1013	Pavlidis et al., "Fundamentals of Bar Code Information Theory," IEEE (1990)

Exhibit No.	Description
1014	Gao et al., “Understanding 2D-BarCode Technology and Applications in M-Commerce – Design and Implementation of a 2D Barcode Processing Solution,” (31st Annual International Computer Software and Applications Conference (2007))
1015	Pavlidis, “A New Paper/Computer Interface: Two-Dimensional Symbolologies,” IEEE (2000)
1016	U.S. Patent Application Publication No. 2012/0024956 to Chen (“Chen”)
1017	Parikh et al., “Localization and Segmentation of a 2D High Capacity Color Barcode,” 2008 IEEE Workshop on Applications of Computer Vision
1018	Bagherinia et al., “A Theory of Color Barcodes,” UC Santa Cruz (2011)
1019	Grillo et al., “High Capacity Colored Two Dimensional Codes,” Proceedings of the International Multiconference on Computer Science and Information Technology (2010)
1020	Claycomb et al., “Using a Two Dimensional Colorized Barcode Solution for Authentication in Pervasive Computing,” ACS/IEEE International Conference on Pervasive Services (2006)
1021	U.S. Patent No. 8,823,494 to Kovitz et al. (“Kovitz”)
1022	U.S. Patent Application Publication No. 2011/0295502 to Faenger (“Faenger”)
1023	U.S. Patent Application Publication No. 2005/0139680 to Anttila et al. (“Anttila”)
1024	U.S. Patent Application Publication No. 2008/0132798 to Hong et al. (“Hong”)
1025	U.S. Patent Application Publication No. 2011/0066009 to Moon et al. (“Moon”)

Exhibit No.	Description
1026	U.S. Patent Application Publication No. 2010/0121227 to Stirling et al. (“Stirling”)
1027	U.S. Patent Application Publication No. 2012/0067944 to Ross (“Ross”)
1028	U.S. Patent Application Publication No. 2008/0210754 to Lovett (“Lovett”)
1029	U.S. Patent Application Publication No. 2005/0032515 to Mastio (“Mastio”)
1030	U.S. Patent Application Publication No. 2010/0321609 to Qui et al. (“Qui”)
1031	U.S. Patent Application Publication No. 2010/0156676 to Mooring et al. (“Mooring”)
1032	U.S. Patent Application Publication No. 2008/0168361 to Forstall et al. (“Forstall”)
1033	<i>Curriculum Vitae</i> of Dr. Prashant Shenoy
1034	File History of U.S. Patent No. 12,230,394

CLAIM LISTING

1.P	A wearable activity device, wherein the wearable activity device is comprised of:
1.1	a display device;
1.2	at least one of an accelerometer configured to track activity and an embedded bio-metric monitoring sensor configured to detect a bio-metric characteristic;
1.3	wireless communication circuitry, wherein the wireless communication circuitry is configured to establish a wireless communications link with a mobile device;
1.4	at least one processor with software, wherein the processor is associated with a memory device and wherein the at least one processor is in signal communication with the display device and the wireless communication circuitry;
1.5	the memory device associated with the at least one processor, wherein the memory device is configured to store wireless pairing information associated with the wireless communication circuitry;
1.6	wherein the processor software is configured to: obtain, from the memory device, the wireless pairing information associated with the wireless communication circuitry,
1.7	generate a color coded digital scannable media responsive to the wireless pairing information,
1.8	control the display device, wherein the display device is configured to display the color coded digital scannable media,
1.9	establish, via the wireless communication circuitry, the wireless communications link with the mobile device responsive to the mobile device scanning and decoding the color coded displayed digital scannable media,
1.10	generate at least one of activity tracking information and bio-metric information, and

1.11	communicate, via the wireless communications link, at least one of the activity tracking information and the bio-metric information to the mobile device.
2	The wearable activity device of claim 1, wherein the wearable activity device is at least one of a smartwatch device and a wearable health monitoring device.
3	The wearable activity device of claim 1, wherein the wireless communication circuitry is further configured to establish at least one of a near field communications link, a wide area network communications link, and a personal area network communications link with the mobile device.
4	The wearable activity device of claim 1, wherein the mobile device is at least one of a smartphone and a tablet device.
5	The wearable activity device of claim 1, wherein the wireless pairing information associated with the wireless communication circuitry is at least one of a MAC address identifier associated with the wireless communication circuitry and an identification identifier associated with the wearable activity device.
6	The wearable activity device of claim 1, wherein the wireless pairing information is encrypted by the processor software.
7	The wearable activity device of claim 1, wherein the wireless pairing information further includes a combination of the wireless communication circuitry information and at least one of user identification identifier and wearable activity device information.
8	The wearable activity device of claim 7, wherein the wearable activity device information is at least one of the wearable activity device type, an error code associated with the wearable activity device, workout performance data generated by the wearable activity device, date and time stamp information generated by the wearable activity device, facility location identifier associated with the physical location of the wearable activity device, user ID information associated with a user of the wearable activity device, wearable activity device software information, and wearable activity device utilization information.

9	The wearable activity device of claim 1, wherein the color coded digital scannable media includes at least one of a QR code, a 2D Matrix code, a 3D barcode, a representation of non-human readable information using colored pixels, an augmented reality marker, an augmented reality image, and an augmented reality code.
10	The wearable activity device of claim 1, wherein the display device is at least one of a touchscreen display, a LED display and a LCD display.
11.P	A method for establishing a communications link between a wearable activity device and a mobile device, the method comprising:
11.1	storing, by a memory device associated with the wearable activity device, wireless pairing information associated with wireless communication circuitry disposed within the wearable activity device,
11.2	receiving, by a processor associated with the wearable activity device, the wireless pairing information associated with the wireless communication circuitry from the memory device,
11.3	generating, by the processor associated with the wearable activity device, a color coded digital scannable media responsive to the wireless pairing information,
11.4	displaying, by a display device associated with the wearable activity device, the color coded digital scannable media,
11.5	scanning, by the mobile device, the color coded digital scannable media,
11.6	processing, by the mobile device, the color coded digital scannable media, and
11.7	establishing, by the mobile device, a wireless communications link with the wearable activity device responsive to the mobile device processing the color coded digital scannable media,
11.8	generating, by the wearable activity device processor, at least one of activity information and bio-metric information, wherein the at

	least one of the activity information and bio-metric information is stored in the memory device associated with the wearable activity device, and
11.9	communicating, via the wireless communications link by the wearable activity device, at least one of the activity tracking information and the bio-metric information to the mobile device.
12	The method of claim 11, wherein the wearable activity device is at least one of a smartwatch device and a wearable health monitoring device.
13	The method of claim 11, wherein the wireless communication circuitry is further configured to establish at least one of a near field communications link, a wide area network communications link, and a personal area network communications link with the mobile device.
14	The method of claim 11, wherein the mobile device is at least one of a smartphone and a tablet device.
15	The method of claim 11, wherein the wireless pairing information associated with the wireless communication circuitry is at least one of a MAC address identifier associated with the wireless communication circuitry and a wearable activity device identification number associated with the wearable activity device.
16	The method of claim 11, wherein the wireless pairing information is encrypted by the wearable activity device processor software.
17	The method of claim 11, wherein the wireless pairing information further includes a combination of at least one of a user identification identifier, the wireless communication circuitry information and the wearable activity device information.
18	The method claim 17, wherein the wearable activity device information is at least one of the wearable activity device type, an error code associated with the wearable activity device, workout performance data generated by the wearable activity device, date and time stamp information generated by the wearable activity device, facility location identifier associated with the physical

	location of the wearable activity device, user ID information associated with a user of the wearable activity device, wearable activity device software information, and wearable activity device utilization information.
19	The method of claim 11, wherein the digital scannable media is at least one of a QR code, a 2D Matrix code, a 3D barcode, a representation of non-human readable information using colored pixels, a augmented reality marker, a augmented reality image, and a augmented reality code.
20	The method of claim 11, wherein the display device is at least one of a touchscreen display, a LED display and a LCD display.

Apple Inc. petitions for *inter partes* review of claims 1-20 of U.S. Patent No. 11,664,123 (“the ’123 patent”; EX1001).

I. INTRODUCTION

The ’123 patent claims nothing new. It is directed to techniques for establishing wireless connections using barcodes and sending biometric data over those connections. During prosecution of a related patent, the Examiner acknowledged that establishing wireless connections using barcodes was known before the earliest possible priority date of the ’123 patent. The patent’s alleged novelty thus stems from the *type* of data communicated once the wireless connection is established. But communicating biometric data over wireless communication links was also well-known before the ’123 patent.

The prior art asserted herein teaches each and every claim element and renders obvious claims 1-20. Bishop, Brown, Ort, Kovitz, and Williams all teach systems for establishing wireless communications links using barcodes that encode wireless pairing information. LeBoeuf and Weiss teach wearable devices that generate biometric and activity related data and communicate it to mobile devices over wireless communications links.

This Petition is supported by the testimony of Dr. Shenoy, an expert in the field of electrical and computer engineering with over 30 years of experience. Dr. Shenoy shows that each claim of the ’123 patent is disclosed by the prior art, and

that a person of ordinary skill in the art (POSA) would have been motivated to adapt the prior art to arrive at the challenged claims.

The Board should thus institute review of the '123 patent and cancel all claims.

II. THE '123 PATENT

A. Summary

The '123 patent teaches a “general system 100 for obtaining, communicating and processing information via a barcode.” EX1001, 3:56-62. The system 100 includes a data generation device that communicates with a user’s mobile device. *Id.* The data generation device “generat[es] user data,” “processes the user data [to] generate[] barcode data,” and displays the barcode data “in graphical form.” *Id.*, 4:5-20. The mobile device then “scan[s] the barcode... processes the barcode data and if necessary, operates in response to the barcode data.” *Id.*, 4:20-25.

In the claims, the data generation device is a *wearable activity device* and the barcode data comprises *wireless pairing information* encoded in a *color coded digital scannable media* (barcode). The *mobile device* scans this color coded barcode to establish a *wireless communications link* with the wearable activity device. The mobile device then receives and displays *activity tracking information* or *bio-metric information* generated by the wearable activity device.

B. Prosecution History

The application that led to the '123 patent was filed February 22, 2021, and

was allowed after a single office action. EX1002, 120-31, 156-63. In response to the office action, the Applicant amended the claims to recite “wireless pairing information” and “color coded digital scannable media.” EX1002, 146-55. After the Notice of Allowance, the Applicant amended the claims again to recite a “wearable activity device” instead of the exercise device. The Examiner again allowed the claims without further rejection.

However, during prosecution of a related application, the same Examiner acknowledged that Brown, asserted herein, “teaches performing Bluetooth pairing between two devices where a first device generates a barcode that encodes the Bluetooth pairing data that is scanned using a camera as a barcode scanner.” EX1034, 177-89. The Examiner also acknowledged that “[t]he prior art teaches encoding pairing information as color information.” *Id.* Despite this, the Examiner allowed the claims because the prior art allegedly did not teach using such established wireless communication links to communicate biometric or activity related data. *See id.* But as explained herein, the asserted prior art teaches these elements.

C. Person of Ordinary Skill in Art (POSA)

A POSA at the time of the ’123 patent was filed would have had a bachelor’s degree in Computer or Electrical Engineering or an equivalent discipline, and approximately two years’ experience in telecommunications or

computer networking. EX1003, ¶¶66-67. Additional education could substitute for professional experience, and significant work experience could substitute for formal education. *Id.*

III. CLAIM CONSTRUCTION

Absent lexicography or disavowal, claim terms in an IPR are given their plain and ordinary meaning in light of the specification and prosecution history.

Sisvel Int’l S.A. v. Sierra Wireless, Inc., 81 F.4th 1231, 1236 (Fed. Cir. 2023).

Petitioner submits that all claim terms should receive their plain and ordinary meaning in the context of the ’123 patent specification. In particular, Petitioner submits that the plain and ordinary meaning of the term “color coded” is: “having color other than ‘black-white’ that encodes data.” *See* EX1001, 28:36-63.

Petitioner submits that no other term needs express construction.

IV. GROUNDS

Apple requests IPR on the following Grounds under 35 U.S.C. § 103:

Ground	Claims	Combination of References
1	1-5, 7-15, 17-20	Bishop-LeBoeuf
2	6, 16	Bishop-LeBoeuf-Williams
3	7-8, 17-18	Bishop-LeBoeuf-Kovitz
4A	1-5, 9-15, 19-20	Brown-Weiss

4B	1-5, 9-15, 19-20	Brown-Weiss-Ort
5A	6, 16	Brown-Weiss-Williams
5B	6, 16	Brown-Weiss-Ort-Williams
6A	7-8, 17-18	Brown-Weiss-Kovitz
6B	7-8, 17-18	Brown-Weiss-Ort-Kovitz

Each reference is prior art to the '123 patent, which claims an earliest possible priority date of August 5, 2011¹:

- U.S. 2011/0072263 (“Bishop”) was filed September 23, 2009, and published March 24, 2011. Bishop is prior art under at least §102(a) and (e).
- U.S. 2008/0146892 (“LeBoeuf”) published June 19, 2008. LeBoeuf is prior art under at least §102(b).
- U.S. 2010/0012715 (“Williams”) published January 21, 2010. Williams is prior art under at least §102(b).
- U.S. 8,823,494 (“Kovitz”) was filed on November 9, 2010, and issued September 2, 2014. Kovitz is prior art under at least §102(e).
- U.S. 2011/0081860 (“Brown”) was filed on October 2, 2009, and

¹ Apple does not concede that the '123 patent is entitled to this priority date.

published April 7, 2011. Brown is prior art under at least §102(a).

- WO 2010/144626 (“Weiss”) published on December 16, 2010. Weiss is prior art under at least §102(a).
- U.S. 2012/0198531 (“Ort”) was filed January 31, 2011, and published August 2, 2012. Ort is prior art under at least §102(a) and (e).

Each of these references is analogous to the claims of the ’123 patent. The ’123 patent claims are in the field of endeavor of establishing wireless communications links between devices to facilitate the communication of information between the devices. EX1001, 39:30-67; EX1003, ¶38. Bishop, Brown, Williams, Kovitz, and Ort are in this field of endeavor because they disclose techniques for establishing wireless communications links between devices. *See, e.g.*, EX1004, ¶6; EX1006, ¶49; EX1009, ¶¶41-43; EX1021, Abstract; EX1008, ¶¶4-6; EX1003, ¶¶69-71, 174, 182, 187-88, 268. LeBoeuf and Weiss are in this field of endeavor because they disclose devices that communicate data over wireless communications links. EX1005, ¶¶101-02; EX1007, 2:8-11, 8:11-14; EX1003, ¶¶72-76, 189.

Moreover, the ’123 patent claims are directed to the problem of how to efficiently and intuitively establish wireless communications between devices for communicating data using those links. EX1001, 39:30-67. Bishop, Brown, Williams, Kovitz, and Ort are reasonably pertinent to this problem because they

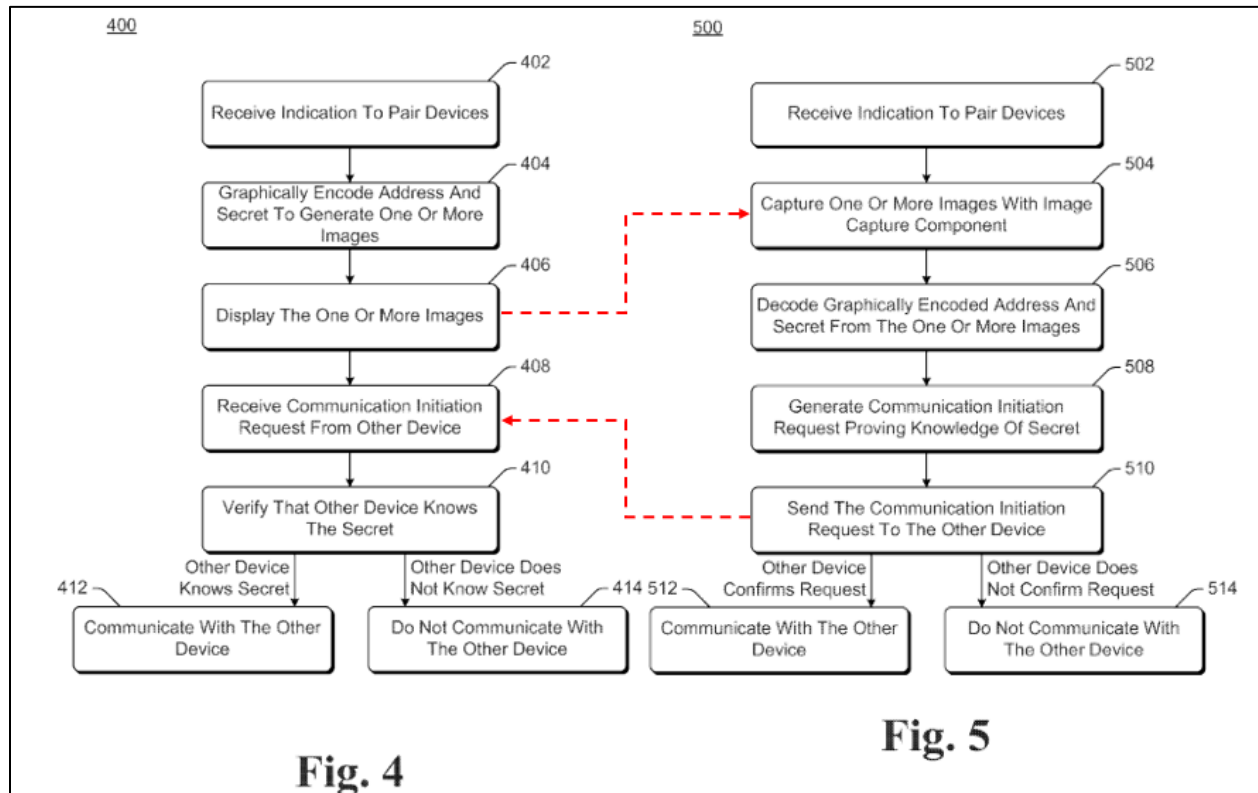
disclose techniques for establishing wireless communications links between devices using digital scannable media (e.g., barcodes). *See, e.g.*, EX1004, ¶6; EX1006, ¶49; EX1009, ¶¶41-43; EX1021, Abstract; EX1008, ¶¶4-6; EX1003, ¶¶69-71, 174, 182, 187-88, 268. LeBoeuf and Weiss are reasonably pertinent to this problem because they disclose devices that communicate data over wireless communications links. EX1005, ¶¶101-02; EX1007, 2:8-11, 8:11-14; EX1003, ¶¶72-76, 189.

V. GROUND 1: BISHOP IN VIEW OF LEBOEUF RENDERS OBVIOUS CLAIMS 1-5, 7-15, AND 17-20.

A. Bishop

Bishop teaches a technique in which “two devices can be easily paired by a user.” EX1004, ¶57; EX1003, ¶¶69-71. Specifically, a first device graphically encodes “an address of a first device” (e.g., IP address) and a secret in an image, and “displays the image of the graphically encoded address and secret.” EX1004, ¶¶12, 57. The second device “captures” the image, “decodes the address and secret,” and “sends a communication initiation request to the first device using the decoded address.” EX1004, ¶12. “If the second device is verified as having knowledge of the secret, then the first and second devices proceed to communicate with one another; otherwise, the first and second devices do not proceed to communicate with one another.” EX1004, ¶12. This process is shown in Figure 4 (from the perspective of the first device) and Figure 5 (from the perspective of the

second device). EX1004, ¶¶59, 67.



EX1004, Figs. 4-5 (annotated).

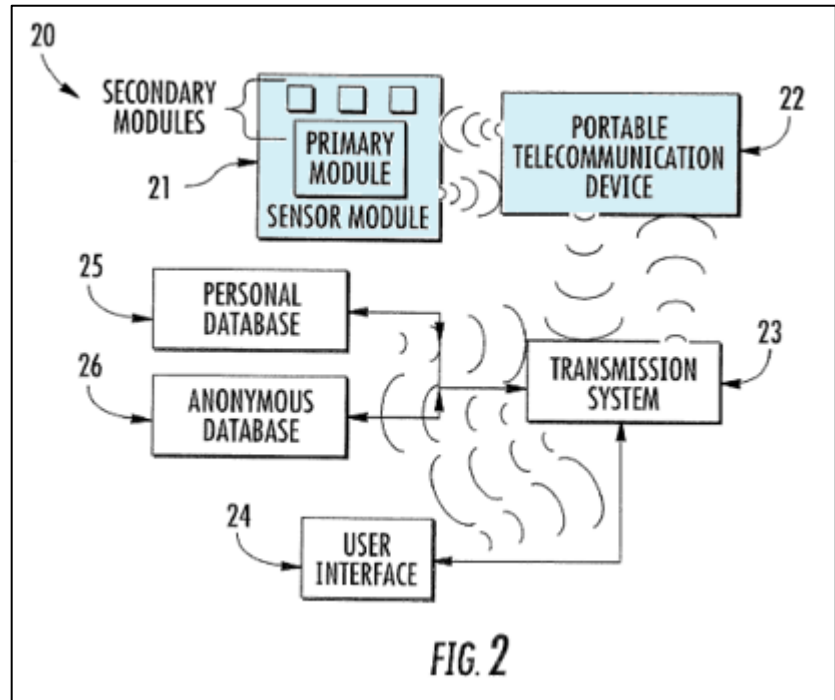
B. LeBoeuf

LeBoeuf teaches techniques for “monitoring various physiological and environmental factors.” EX1005, Abstract; EX1003, ¶¶72-76. It discloses a “wearable monitoring device”² that implements “at least one physiological sensor 11.” EX1005, ¶79. Using these sensors, the wearable monitoring device “monitor[s] the physiological functioning of the body, such as, but not limited to...

² LeBoeuf uses the terms “wearable monitoring device” and “sensor module” interchangeably. EX1005, ¶99.

heart rate, pulse rate, breathing rate, blood flow, heartbeat signatures,” etc.

EX1005, ¶80.



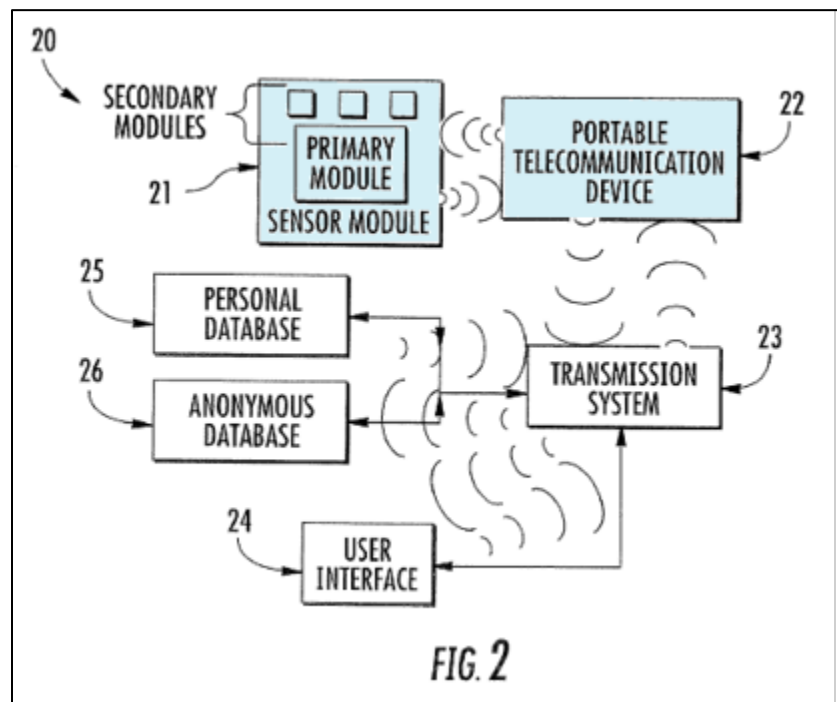
EX1005, Fig. 2 (annotated).

The wearable monitoring device is also configured to “communicate[] wirelessly with the portable telecommunication device 22, preferably in an open architecture configuration, such as Bluetooth® or ZigBee.” EX1005, ¶101. For instance, the wearable monitoring device wirelessly transmits information obtained using the physiological sensors to the portable telecommunications device so that this information can be displayed in “an end-user graphical interface” of the device. EX1005, ¶102.

C. Motivation to Combine

A POSA would have found it obvious to combine Bishop and LeBoeuf to

arrive at the claims of the '123 patent. EX1003, ¶77. As explained above, LeBoeuf's wearable monitoring device "communicates wirelessly with the portable telecommunication device 22, preferably in an open architecture configuration, such as Bluetooth®." EX1005, ¶101, *see also* ¶5, 58, 148. However, LeBoeuf does not teach how to establish such wireless connection (e.g., Bluetooth link) between these devices.



EX1005, Fig. 2 (annotated).

A POSA would have sought to provide an intuitive, user-friendly process for wirelessly connecting the devices. EX1003, ¶78. This would have led a POSA to Bishop, which teaches a technique in which "two devices can be easily paired by a user." EX1004, ¶57; EX1003, ¶79. Bishop sought to improve upon conventional pairing processes, which were "cumbersome." EX1004, ¶¶1, 57. Bishop describes

a technique in which “two devices can be easily paired” using “graphically encoded data” such as a barcode that stores information to establish communications between the two devices. EX1004, ¶57.

A POSA would have found it obvious to adapt LeBoeuf’s devices to establish a wireless communication link using Bishop’s pairing technique. EX1003, ¶80. Bishop provides express motivation, explaining that its technique avoids the “cumbersome processes for configuring the devices to be able to communicate” found in conventional pairing processes. EX1004, ¶57. Such conventional processes could be “time consuming and cumbersome,” and lacked “user friendliness.” EX1004, ¶1. Bishop’s process, by contrast, is performed “without the need for any additional input by the user,” and thus does not require users to make “numerous settings or other configuration changes” to the devices. EX1004, ¶¶1, 57. A POSA would have thus been motivated to implement Bishop’s technique in LeBoeuf to provide an efficient, user-friendly process for “easily pair[ing]” devices. EX1004, ¶57; EX1003, ¶¶80-81.

Bishop’s technique also provides strong security via its “shared secret.” EX1004, ¶40. Namely, Bishop includes a “secret” in the graphically encoded data and requires the second device to “prove it has knowledge of the secret” before the communication link is established. EX1004, ¶¶40, 45, 56. This ensures that “the device from which the communication initiation request is received is indeed a

device to which the graphically encoded secret was displayed.” EX1004, ¶¶40, 56.

Bishop’s process thus enables users to ensure that the devices being paired are the correct devices, and not malicious actors. EX1003, ¶82.

A POSA would have thus been further motivated to combine Bishop and LeBoeuf to implement a *secure* pairing process. Security is particularly important because LeBoeuf’s wearable monitoring device collects “personal and private [] information” regarding user health. EX1005, ¶17. A POSA would have recognized the importance of a secure pairing process in LeBoeuf to prevent malicious actors from obtaining such information. EX1003, ¶83.

A POSA would have had a reasonable expectation of success in making this combination. EX1003, ¶87. Bishop’s techniques are “platform-independent,” and “can be implemented on a variety of commercial computing platforms,” even on “low-resource device[s] with limited memory and/or processing resources.” EX1004, ¶¶15, 81. Bishop’s technique also applies to “various usage scenarios,” and can be implemented “[a]nywhere communication between two devices is desired.” EX1004, ¶58. In other words, Bishop’s techniques were designed and advertised to improve devices like LeBoeuf’s.

Indeed, LeBoeuf’s wearable monitoring device can take a “variety of form factors,” including a “wrist-watch,” and the portable telecommunication device, can be “any portable device, such as a cell phone (which includes a ‘smartphone’),

PDA, laptop computer, Blackberry,” etc. EX1005, ¶¶101, 141. Moreover, LeBoeuf’s data is transferrable over a wireless communication link. EX1005, ¶102. It was within a POSA’s skill to implement Bishop’s techniques in LeBoeuf’s devices. EX1003, ¶¶84-96.

For instance, it was within a POSA’s skill to adapt LeBoeuf’s devices to implement Bishop’s hardware and software components to the extent necessary to implement Bishop’s device pairing process. *Id.* For instance, a POSA would have readily been able to implement Bishop’s device pairing modules, display screen, processing devices, memory devices, or other suitable components in LeBoeuf’s devices. *Id.* This would amount to, at most, a simple substitution of known electronic components in conventional manners to achieve predictable results. *See id.*; EX1004, ¶¶73-76, Fig. 6.

For instance, LeBoeuf’s wearable monitoring device includes a “visual monitor” display. EX1005, ¶105. It was within a POSA’s skill to implement Bishop’s graphical-pairing approach using LeBoeuf’s visual monitor—doing so would have required routine software development. EX1003, ¶¶86, 95. To the extent any hardware modifications were required, these would be achieved using simple substitutions of known electronic components (Bishop’s screen, or any other like it) in an existing application (LeBoeuf’s device). *Id.*; EX1004, ¶¶23, 30.

These adaptations would have been straight forward and readily

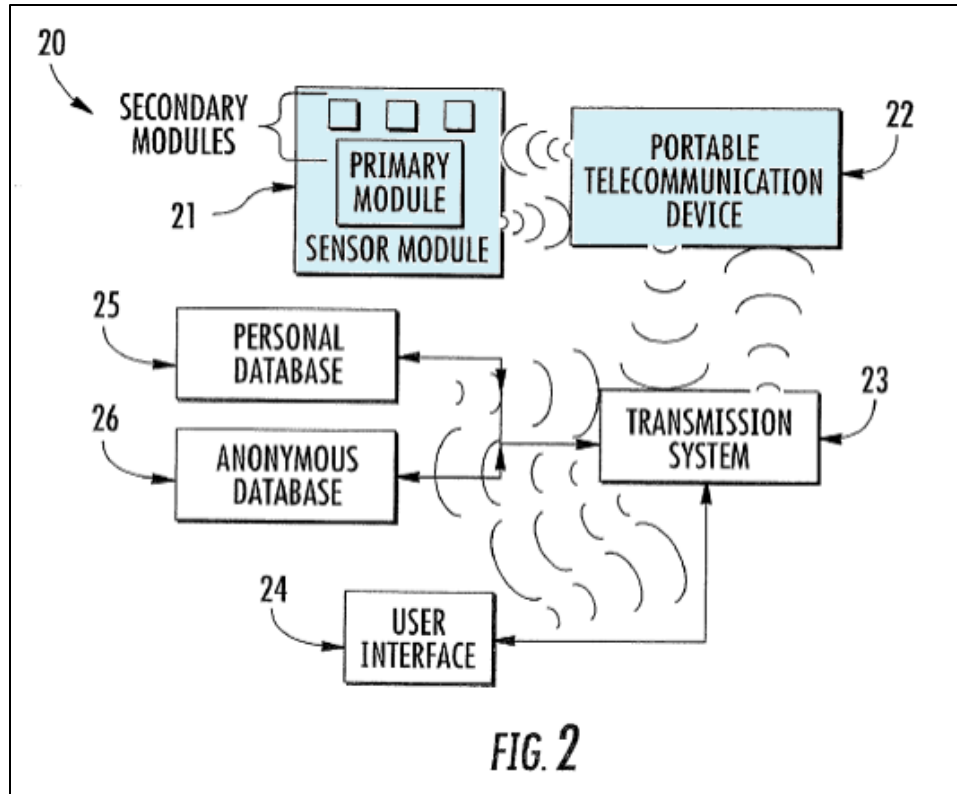
implementable by a POSA. EX1003, ¶96. Indeed, as explained, Bishop’s technique “supports various usage scenarios,” and can be implemented even by “low-resource device[s].” EX1004, ¶¶15, 58. In view of this, a POSA would have recognized that the combination of Bishop and LeBoeuf would merely amount to the use of Bishop’s known technique (encoding and displaying wireless pairing information in barcodes) to improve LeBeouf’s similar devices in the same way (to efficiently and securely establish wireless communications). EX1003, ¶96.

D. Independent Claims

1. Claim 1

a. [1.P] A wearable activity device, wherein the wearable activity device is comprised of:

LeBoeuf teaches a wearable monitoring device/sensor module. *See* EX1005, ¶101; EX1003, ¶97. The wearable monitoring device is a *wearable activity device* as claimed because it is “worn by” the user, includes “at least one physiological sensor 11” and “at least one environmental sensor 12,” and is configured to measure “basic vital signs” of the user, such as “breathing rate, pulse rate, and the like.” EX1005, ¶¶14, 79, 97, Figs. 1-2, 8; EX1003, ¶97. The wearable monitoring device is also configured “to track the caloric intake, health, and physical activity of dieters,” and “to monitor the diet, physical activity, health, and environment of athletes.” EX1005, ¶110, *see also* ¶112.



EX1005, Fig. 2 (annotated).

As explained below, the wearable monitoring device/sensor module taught by the combination of Bishop and LeBoeuf discloses the componentry and functionality of the claimed *wearable activity device*. EX1003, ¶98.

b. [1.1] a display device;

LeBoeuf's wearable monitoring device includes a "visual monitor" for displaying a user interface. EX1005, ¶105. Bishop's device 102 includes a screen 112 (*display device*) for displaying graphically encoded data. See EX1004, ¶¶20, 23, 30. In the combined system, LeBoeuf's monitoring device would be adapted to implement hardware (e.g., a display) and software disclosed by Bishop to generate and display graphically encoded data to establish wireless communications

between itself and a mobile device. *See* Section V.C *supra*. Thus, the combination of Bishop and LeBoeuf teaches this element. EX1003, ¶99.

- c. **[1.2] at least one of an accelerometer configured to track activity and an embedded bio-metric monitoring sensor configured to detect a bio-metric characteristic;**

LeBoeuf's wearable monitoring device includes "one or more accelerometers" that are used to *track activity*. EX1005, ¶120; EX1003, ¶100. For instance, the *accelerometers* are configured to "measur[e] body motion in real-time," "gage the distance a person has traveled," and to measure "[c]aloric intake, physical activity, [] metabolism," "the number of steps walked during a day," etc. EX1005, ¶¶120, 157, 159, 163, 170.

Leboeuf's wearable monitoring device also includes *an embedded bio-metric monitoring sensor*, such as "physiological sensor[s] 11... for monitoring the physiological functioning of the body" (*detecting bio-metric characteristics*³). EX1005, ¶¶79-80; EX1003, ¶101. These sensors include, for instance, sensors for monitoring and detecting "heart rate, pulse rate," "blood pressure," "glucose," "body fat density," etc. EX1005, ¶¶80, 151, *see also* ¶81.

³ The '123 patent specification provides examples of "biometric" characteristics, such as "body weight, body fat %, etc" and "fingerprint, heart rate, DNA, etc." EX1001, 6:65-7:5, 21:58-64.

- d. [1.3] wireless communication circuitry, wherein the wireless communication circuitry is configured to establish a wireless communications link with a mobile device;**

LeBoeuf's wearable monitoring device includes "telemetric modules" (*wireless communication circuitry*), such as a Bluetooth module comprising a "Bluetooth chip." EX1005, ¶148, Fig. 8; EX1003, ¶103. Using such telemetric modules, the wearable monitoring device "communicates wirelessly with the portable telecommunication device 22" (*mobile device*). EX1005, ¶101. To do so, the telemetric module establishes a *wireless communications link* with the portable telecommunications device, "preferably in an open architecture configuration, such as Bluetooth®." EX1005, ¶101, *see also* ¶58; EX1003, ¶104.

Moreover, Bishop's device 102 includes a "device pairing module 120" that "manages... the pairing of or initiation of communication between devices." EX1004, ¶24. The device pairing module is implemented as combination of software and "hardware (e.g., fixed logic circuitry)." EX1004, ¶¶19, 59, 81. The device also includes a "network card" and "communications... modules for wirelessly sending data to and/or receiving data from other devices." EX1004, ¶¶17-18, 77.

The combined *wearable activity device* thus comprises *communication circuitry* as claimed. EX1003, ¶105.

- e. **[1.4] at least one processor with software, wherein the processor is associated with a memory device and wherein the at least one processor is in signal communication with the display device and the wireless communication circuitry;**

As explained in Section V.C, the Bishop-LeBoeuf system adapts LeBoeuf's wearable monitoring device to implement Bishop's device pairing technique. In the combined system, the wearable monitoring device comprises *at least one processor with software*. EX1003, ¶106. For instance, LeBoeuf's wearable monitoring device comprises a "microprocessor[]" for implementing the functionality of the device. EX1005, ¶¶59, 87. Bishop's mobile device 102 further comprises "one or more processors or processing units 602" that execute "software" comprising instructions for implementing Bishop's disclosures, such as the process 400 of Figure 4. EX1004, ¶¶59, 73-74, 76. For instance, the software is implemented by modules 114-120. EX1004, ¶19.

The processor(s) of the adapted wearable monitoring device are *associated with a memory device* in the form of "one or more computer readable media 604 that can include one or more memory and/or storage components 606." EX1004, ¶74, *see also* ¶¶76, 81; EX1003, ¶107. The processor(s) are further *in signal communication with the display device* because they cause the display device to "output[] a user interface for display," and to display images depicting graphically encoded data. EX1004, ¶¶22, 27, *see also* ¶19; EX1003, ¶108. The processor(s) are

further *in signal communication with the wireless communication circuitry* because they cause the wireless communication circuitry to communicate with Bishop's mobile device 104. EX1004, ¶44; EX1005, ¶101; EX1003, ¶¶108-09.

- f. [1.5] the memory device associated with the at least one processor, wherein the memory device is configured to store wireless pairing information associated with the wireless communication circuitry;**

LeBoeuf's wearable monitoring device includes a "storage component," such as "any solid-state storage device, such as flash memory, random-access memory (RAM), magnetic storage, or the like." EX1005, ¶113. Moreover, as described above, Bishop's mobile device 102 includes "memory and/or storage components 606" that store "one or more instructions that are executed by one or more processors or controllers of [the] device." EX1004, ¶¶19, 74-76, 81. Bishop's memory further *stores wireless pairing information associated with the wireless communication circuitry*. EX1003, ¶110. For instance, mobile device 102 includes "a setting or configuration store" that stores "an address of device 102" (*wireless pairing information*). EX1004, ¶¶23-24. A POSA would have understood that this setting or configuration store is implemented via the *memory device* that stores data. EX1003, ¶110.

The address comprises *wireless pairing information associated with the wireless communication circuitry* because it is used to "pair[] devices 102 and 104" so that they are "able to communicate with one another." EX1004, ¶18;

EX1003, ¶111. The address “identifies device 102 on communication network 108,” and enables “other devices on network 108 [to] send messages to device 102.” EX1004, ¶18. For instance, the address is “an IP (Internet Protocol) address,” or other address depending “on the protocol used by communication network 108,” which is used to carry out device pairing. EX1004, ¶¶23-24. The address is *associated with the wireless communication circuitry* because it enables the device 102 to establish network communications via the *wireless communication circuitry*. EX1003, ¶112. That is, the address is “used to initiate communication between devices 102 and 104” using the wireless communication circuitry. EX1004, ¶23, *see also* ¶17.

As explained in Section V.C, in the Bishop-LeBoeuf system, the combined wearable monitoring device is configured to establish a wireless communications link with the mobile device, such as LeBoeuf’s Bluetooth link. EX1005, ¶¶101-02. The wearable device stores *wireless pairing information* (address) associated with its *wireless communications circuitry* that is used to initiate the pairing process. EX1003, ¶¶113-15. As Dr. Shenoy explains, a POSA would have understood, or at least found it obvious, that such implementation would use a Bluetooth or MAC address as the address used for pairing, consistent with Bluetooth’s pairing procedures. *See id.*; EX1004, ¶¶18, 24. This address is *associated with the wireless communication circuitry* because it is assigned to the Bluetooth chip and used to

establish the wireless communication link. *Id.*

- g. [1.6] wherein the processor software is configured to; obtain, from the memory device, the wireless pairing information associated with the wireless communication circuitry,**

As explained for element [1.4], Bishop's device 102 includes one or more processing units 602 that execute "one or more instructions" (*processor software*), which are configured to implement the wireless pairing process. EX1004, ¶19. To implement this process, the device's *processor software* obtains "an address of device 120" (*wireless pairing information*) from "a setting or configuration store" (*memory*) of device 102. EX1004, ¶24; *see also* discussion for element [1.5]. As explained in Section V.C, in the Bishop-LeBoeuf system, the wearable monitoring device would be configured to initiate the wireless pairing process and would thus be configured to obtain the *wireless pairing information* from memory. EX1003, ¶¶117-18.

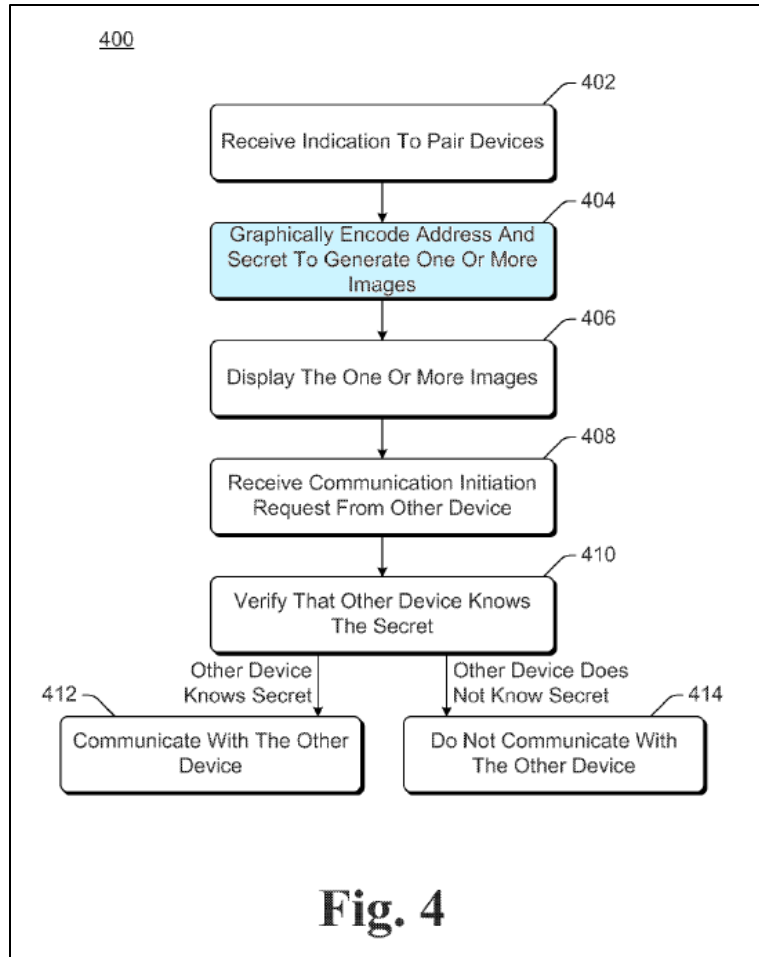
- h. [1.7] generate a color coded digital scannable media responsive to the wireless pairing information;**

Bishop's device 102's *processor software* generates "graphically encoded data" that is displayed on the screen of device 102. EX1004, ¶¶16, 19, 22-23; EX1003, ¶121. The graphically encoded data is a "high capacity color barcode (HCCB)," which as Dr. Shenoy explains, is a *color coded digital scannable media* as claimed because it encodes data via different colors, such that the colors

themselves encode data. EX1003, ¶119. As Dr. Shenoy further explains, HCCBs were well-known and commercialized prior to 2011. EX1004, ¶¶23, 30; EX1003, ¶¶44-54, 119.

In Bishop, the HCCB is generated *responsive to the wireless pairing information* because it “encodes the obtained address” (*wireless pairing information*) that is used to pair the devices. EX1004, ¶27; EX1003, ¶120. In particular, Bishop’s “[d]evice pairing module 120 provides both the obtained address of device 102 and [a] secret⁴ to graphical encoding module 118,” which “in turn, graphically encodes the obtained address and secret to generate one or more images.” EX1004, ¶27, *see also* ¶19.

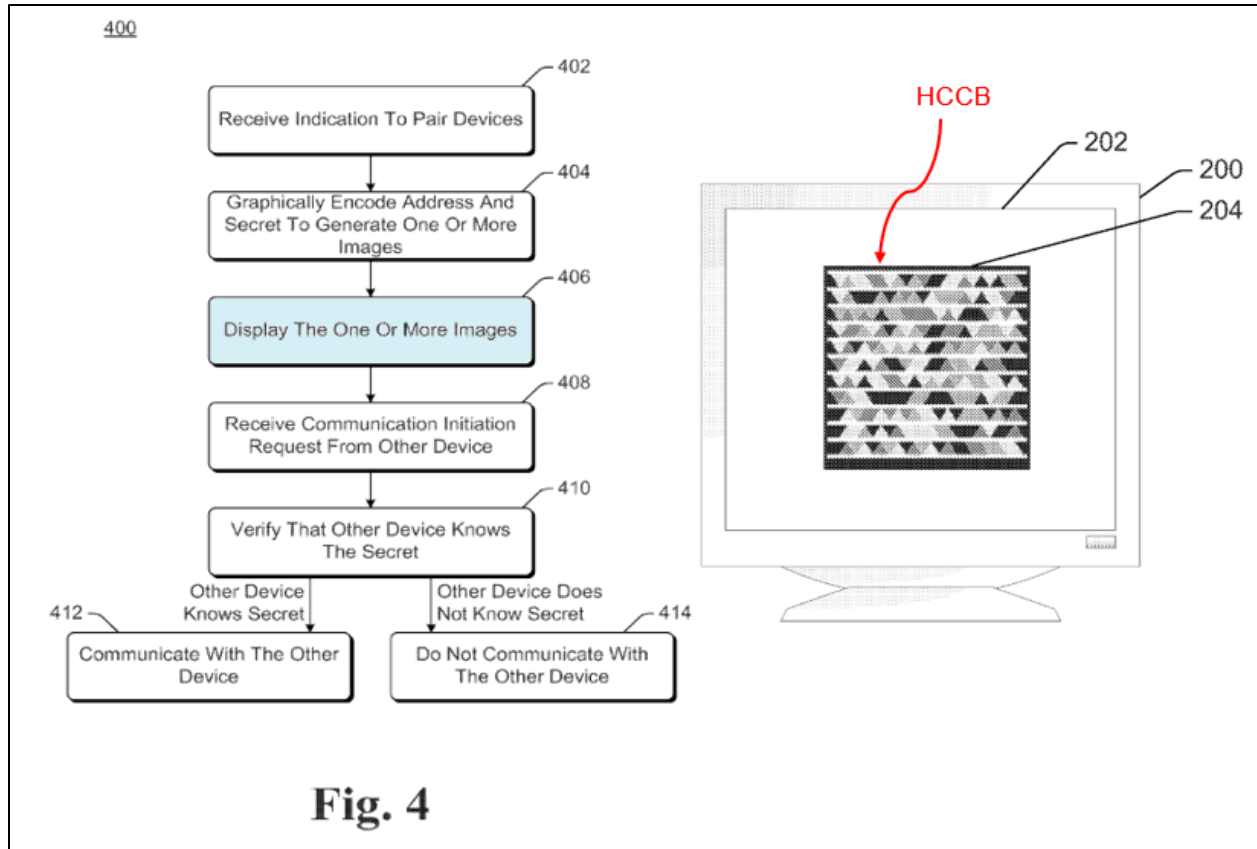
⁴ Petitioner does not rely on the secret as the claimed *wireless pairing information*.



EX1004, Fig. 4 (annotated).

- i. **[1.8] control the display device, wherein the display device is configured to display the color coded digital scannable media,**

Bishop's device 102's *processor software* "display[s]" the HCCB image (*color coded digital scannable media*) "on screen 112." EX1004, ¶27, *see also* ¶¶19, 30. The software thus *controls* the screen 112 (*display device*) to display the *color coded digital scannable media*. EX1004, ¶29 (the image is displayed "in response to a variety of different events or actions"); EX1003, ¶¶122-23.



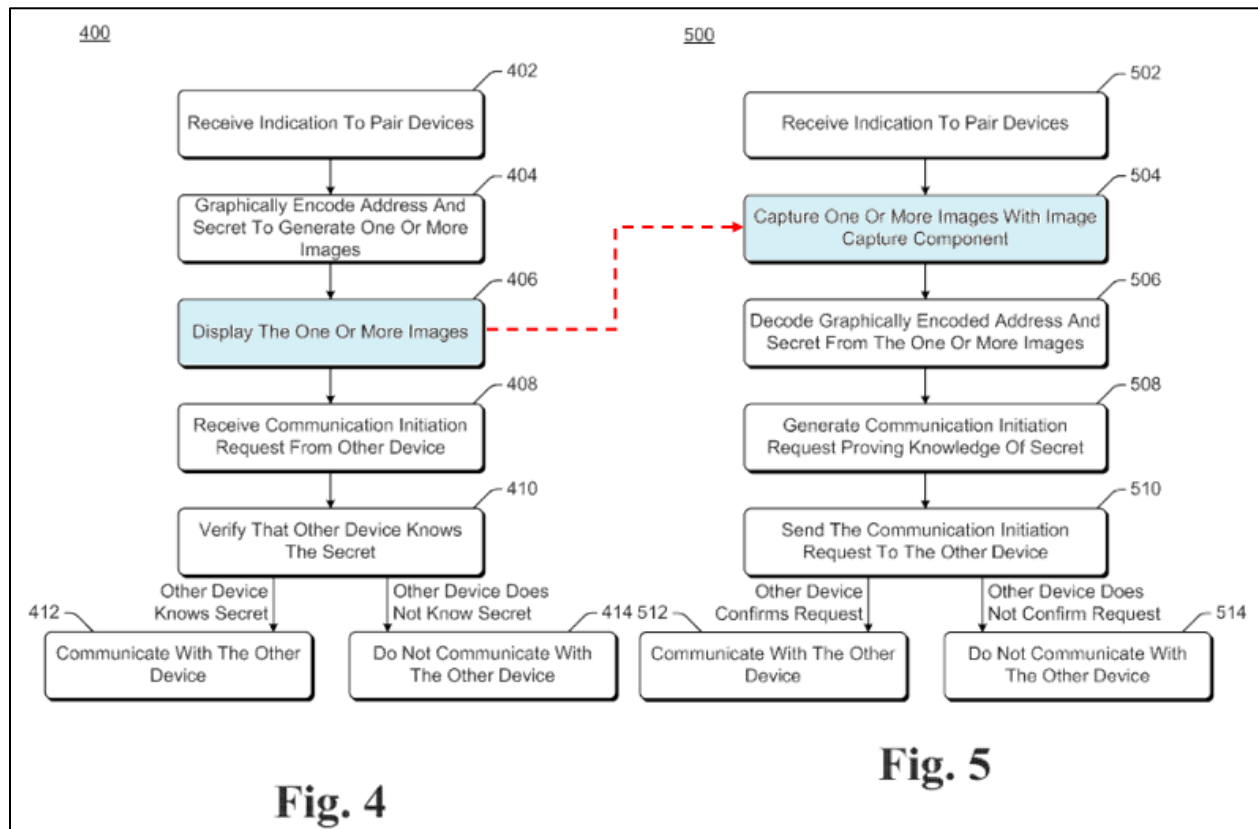
EX1004, Figs. 4 and 2 (annotated).

- j. [1.9] establish, via the wireless communication circuitry, the wireless communications link with the mobile device responsive to the mobile device scanning and decoding the color coded displayed digital scannable media,

Bishop's device 102's *processor software* uses the HCCB (*color coded digital scannable media*) to establish a wireless communications link with a second device, such as mobile device 104 (*mobile device*). See EX1004, ¶19. This occurs responsive to the mobile device scanning and decoding the HCCB. EX1003, ¶¶124-25.

In particular, when the device 102 displays the HCCB image on its screen

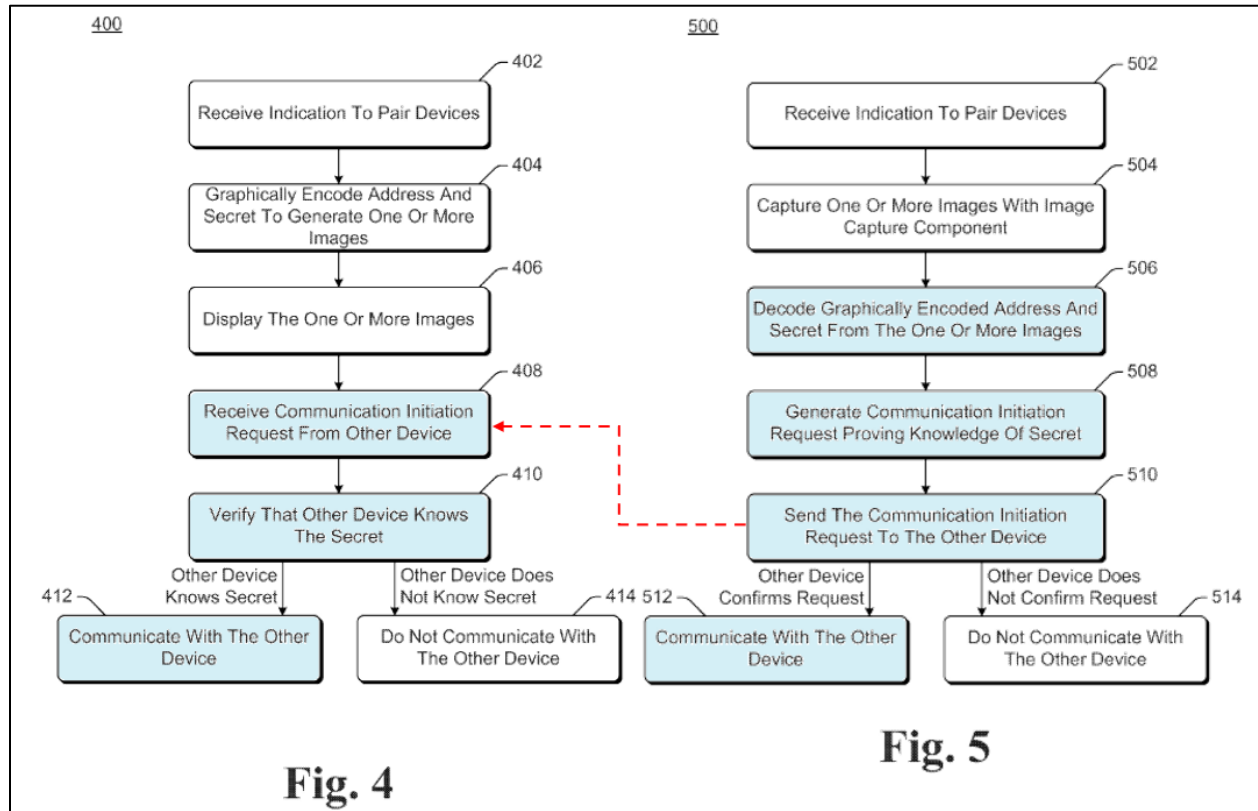
112, the mobile device 104 captures (*scans*) the displayed image using an “image capture component.” EX1004, ¶¶16, 23, 39. The image capture component *scans* the image using a “digital camera” implemented, for instance, using “CCD (charge coupled device) technology, CMOS (complementary metal oxide semiconductor) technology, and so forth.” EX1004, ¶33.



EX1004, Figs. 4, 5 (annotated).

The mobile device 104 then “decodes the data encoded in the image[]” (i.e., in the HCCB) (*color coded displayed digital scannable media*), and “generates a communication initiation request that targets (e.g., is addressed to) device 102” (i.e., using the address obtained from the decoded data). EX1004, ¶¶37, 39, 40, *see also* ¶70. Upon verifying the communication initiation request, the device 102

“proceed[s] with communicating with device 104.” EX1004, ¶¶43-44. At this point, the devices are “paired.” EX1004, ¶57.



EX1004, Figs. 4, 5 (annotated).

This process is thus “used to initiate communication between devices 102 and 104” (*establish the wireless communications link*). EX1004, ¶23; EX1003, ¶¶125-127. Indeed, the device 102 receives a “communication initiation request” from device 104 to “pair” devices 102 and 104. EX1004, ¶¶18, 44, 76. Once the devices are “paired together,” they are “able to communicate with one another” via communications network 108. EX1004, ¶18. For instance, the devices use the *wireless communications link* to “wirelessly send[] data to and/or receiv[e] data from” one another. EX1004, ¶17, *see also* ¶¶44, 58, 80.

The *wireless communications link* is established via at least device pairing module 120 and communications modules (*via the wireless communication circuitry*) of the device 102. *See* EX1004, ¶¶17, 24; EX1003, ¶¶128-29. It is also established using the HCCB data scanned and decoded by the device 104 (*responsive to the mobile device scanning and decoding the color coded displayed digital scannable media*). EX1004, ¶¶63-64; EX1003, ¶¶128-29.

As explained in Section V.C, in the combined Bishop-LeBoeuf system, the wearable monitoring device (acting as device 102 in Bishop's pairing process) would be paired with the *mobile device*. As described, the mobile device would capture and decode an image of the graphically encoded data (HCCB) displayed by the wearable monitoring device. The wearable monitoring device would then receive a communication initiation request from the mobile device to establish the wireless connection between the devices, via its *processor software*. *See* EX1004, ¶19. The wireless communication link would be, for instance, a Bluetooth link, as taught by LeBoeuf. EX1005, ¶¶101-02. Thus, the combination of Bishop and LeBoeuf teaches this element. EX1003, ¶130.

k. [1.10] generate at least one of activity tracking information and bio-metric information,

The combination of Bishop and LeBoeuf teaches this element. EX1003, ¶131.

LeBoeuf's wearable monitoring device/sensor module generates sensor data

“relating [to] health and environment, as well as real-time biofeedback and the like.” EX1005, ¶102, *see also* ¶¶5, 87, 129, 137. This generated sensor data includes *activity tracking information and bio-metric information*. For instance, the wearable monitoring device includes “physiological sensor[s] 11... for monitoring the physiological functioning of the body, such as, but not limited to, sensors for monitoring: heart rate, pulse rate, breathing rate, blood flow, heartbeat signatures,” etc. EX1005, ¶¶79-80. The physiological sensors thus collect, process, and transmit such data related to “basic vital signs” (*activity tracking information and bio-metric information*). EX1005, ¶97; EX1003, ¶131.

The physiological sensors are also configured to generate additional *activity tracking information* such as, for instance, “physical activity, caloric intake... physical and/or psychological stress levels and/or stress level indicators... physical exertion... sleep patterns, hunger and/or thirst,” etc. EX1005, ¶6, *see also* ¶163. For instance, the monitoring device includes “accelerometers” that “measur[e] body motion in real-time,” and “gauge the distance a person has traveled.” EX1005, ¶¶120, 170. The monitoring device also includes “a variety of other body motion sensors, such as acoustic sensors” or “MEMS motion sensors” to “monitor footsteps.” EX1005, ¶120, *see also* ¶159.

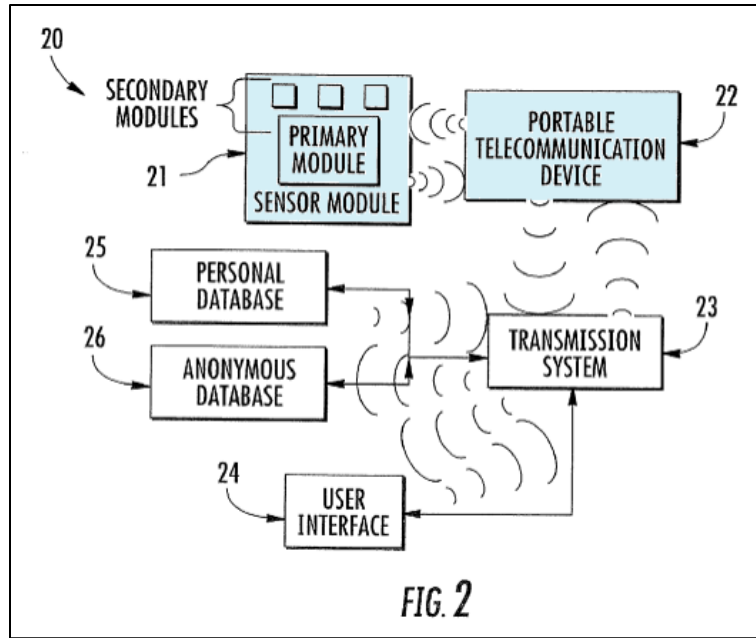
The *activity tracking information and bio-metric information* is generated using “various algorithms” (*processor software*) for “extraction of physiological

and/or environmental information from the various environmental and/or physiological sensors.” EX1005, ¶117, *see also* ¶¶113, 129. In the combined Bishop-LeBoeuf system, such algorithms would be implemented by the *processor software* taught by the combination of Bishop and LeBoeuf. *See* EX1004, ¶¶19, 59, 81; EX1003, ¶¶132-33.

I. [1.11] communicate, via the wireless communications link, at least one of the activity tracking information and the bio-metric information to the mobile device.

The combination of Bishop and LeBoeuf teaches this element. EX1003, ¶135.

LeBoeuf’s wearable monitoring device/sensor module (*wearable activity device*) “communicates wirelessly with the portable telecommunication device 22” (*mobile device*), “preferably in an open architecture configuration, such as Bluetooth® or ZigBee” (*via a wireless communications link*) EX1005, ¶101; EX1003, ¶¶136-137. In LeBoeuf, the wearable monitoring device communicates, to the portable telecommunication device, sensor data “relating [to] health and environment, as well as real-time biofeedback and the like.” EX1005, ¶102, *see also* ¶¶5 (“Health and environmental information, sensed by the sensors is transmitted wirelessly, in real-time, to a recording device, capable of processing and organizing the data into meaningful displays”), 87, 129, 137.



EX1005, Fig. 2 (annotated).

As explained for element [1.10], this transmitted sensor data includes *activity tracking information and bio-metric information* generated by the wearable monitoring device, such as “basic vital signs” and “physical activity, caloric intake... physical and/or psychological stress levels and/or stress level indicators... physical exertion... sleep patterns, hunger and/or thirst,” etc. EX1005, ¶¶6, 97, *see also* ¶163; EX1003, ¶137.

As explained in Section V.C, in the Bishop-LeBoeuf system, the wearable monitoring device’s *processor software* would generate such information and wirelessly transmit it to the mobile device over the *wireless communications link* established using Bishop’s communication initiation procedures. This is consistent with Bishop’s teaching that, once communication is established between devices 102 and 104, the devices can “transfer data (e.g., a report, song, or other data from

one device to another)” and “control information, and so forth to one another.”

EX1004, ¶¶44, 58. The device 102’s *processor software* communicates this information *via the wireless communication link* established using Bishop’s process. *See* EX1004, ¶¶19, 59, 81. Thus, the combination of Bishop and LeBoeuf teaches this element. EX1003, ¶¶135-138.

2. Claim 11

- a. **[11.P] A method for establishing a communications link between a wearable activity device and a mobile device, the method comprising:**

The combination of Bishop and LeBoeuf teaches this element. EX1003, ¶139. As explained in Section V.C, and for claim 1, Bishop teaches a *method for establishing a communications link between two mobile devices*. EX1004, ¶12. LeBoeuf teaches a method in which a wearable monitoring device (*wearable activity device*) communicates wirelessly with a portable telecommunication device (*mobile device*). EX1005, ¶¶101. In the combined system, Bishop’s wireless communication link establishment technique is used to establish the wireless communications link between the wearable monitoring device a mobile device, as taught by the combination of Bishop and LeBoeuf. EX1003, ¶139.

- b. **[11.1] storing, by a memory device associated with the wearable activity device, wireless pairing information associated with wireless communication circuitry disposed within the wearable activity device,**

The combination of Bishop and LeBoeuf teaches this element for the reasons

provided for element [1.5]. EX1003, ¶140. For instance, Bishop-LeBoeuf's wearable monitoring device stores "an address of device 102" (*wireless pairing information associated with wireless communication circuitry*) in "a setting or configuration store" (implemented via a *memory device*). *E.g.*, EX1004, ¶¶17-18, 23-24.

- c. **[11.2] receiving, by a processor associated with the wearable activity device, the wireless pairing information associated with the wireless communication circuitry from the memory device,**

The combination of Bishop and LeBoeuf teaches this element for the reasons provided for element [1.6]. EX1003, ¶141. For instance, Bishop-LeBoeuf's wearable monitoring device's *processor* receives or obtains the "address of device 102" (*wireless pairing information*) from the setting or configuration store (*memory device*). *See, e.g.*, EX1004, ¶¶19, 24.

- d. **[11.3] generating, by the processor associated with the wearable activity device, a color coded digital scannable media responsive to the wireless pairing information,**

The combination of Bishop and LeBoeuf teaches this element for the reasons provided for element [1.7]. EX1003, ¶142. For instance, Bishop-LeBoeuf's wearable monitoring device's *processor* generates an image of an HCCB (*color coded digital scannable media*) that encodes the address of device 102 (*wireless pairing information*). *See e.g.*, EX1004, ¶¶19, 23, 27.

- e. **[11.4] displaying, by a display device associated with the wearable activity device, the color coded digital scannable media,**

The combination of Bishop and LeBoeuf teaches this element for the reasons provided for element [1.8]. EX1003, ¶143. For instance, Bishop-LeBoeuf's wearable monitoring device displays the HCCB (*color coded digital scannable media*) image on screen 112. *See, e.g.*, EX1004, ¶¶23, 27.

- f. **[11.5] scanning, by the mobile device, the color coded digital scannable media,**

The combination of Bishop and LeBoeuf teaches this element for the reasons provided for element [1.9]. EX1003, ¶144. For instance, Bishop-LeBoeuf's mobile device captures (*scans*) the HCCB (*color coded digital scannable media*) image using an image capture component (*e.g.*, digital camera). *See, e.g.*, EX1004, ¶¶33-36, 69.

- g. **[11.6] processing, by the mobile device, the color coded digital scannable media, and**

The combination of Bishop and LeBoeuf teaches this element for the reasons provided for element [1.9]. EX1003, ¶145. For instance, Bishop-LeBoeuf's mobile device *processes* the HCCB (*color coded digital scannable media*), such as by analyzing and decoding the HCCB depicted in the image. *See, e.g.*, EX1004, ¶¶37-39, 70.

- h. [11.7] establishing, by the mobile device, a wireless communications link with the wearable activity device responsive to the mobile device processing the color coded digital scannable media,**

The combination of Bishop and LeBoeuf teaches this element for the reasons provided for element [1.9]. EX1003, ¶146. For instance, Bishop-LeBoeuf's mobile device generates and sends a "communication initiation request" to the wearable monitoring device *responsive to* decoding the graphically encoded data in the HCCB. *See, e.g.*, EX1004, ¶¶40-42, 70-71. The devices then complete the pairing process and "proceed to communicate with one another." *See, e.g.*, EX1004, ¶¶12, 18, 44.

- i. [11.8] generating, by the wearable activity device processor, at least one of activity information and bio-metric information, wherein the at least one of the activity information and bio-metric information is stored in the memory device associated with the wearable activity device, and**

The combination of Bishop and LeBoeuf teaches this element for the reasons provided for elements [1.10]-[1.11]. EX1003, ¶147. For instance, Bishop-LeBoeuf's wearable monitoring device's *processor* generates *activity information* and *bio-metric information* such as "basic vital signs" and "physical activity, caloric intake... physical and/or psychological stress levels and/or stress level indicators... physical exertion... sleep patterns, hunger and/or thirst," etc. *See, e.g.*, EX1005, ¶¶6, 97, *see also* ¶163.

Moreover, this *activity information* and *bio-metric information* is stored in *the memory device associated with* the wearable monitoring device. EX1003, ¶148.

For instance, the wearable monitoring device “store[s]” “data” relating to a “subject’s health and environment.” EX1005, ¶111. The wearable monitoring device includes a “data storage component,” such as “any solid-state storage device, such as flash memory, random access memory (RAM), magnetic storage, or the like,” that “allows processed signal data to be stored, analyzed, and manipulated to provide new knowledge to the user.” EX1005, ¶113.

- j. **[11.9] communicating, via the wireless communications link by the wearable activity device, at least one of the activity tracking information and the bio-metric information to the mobile device.**

The combination of Bishop and LeBoeuf teaches this element for the reasons provided for element [1.11]. EX1003, ¶150. For instance, Bishop-LeBoeuf’s wearable monitoring device communicates, to the portable telecommunications device (*mobile device*), sensor data, such as “basic vital signs,” “physical activity, caloric intake... physical and/or psychological stress levels and/or stress level indicators... physical exertion... sleep patterns, hunger and/or thirst,” etc. EX1005, ¶¶6, 97, *see also* ¶¶102, 163. This data is communicated over the *wireless communications link* established using Bishop’s pairing technique.

E. Dependent Claims

1. Claims 2 and 12

LeBoeuf's wearable monitoring device is a *wearable health monitoring device* because it is a "health and environmental monitor[]" "worn by" the user and is configured to measure "basic vital signs" of the user, such as "breathing rate, pulse rate, and the like." EX1005, ¶¶4, 79, 97, 138; EX1003, ¶152; *see also* discussion for element [1.P] *supra*. The wearable monitoring device can be implemented as a "wrist-watch." EX1005, ¶141. In such configuration, the wearable monitoring device is also a *smartwatch* because it includes a "signal processor" for determining user vital signs, and a "transmitter/receiver 14" for establishing wireless connections with other devices. EX1005, ¶¶79, 83, 87-88; EX1003, ¶152.

2. Claims 3 and 13

Bishop-LeBoeuf's communication circuitry is configured to establish a wireless connection between the wearable monitoring device and the portable telecommunication device, for instance, over a Bluetooth or ZigBee network, which, as Dr. Shenoy explains, are personal area networks EX1003, ¶¶154-55; *see also* EX1009, ¶40.

3. Claims 4 and 14

Bishop's device 104 can be a "cellular or other wireless phone," which as Dr. Shenoy explains, comprise smartphones. EX1004, ¶15; EX1003, ¶¶157-58.

LeBoeuf's portable telecommunication device can be a "cell phone (which includes a 'smartphone')." EX1005, ¶101. Thus, the combination of Bishop and LeBoeuf teaches a mobile device that is a smartphone device. EX1003, ¶158.

4. Claims 5 and 15

Bishop-LeBoeuf's *wireless pairing information* includes "an address" of the wearable monitoring device, such as an IP address or other network address depending on the network protocol used. EX1004, ¶24. The address comprises *an identification identifier/number associated with the* wearable monitoring device because it "identifies [the device] on communication network 108," and enables "devices on network 108 [to] send messages to [the device]." EX1004, ¶¶18 ("an address of device 102"), 23-24; EX1003, ¶160.

Moreover, as explained for element [1.5], the pairing process is used to establish LeBoeuf's Bluetooth connection. In such implementation, the "address" would be a Bluetooth address, which, as Dr. Shenoy explains, is a type of MAC address. EX1003, ¶161; *see* EX1005, ¶40.

5. Claims 7 and 17

During prosecution, the originally filed claims recited "information associated with the wireless communication circuitry." EX1002, 87. The Applicant then amended the independent claims to recite "wireless pairing information associated with the wireless communication circuitry." EX1002, 147. The

Applicant concurrently amended claims 7 and 17 to recite “the wireless pairing information further includes... the wireless communication circuitry.” EX1002, 148. A POSA would have thus understood “wireless communication circuitry information” to encompass “wireless pairing information associated with the wireless communication circuitry.” EX1003, ¶164.

As explained for claims 5 and 15, Bishop-LeBoeuf’s wireless pairing information comprises “an address” of the wearable monitoring device (*wireless communication circuitry information*). EX1004, ¶¶23-24. It also includes “additional location information regarding” the wearable monitoring device (*wearable activity device information*). EX1004, ¶27, *see also* ¶¶18, 24. The combination of Bishop and LeBoeuf thus teaches *wireless pairing information* that comprises a combination of *wireless communication circuitry information* and *wearable activity device information*. EX1003, ¶165.

6. Claims 8 and 18

As explained for claims 7 and 17, Bishop’s *wireless pairing information* includes “location information regarding” the wearable monitoring device. EX1004, ¶27, *see also* ¶¶18, 24. A POSA would have understood that this location information comprises a *facility location identifier associated with the physical location of the* Bishop-LeBoeuf wearable monitoring device, such as a street address or GPS coordinates. EX1003, ¶167. For instance, as Dr. Shenoy explains,

such location is *associated with the physical location* of the device because the location is used to “determine how to communicate with” it. EX1004, ¶24; EX1003, ¶167. Moreover, Bishop’s pairing process requires line of sight communications (e.g., via the image capture), the location information encoded in the HCCB thus indicates that the wearable monitoring device is located in proximity to the mobile device. EX1003, ¶168. Such information is associated with a facility, for instance, in which the wearable monitoring device is located (e.g., an address or coordinates of a facility). *Id.*

Moreover, LeBoeuf’s wearable monitoring device determines and communicates “physical location” and “proximity to various locations or properties.” EX1005, ¶104, *see also* ¶¶86 (disclosing proximity detection by the wearable monitoring device), 138 (wearable monitoring device includes “location sensors”). It also communicates “personal information” and “biometric identification” of users (*user ID information*), as well as “exercise monitoring” data (*workout performance data*). EX1005, ¶¶82, 104, 163.

A POSA would have found it obvious to implement such information in the combined Bishop-LeBoeuf *wearable activity device information* to establish a *wireless communications link*. EX1003, ¶169. As Bishop discloses device location information as wireless pairing information, a POSA would have found it obvious to additionally or alternatively implement LeBoeuf’s similar location information

as wireless pairing information, as merely a simple substitution of known elements to achieve predictable results. *Id.* Implementing such additional information as part of the *wearable activity device information* was well within the skill of a POSA.

Id.

7. Claims 9 and 19

Bishop’s graphically encoded data is stored in a HCCB (*color coded digital scannable media*), which, as Dr. Shenoy explains, is a *2D matrix code* and a *representation of non-human readable information using colored pixels*. EX1004, ¶23. EX1003, ¶171.

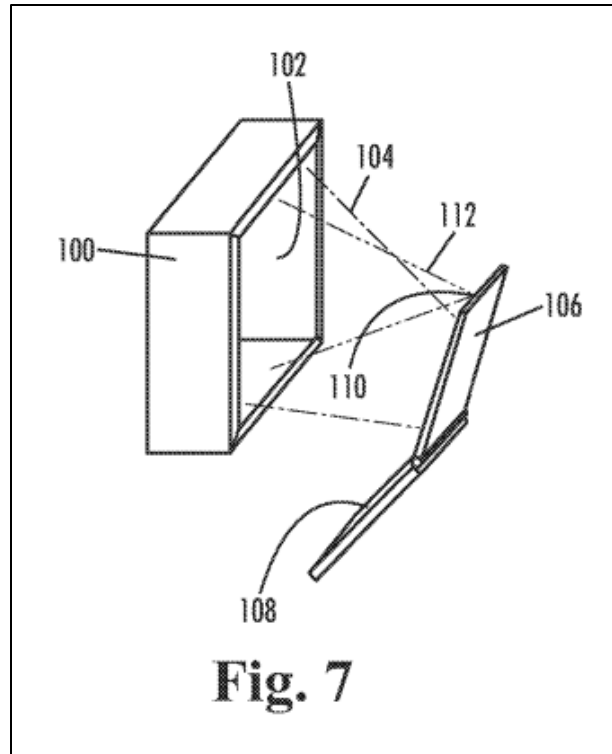
8. Claims 10 and 20

As explained in element [1.1], Bishop-LeBoeuf’s wearable monitoring device includes a *display device*, as taught by the combination of Bishop and LeBoeuf, that displays “graphically encoded data” (i.e., within an HCCB). *See* EX1004, ¶¶20, 23, 30. Bishop-LeBoeuf’s “[d]evice 102 includes a screen 112,” which “can be implemented in a variety of different manners, such as using liquid crystal display (LCD) technology.” EX1004, ¶¶19-20. Thus, the combination of Bishop and LeBoeuf teaches a display device that is an *LCD display*. EX1003, ¶173.

**VI. GROUND 2: BISHOP-LEBOEUF FURTHER IN VIEW OF
WILLIAMS RENDERS OBVIOUS CLAIMS 6 AND 16.**

1. Williams

Williams teaches a system for “establishing a wireless connection” between devices by “encod[ing] wireless pairing information, for example a device address and PIN number” in a barcode. EX1009, ¶¶5, 26; EX1003, ¶174. “The encoded information is displayed as one or more encrypted or non-encrypted images” of barcodes. EX1009, ¶26. The wireless connection can be a “BLUETOOTH connection.” EX1009, ¶¶37-38. This connection can be established using a “pairing process after which the mobile device and the mobile module can securely communicate with each other.” EX1009, ¶41. For instance, a “mobile module” can initiate a “pairing request” by generating and displaying an “optical image” encoding the wireless pairing information. EX1009, ¶42. The encoded pairing information includes “the device address associated with the initiating device” and “a PIN code associated with the device address.” EX1009, ¶42. The address is a “unique BLUETOOTH device address.” EX1009, ¶45. A handheld device captures the image and “decodes and processes the pairing message.” EX1009, ¶43. The devices then establish the wireless connection in accordance with, for instance, the Bluetooth protocol. EX1009, ¶45.



EX1009, Fig. 7.

2. Claims 6 and 16

As explained above, Williams teaches that its wireless pairing information is “encrypted” using various “encryption method[s].” EX1009, ¶¶26-29. This results in an “encrypted image containing the” wireless pairing information. EX1009, ¶28. A POSA would have found it obvious to implement Williams’s encryption techniques in Bishop-LeBoeuf to provide increased security of the device pairing process. EX1003, ¶¶177-79.

As explained in Section V.C, LeBoeuf’s monitoring device transmits “personal and private” health information over the wireless communication link. EX1005, ¶17. A POSA would have sought to improve security of the device pairing process to better ensure that malicious actors cannot pair with LeBoeuf’s

device to obtain this information. *See* EX1004, ¶¶45; EX1003, ¶177. Indeed, encrypting the data encoded in Bishop’s barcode would ensure that only parties with the relevant encryption key would be able to decipher the pairing data and pair with the device (and thus obtain access to the private information).

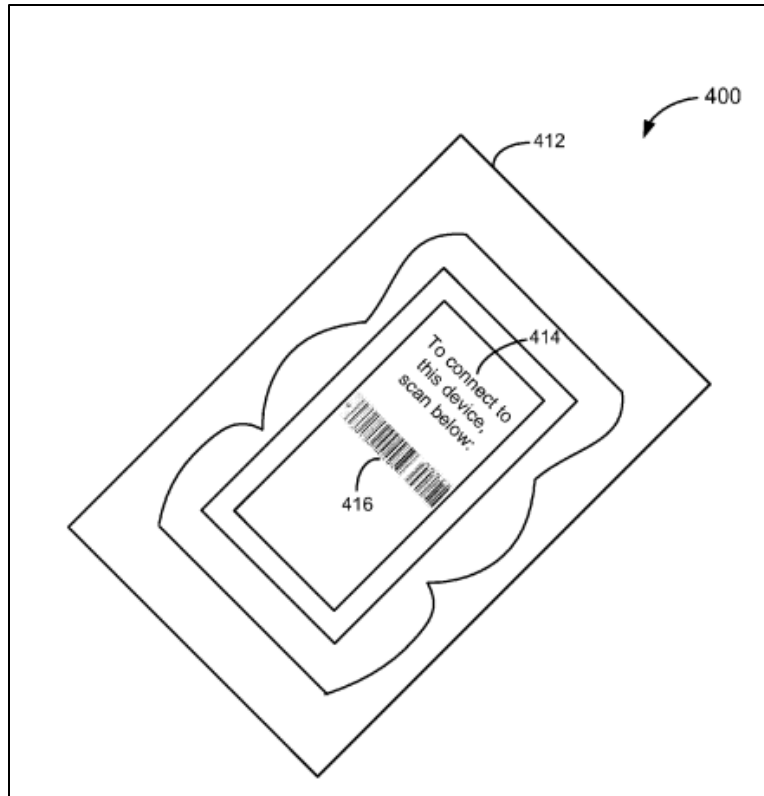
Indeed, as Dr. Shenoy explains, encryption was a well-known technique for implementing secure communications. EX1003, ¶¶177-78. As Dr. Shenoy also explains, it was well known to encrypt information encoded in barcodes. *Id.* A POSA would have thus found it obvious to encrypt Bishop-LeBoeuf’s graphically encoded data and would have had a reasonable expectation of success in doing so. EX1003, ¶179. Indeed, encryption was commonly performed to secure data and a POSA would have readily understood how to implement Williams’s encryption techniques. *Id.* For instance, a POSA would have readily understood how to implement and communicate suitable keys for encrypting and decrypting the data in accordance with well-established and conventional techniques. *Id.*; *see also*, *e.g.*, EX1009, ¶¶9, 43. This would have been obvious as merely requiring the use of a known technique (encrypted barcode images) to improve similar processes (wireless pairing processes) in the same way (provide enhanced security). EX1003, ¶179.

VII. GROUND 3: BISHOP-LEBOEUF FURTHER IN VIEW OF KOVITZ RENDERS OBVIOUS CLAIMS 7-8 AND 17-18

As explained in Section V.E.5, Bishop-LeBoeuf’s *wireless pairing*

information includes *wearable activity device information* in the form of “additional location information regarding” the wearable monitoring device (*wearable activity device information*). EX1004, ¶27, *see also* ¶¶18, 24. However, to the extent Bishop does not disclose the wearable activity device information required by claims 7-8 and 17-18, Kovitz does. EX1003, ¶181.

Like Bishop, Kovitz teaches techniques for “wireless device connection and pairing” using barcodes. EX1021, Abstract; EX1003, ¶182. “To facilitate connection or pairing, a first device may optically acquire or capture the printed or displayed [barcode]... in order to initiate an automatic connection or pairing process with one or more other devices.” EX1021, 3:54-59. “For example, a scanner or camera associated with a laptop computer may optically acquire a barcode in order to initiate automatic Bluetooth pairing between the laptop computer and any number of other Bluetooth devices, such as peripherals.” EX1021, 3:59-63. The barcodes encode connection parameters including “network addresses.” EX1021, 6:50-58, 12:9-15. The barcodes also encode software “applications supported or required by a device” (*device software information*) and “usage requirements, power requirements, current battery levels” of the device (*device utilization information*). EX1021, 11:40-45, 12:36-13:14. This *device software information* and *device utilization information* are types of *wearable activity device information*. EX1003, ¶182.



EX1021, Fig. 4.

A POSA would have found it obvious to implement Kovitz's *device software information* and *device utilization information* in Bishop-LeBoeuf's *wireless pairing information*. EX1003, ¶183. Kovitz teaches that encoding specific application identifiers in the pairing data would inform the pairing device of particular "applications supported or required by a device," such as "software or code [] necessary to enable or configure communication with the device." EX1021, 12:36-51. This would enable the pairing device to determine if it "has all required applications installed," and if not, to download such applications. EX1021, 12:56-13:14. As another example, including the *utilization information* in the pairing data would enable the devices to "negotiate" a suitable protocol to use based on this

information, as taught by Kovitz. EX1021, 16:13-17:11; EX1003, ¶183; *see also* EX1004, ¶24.

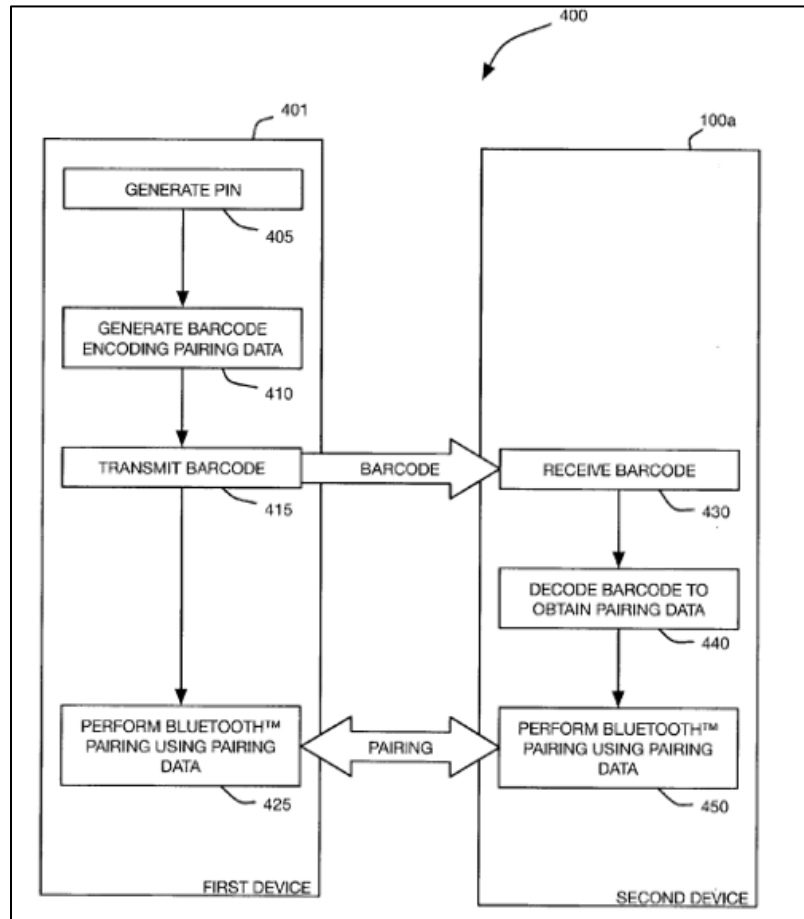
A POSA would have sought to implement these features in Bishop-LeBoeuf to enhance the pairing process, and to tailor it to the specific requirements of the devices being paired. EX1003, ¶185. As Bishop already teaches a wireless pairing process using barcodes, a POSA would have readily been able to implement Kovitz’s techniques in Bishop-LeBoeuf, such that the wearable monitoring device encoded software and utilization information in its *wireless pairing information*. *Id.* Indeed, a POSA would have recognized that this would merely amount to the use of a known technique (encoding device utilization and software information in barcodes) to improve similar devices in the same way (an enhanced pairing process that accounts for device requirements or capabilities). *Id.*

VIII. GROUND 4A: BROWN IN VIEW OF WEISS RENDERS OBVIOUS CLAIMS 1-5, 9-15, AND 19-20

A. Brown

Brown teaches techniques for “performing Bluetooth pairing between a first device and a second device.” EX1006, Abstract; EX1003, ¶¶187-188. For instance, a first device “encodes Bluetooth pairing data... in a barcode.” EX1006, ¶75. The pairing data includes a “personal identification number (PIN) code” and “the network address of the first device (e.g., MAC address).” EX1006, ¶¶71, 75. The first device “display[s] the image on [its] display,” and a second device

“capture[s]” the image, “extracts the barcode,” and “decodes [it] to obtain the Bluetooth pairing data.” EX1006, ¶¶79, 83-84. The second device then “transmits Bluetooth pairing data... to first device 401,” and the devices “carr[y] out Bluetooth pairing in known manner.” EX1006, ¶¶80, 85.

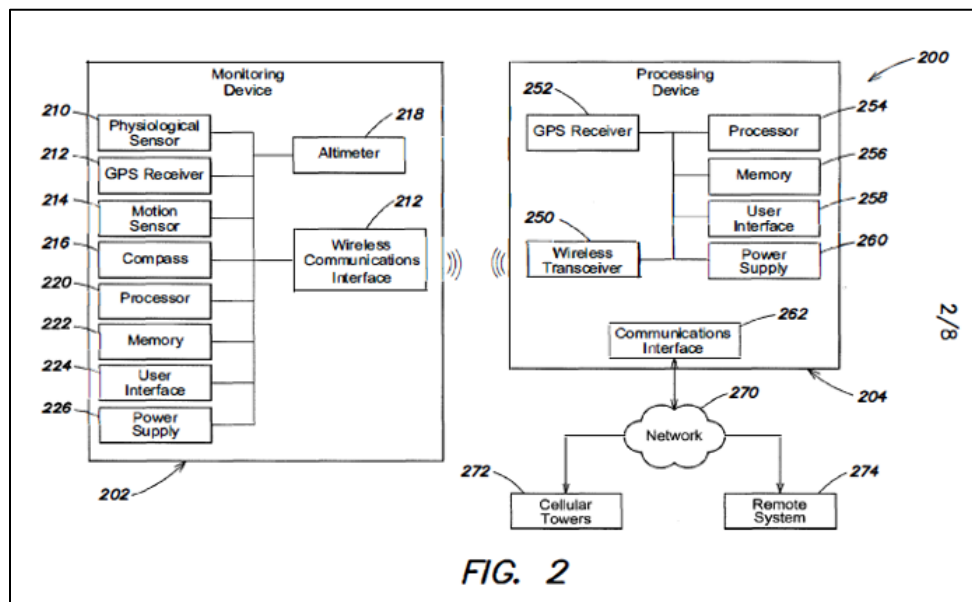


EX1006, Fig. 4.

B. Weiss

Weiss discloses a system for “monitoring one or more physiological conditions” that includes a “personal monitoring device” that is “designed to be easily wearable and include[s]... a plurality of sensors for detecting one or more physiological attributes” of a user. EX1007, 1:23-28, 2:11-15; EX1003, ¶¶189. The

monitoring device communicates such physiological attributes to a “processing device,” for instance, “using the Bluetooth™ open wireless standard.” EX1007, 2:8-11. The processing device is a “smartphone” configured to “process data received from the monitoring device [] and detect at least one event based on a... physiological condition, or combination of physiological conditions, of the user.” EX1007, 8:11-14. The processing device is also configured to “generat[e] and/or display[] reports such as charts, tables, figures, data plots versus time or other parameters, summaries” relating to the “data communicated by the monitoring device.” EX1007, 17:28-18:4.

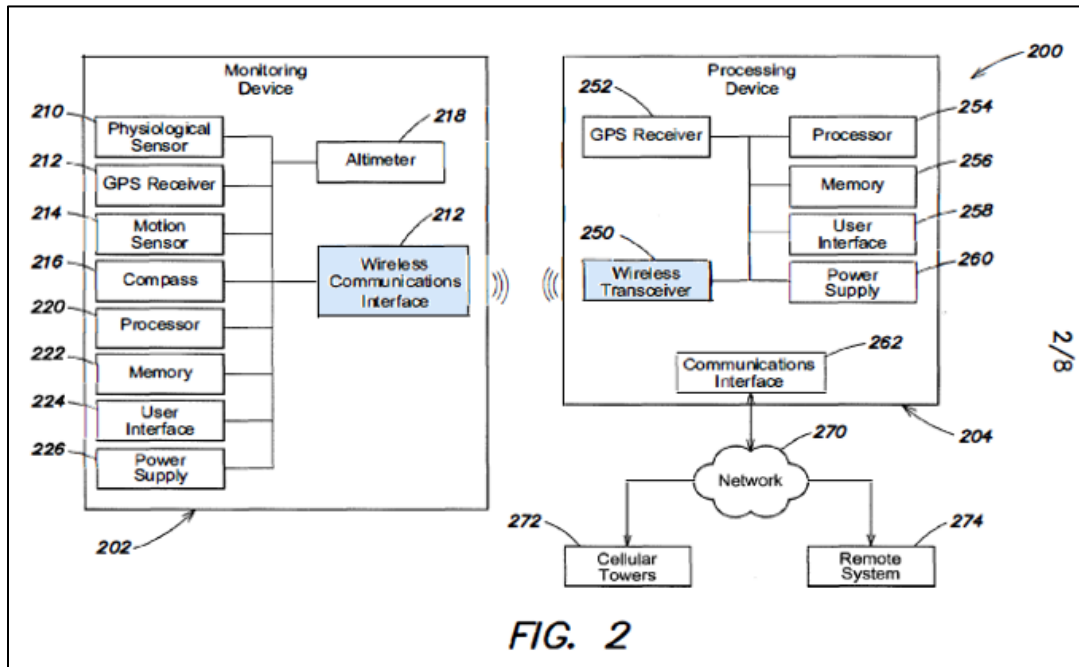


EX1007, Fig. 2.

C. Motivation to Combine

A POSA would have found it obvious to combine Brown and Weiss to arrive at the claims of the '123 patent. EX1003, ¶190. As explained above, Weiss's

monitoring device is configured to “transmit[] data acquired from one or more [sensors] to the processing device” over a Bluetooth communication link. EX1007, 2:8:11, 7:30-8:2. However, Weiss does not teach how to establish this Bluetooth link between these devices.



EX1007, Fig. 2 (annotated).

A POSA would have sought to minimize the difficulties in establishing a Bluetooth connection between Weiss’s devices. EX1003, ¶191. This would have led a POSA to Brown, which teaches techniques for “performing Bluetooth pairing between a first device and a second device.” EX1003, ¶192; EX1006, Abstract. Brown sought to improve upon conventional Bluetooth pairing techniques, which provided low “security” and/or could only be implemented by devices with “significant processing capability.” EX1006, ¶44. To address this, Brown describes

a technique in which Bluetooth pairing is performed by encoding Bluetooth pairing data in a barcode. EX1006, Abstract, ¶39.

A POSA would have found it obvious to adapt Weiss's monitoring and processing devices to implement Brown's Bluetooth pairing technique. EX1003, ¶193. Brown provides express motivation, explaining that its technique "simplif[ies] the discovery and pairing process," and can be "employed in devices with limited processing power and input capability." EX1006, ¶¶46-47. Brown's technique also "make[s] it more difficult for an attacker" to snoop on the pairing process. EX1006, ¶46. This avoids the need to rely on "public key cryptographic techniques," which require increased processing power. EX1006, ¶44; EX1003, ¶¶193-94.

A POSA would have thus been motivated to implement Brown's technique in Weiss. EX1003, ¶194. Weiss's monitoring device is "designed to be easily wearable," and includes "integrated" sensors, thereby allowing for "increased mobility." EX1007, 1:15-20, 2:11-15. For instance, the device may be "integrated into" a "wristwatch" or "arm band." EX1007, 7:24-28. A POSA would have sought to implement Brown's "simplif[ied] and "secure" pairing process in Weiss to provide the user with an efficient and user-friendly pairing process for the wearable device. *See* EX1006, ¶¶38, 44-47; EX1003, ¶195.

A POSA would have had a reasonable expectation of success in combining

the references to arrive at the claims. EX1003, ¶199. Weiss's monitoring and processing devices already communicate using Bluetooth. A POSA would have had no trouble adapting the devices to implement Brown's techniques, which "may be employed in devices with limited processing power and input capability." *Id.*; EX1006, ¶46. Moreover, Weiss's monitoring device can be implemented as a variety of devices, including a "wristwatch," and its portable telecommunication device can be a "smartphone," such as an "iPhone" or "Blackberry." EX1007, 7:24-28, 12:14-19.

It was thus within a POSA's skill to adapt Weiss's devices to implement Brown's hardware and software components to the extent necessary to implement Brown's device pairing process. EX1003, ¶¶196-201. For instance, a POSA would have readily been able to adapt Weiss's devices to implement Brown's "short-range communications subsystem 122," "physical computer-readable storage media," "memory," "display 700," and "processor" or other suitable components for implementing the pairing process. *Id.*; EX1006, ¶¶15, 72, 75, 106. This would amount to, at most, a simple substitution of known electronic components in conventional manners to achieve predictable results. EX1003, ¶198.

For instance, a POSA would have had no trouble adapting Weiss's monitoring device to implement a display that displays graphically encoded data, as taught by Brown. EX1006, ¶¶23, 75, 79; EX1003, ¶200. Nor would a POSA

have had trouble adapting the monitoring device to encode the Bluetooth pairing data in a barcode as taught by Brown. EX1003, ¶200. Indeed, as Dr. Shenoy explains, it was well known for electronic devices, including watches, to generate and display barcodes that encoded information, including information used for establishing wireless communication links between devices. *Id.*

A POSA would have recognized that these adaptations would have been straightforward and would have been implemented without undue burden. EX1003, ¶¶201-202. Indeed, as explained, Brown’s disclosures “may be employed in devices with limited processing power and input capability.” EX1006, ¶46. In view of this, a POSA would have recognized that the combination of Brown and Weiss would merely amount to the use of a known technique (encoding Bluetooth pairing data in barcodes) to improve similar devices (Weiss’s mobile devices) in the same way (to efficiently and securely Bluetooth communications). EX1003, ¶202.

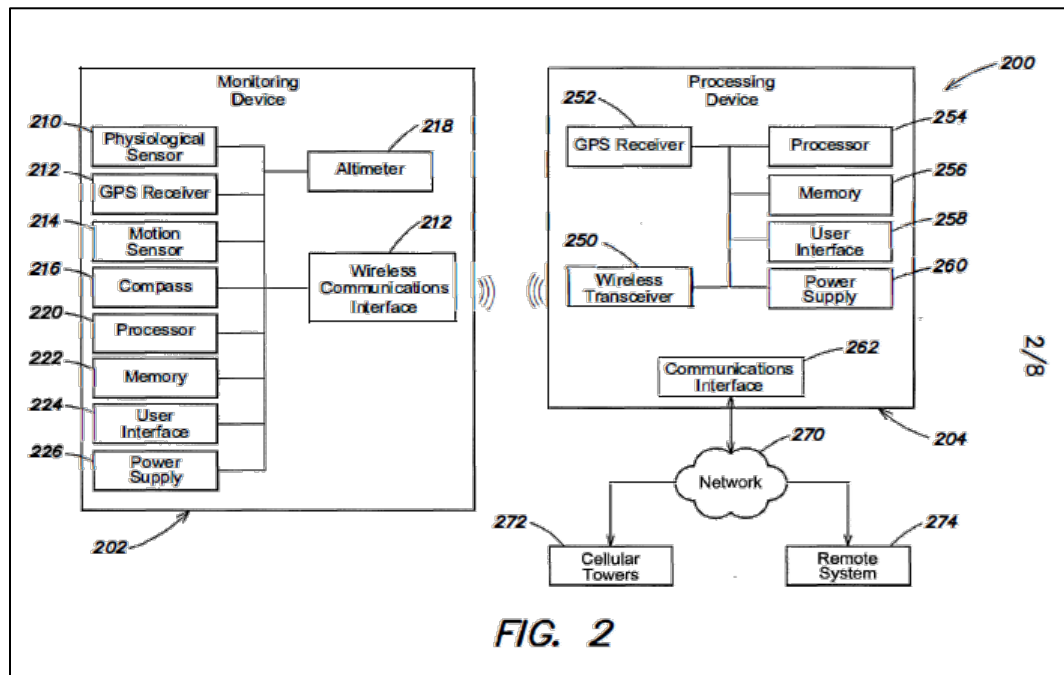
D. Independent Claims

1. Claim 1

a. [1.P]

Weiss teaches a monitoring device that communicates with a processing device. *See* EX1007, 2:8-11. The monitoring device is a *wearable activity device* as claimed because it is “designed to be easily wearable and include one or a plurality of sensors for detecting one or more physiological attributes, including,

but not limited to, pulse, blood oxygen level, temperature, respiration, heart waveform, heart-rate, galvanic skin response, activity, perspiration, body fluid chemistry, and other such detectable attributes.” EX1007, 2:8-15; EX1003, ¶203. For instance, the monitoring device can be “integrated into... a wristwatch.” EX1007, 7:26-29.



EX1007, Fig. 2.

As explained below, the monitoring device taught by the combination of Brown and Weiss discloses the componentry and functionality of the claimed *wearable activity device*. See Section VIII.C *supra*.

b. [1.1]

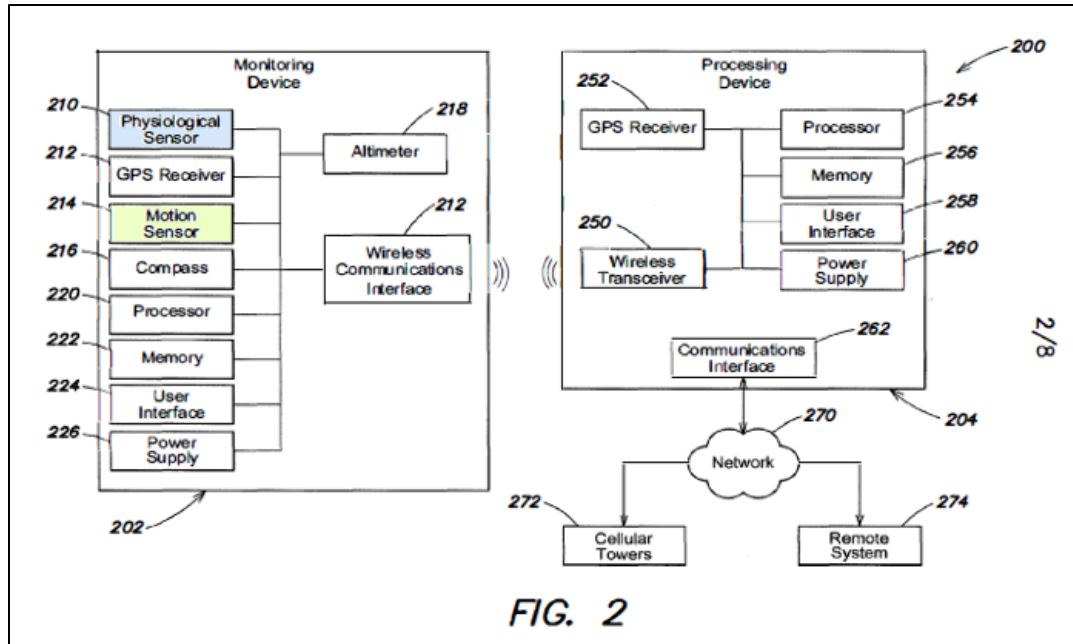
Weiss’s monitoring device includes a “user interface 224.” EX1007, 11:14-16. Brown’s device 401 includes a display, on which it displays a barcode image that encodes Bluetooth pairing data. EX1006, ¶¶37, 75, 79, *see also* ¶16. In the

combined system, to the extent Weiss’s monitoring device’s user interface does not include a display device, it would be adapted to implement such display device, as explained in Section VIII.C. EX1003, ¶205. Thus, the combined Brown-Weiss monitoring device includes a *display device*. *Id.*

c. [1.2]

Weiss’s monitoring device includes “a motion sensor 214 (e.g., accelerometer)” for “detecting the location and motion of an individual wearing the device” (*tracking activity*). EX1007, 11:12-14, *see also* 12:3-9 (monitoring device includes an “accelerometer... for determining rate and/or direction of movement of the user.”); EX!003, ¶206.

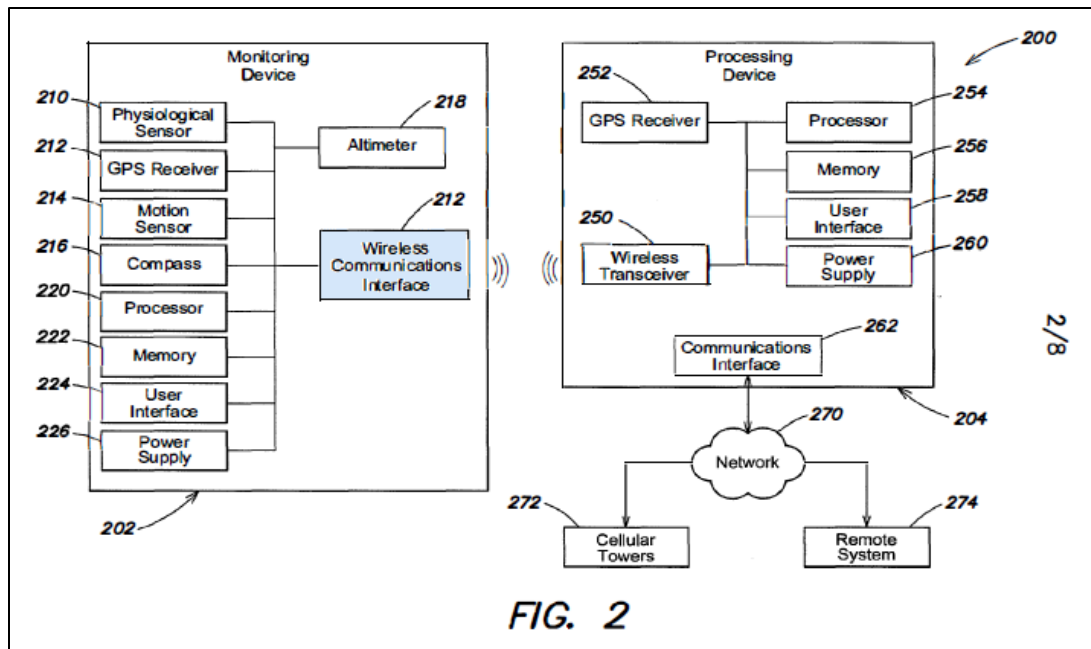
The monitoring device also includes “a plurality of sensors for detecting one or more physiological attributes” (*embedded bio-metric monitoring sensors*). EX1007, 2:11-15, *see also* 1:15-20 (sensors are “integrated into” portable devices), 21:30-22:5. The physiological attributes include *bio-metric characteristics*, such as “pulse, blood oxygen level, temperature, respiration, heart waveform, heart-rate, galvanic skin response, activity, perspiration, body fluid chemistry, and other such detectable attributes.” EX1007, 2:11-15, *see also* 7:21-23, 11:26-29, 21:30-22:5; EX1003, ¶¶206-07.



EX1007, Fig. 2 (annotated).

d. [1.3]

Weiss's monitoring device includes a "wireless communications interface" that is a "Bluetooth™-compatible transmitter." EX1007, 11:10-12, *see also* 7:30-8:2 (monitoring device includes a "wireless transmitter 114, such as a Bluetooth™ transmitter, for transmitting data acquired from one or more of the sensors 112 to the processing device 120."). A POSA would have understood that the wireless communication interface comprises *wireless communication circuitry* to establish wireless communication with the processing device (*mobile device*) using, for instance, the Bluetooth protocol. EX1003, ¶¶208-209.



EX1007, Fig. 2 (annotated).

e. [1.4]

The combination of Brown and Weiss teaches this element. EX1003, ¶210. Weiss’s monitoring device includes a processor 220 that carries out the functionality of the device, and which may be “included in a microcontroller.” EX1007, 11:17-19. The processor is associated with “memory 222,” which “may be, for example, static RAM, dynamic RAM, ROM, EPROM, EEPROM, or flash memory.” EX1007, 11:14-17.

Moreover, as explained in Section VIII.C, the combined Brown-Weiss monitoring device is adapted to implement Brown’s wireless pairing technique. The combined monitoring device includes “software instructions stored on physical computer-readable storage media [*memory device*] and executable by a processor” for implementing the pairing functionality described below. EX1006,

¶106, *see also* ¶¶19, 70. The combined monitoring device thus includes at least one processor with software. EX1003, ¶211. The processor is also *in signal communication with the display device and the wireless communication circuitry*. *See* EX1006, ¶¶15 (“Microprocessor 102 may also interact with...display 110” and “short-range communications subsystem 122”), 49, 57; EX1003, ¶211.

f. [1.5]

The combination of Brown and Weiss teaches this element. EX1003, ¶212. As explained for element [1.4], Weiss’s monitoring device includes “memory” associated with processor 220 and a “wireless communications interface” (*wireless communication circuitry*). EX1007, 11:7-19. Brown’s device 401 also includes “a memory (e.g., random access memory, Flash memory, etc.),” and *wireless communication circuitry* in the form of a short-range communications subsystem, which can be a “Bluetooth communication interface.” EX1006, ¶70, *see also* ¶¶15-16, 22. Brown’s memory is configured to store Bluetooth pairing data that is *associated with* the Bluetooth communication interface. The Bluetooth pairing data includes a “MAC address,” which is *wireless pairing information* as claimed because it is used to pair devices and to establish a wireless communications link in accordance with the Bluetooth protocol.⁵ EX1006, ¶¶40-42, 49, 75; EX1003,

⁵ Brown’s “Bluetooth pairing data” also comprises a “personal identification

¶212. As Dr. Shenoy explains, a POSA would have understood that the MAC address is stored in memory of the device 401 because it is a “unique network address that [was] assigned to [the] device (i.e., when it [was] manufactured).” EX1006, ¶40; EX1003, ¶¶213-14.

g. [1.6]

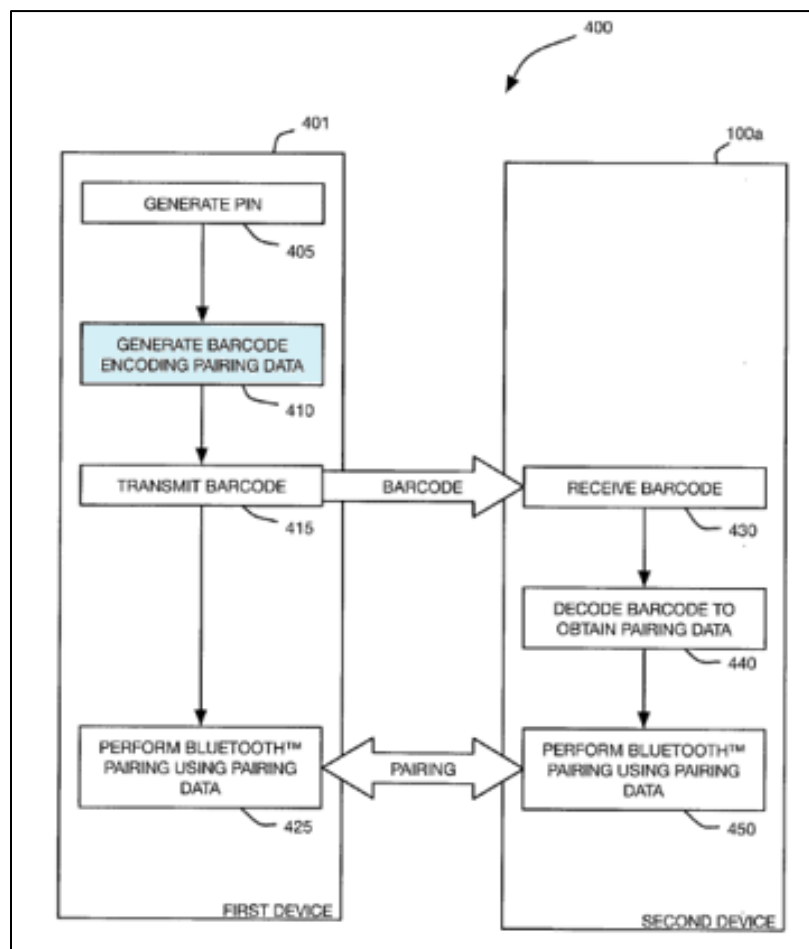
To generate a barcode encoding Bluetooth pairing data, including the MAC address (*wireless pairing information*) and PIN code, Brown’s device 401, via its processor software, “select[s]” (*obtains*) the PIN code that is “stored in memory.” EX1006, ¶72, *see also* ¶75. A POSA would have understood that the device also *obtains* the MAC address from memory because as explained above, it is a “unique network address that [was] assigned to [the] device (i.e., when it [was] manufactured,)” and is thus stored in memory. EX1006, ¶40; EX1003, ¶215.

Brown’s device 401 carries out the device pairing process “by executing an application (e.g. comprising one or more application modules).” EX1006, ¶70. The application is “provided as software instructions stored on physical computer-readable storage media and executable by a processor” (*processor software*). EX1006, ¶106, *see also* ¶57; EX1003, ¶216.

number” (PIN). EX1006, ¶¶41, 75. Petitioner does not rely on the PIN as the claimed *wireless pairing information*.

h. [1.7]

Brown teaches or renders obvious this element. EX1003, ¶217. Brown's device 401's *processor software* "encodes Bluetooth pairing data," including the MAC address (*wireless pairing information*), to generate a "color barcode." EX1006, ¶¶2, 49, 75-76, *see also* ¶¶57, 106. The barcode is generated *responsive to* the Bluetooth pairing data because it encodes this data and is generated in response to obtaining the data. EX1006, ¶75; EX1003, ¶¶217-18.



EX1006, Fig. 4 (annotated).

Brown's "color barcode" is a *color coded digital scannable media*, as

claimed, because it “employ[s] different color combinations.” EX1006, ¶76. A POSA would have understood that such color barcode encodes data through the different colors, such that the colors themselves encode data. EX1003, ¶219. For instance, Brown’s barcode can be a 2D matrix barcode (e.g., quick response (QR) code or Datamatrix). *See* EX1006, ¶36, Fig. 7. As Dr. Shenoy explains, such barcodes encode binary data in black and white modules, with black modules representing a “1” value and white modules representing a “0” value. EX1003, ¶219. A POSA would have understood that, in Brown’s color barcode, a first color (e.g., blue) would similarly represent a first value (e.g., “1”) and a second color (e.g., grey) would represent a second value (e.g., “0”). *Id.* Thus, a POSA would have understood that such color barcode is a *color coded digital scannable media*, as claimed. *Id.*

As Dr. Shenoy also explains, a POSA would have also understood that Brown’s color barcode encompasses barcodes that use more than two colors to encode data, such as the HCCB barcode, which encodes different data values using four (or more) different colors. EX1003, ¶220. Such color-coded barcodes were well-known before the ’123 patent’s priority date. *Id.* A POSA would have understood Brown to encompass such barcodes because they represent well-known examples of color barcodes that employ “different color combinations.” *See* EX1006, ¶¶2, 76; EX1003, ¶¶219-20.

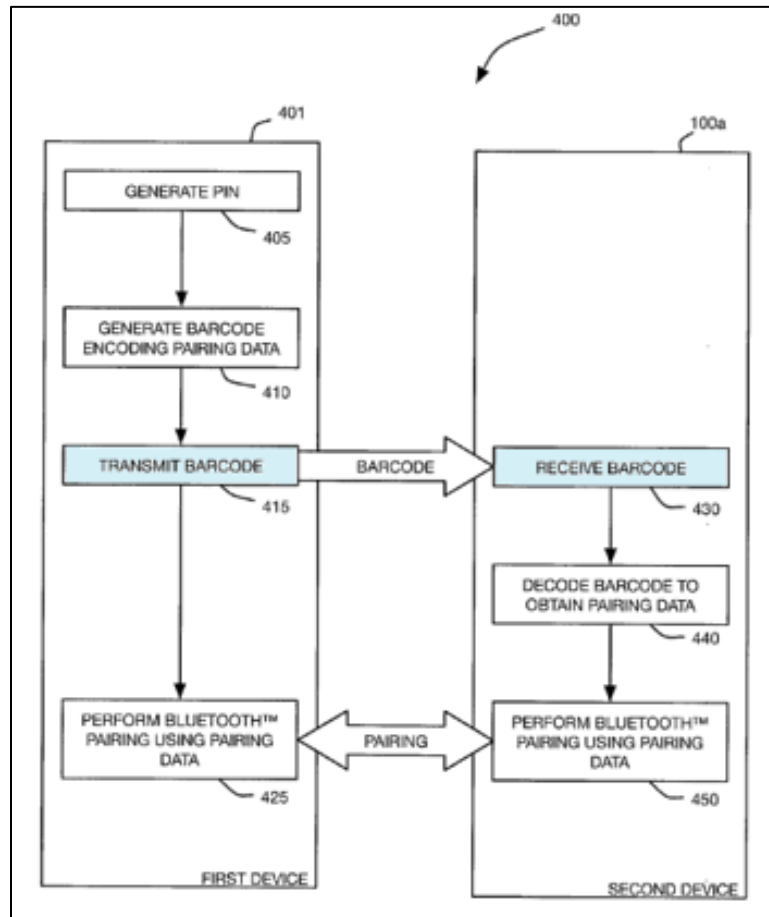
At the very least, a POSA would have found it obvious to implement such color-coded barcode (e.g., that encodes data through more than two colors) in Brown based on Brown's disclosure of a "color barcode." EX1003, ¶¶220-21. As Dr. Shenoy explains, color coded barcodes are advantageous in that they enable greater data density, such that more data can be stored in barcodes of smaller physical size. *Id.* A POSA would have been motivated to implement such color coded barcode to reduce the barcode size necessary to display the Bluetooth pairing data, and would have also found it obvious to implement such color coded barcode as a matter of a simple substitution of one known element (Brown's barcode) for another (a color coded barcode) to obtain predictable results (encoding device pairing data). *Id.*

i. [1.8]

Upon generating the color barcode image encoding the Bluetooth pairing data (*color coded digital scannable media*), Brown's device 401's *processor software* controls the display device by "displaying the image [that depicts the barcode] on a display." EX1006, ¶79, *see also* ¶¶67 ("displaying the barcode on a display associated with the first device"), 57, 70, 106.

As explained in Section VIII.C, in the Brown-Weiss system, the combined monitoring device would be adapted to implement a display for displaying Brown's color barcode. Thus, the combination of Brown and Weiss teaches this

element. EX1003, ¶¶222-23.

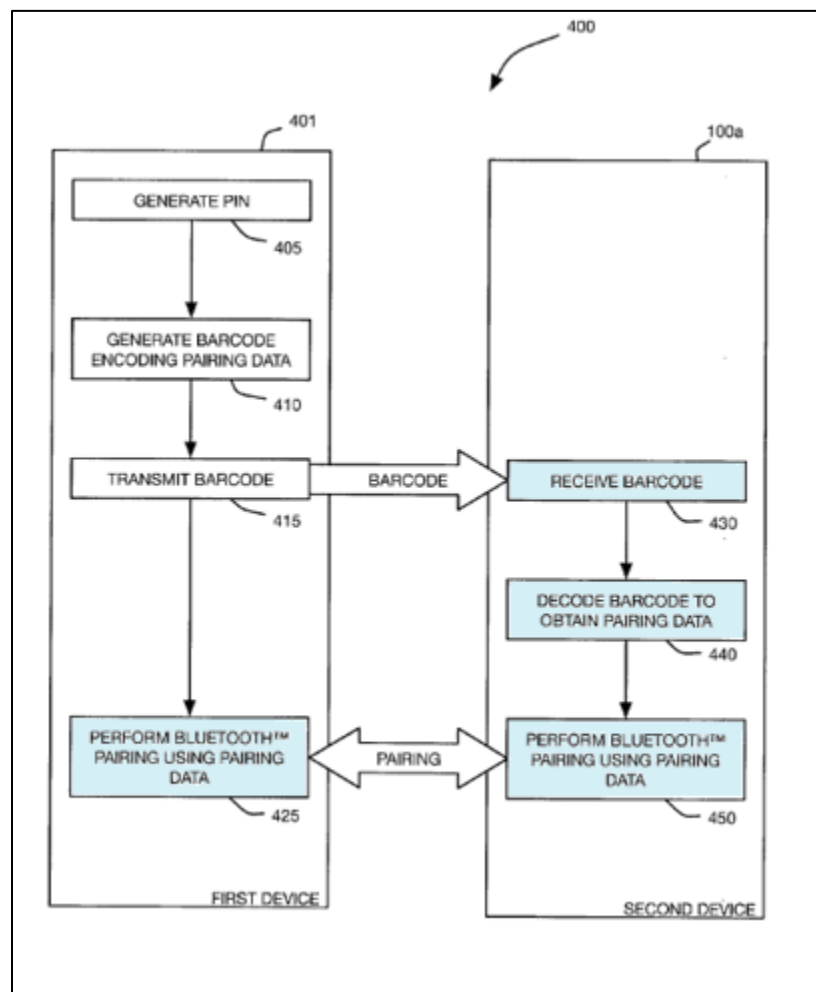


EX1006, Fig. 4 (annotated).

j. [1.9]

Brown’s device 401’s *processor software* “establish[es] communications [between the devices] for the first time” (*establishes the wireless communications link*). EX1006, ¶41, *see also* ¶43 (pairing “establish[es] a communication link” between devices), 105 (“pairing data [used] to establish wireless connections between devices”), 57, 70, 106. It does so *responsive to the mobile device scanning and decoding the color coded displayed digital scannable media*. EX1003, ¶¶224-25.

In particular, the device 100a “receives the image comprising the barcode,” which includes “scan[ing] (e.g., using a camera associated with the device) [the] barcode.” EX1006, ¶¶83, 91, *see also* ¶93. The device 100a then “extracts the barcode” and “decodes the barcode to obtain the Bluetooth pairing data.” EX1006, ¶¶83-84. The device 100a then “transmits Bluetooth pairing data, which depends in part on the PIN code... decoded from the barcode... to first device 401,” which, upon receiving this data, “continues the Bluetooth pairing process with second device 100a in known manner.” EX1006, ¶80, *see also* ¶85.



EX1006, Fig. 4 (annotated).

As explained in Section VIII.C, in the combined Brown-Weiss system, Weiss's monitoring device would be paired with the *mobile device*. As described, these devices would use Brown's device pairing process to "establish a communication link" between them. EX1003, ¶¶224-26. For instance, in the pairing process, the mobile device would scan and decode the HCCB displayed by the monitoring device in order to establish the wireless communications link between the devices. *Id.*

k. [1.10]

The combination of Brown and Weiss teaches this element for the reasons provided for element [1.2]. EX1003, ¶228. Weiss's monitoring device includes "a plurality of sensors for detecting one or more physiological attributes," such as "pulse, blood oxygen level, temperature, respiration, heart waveform, heart-rate, galvanic skin response, activity, perspiration, body fluid chemistry, and other such detectable attributes" (*bio-metric information and activity tracking information*). EX1007, 2:11-20. The monitoring device also includes sensors "for detecting the location and motion of an individual wearing the device" (*activity tracking information*). EX1007, 11:12-14, *see also* 12:3-9.

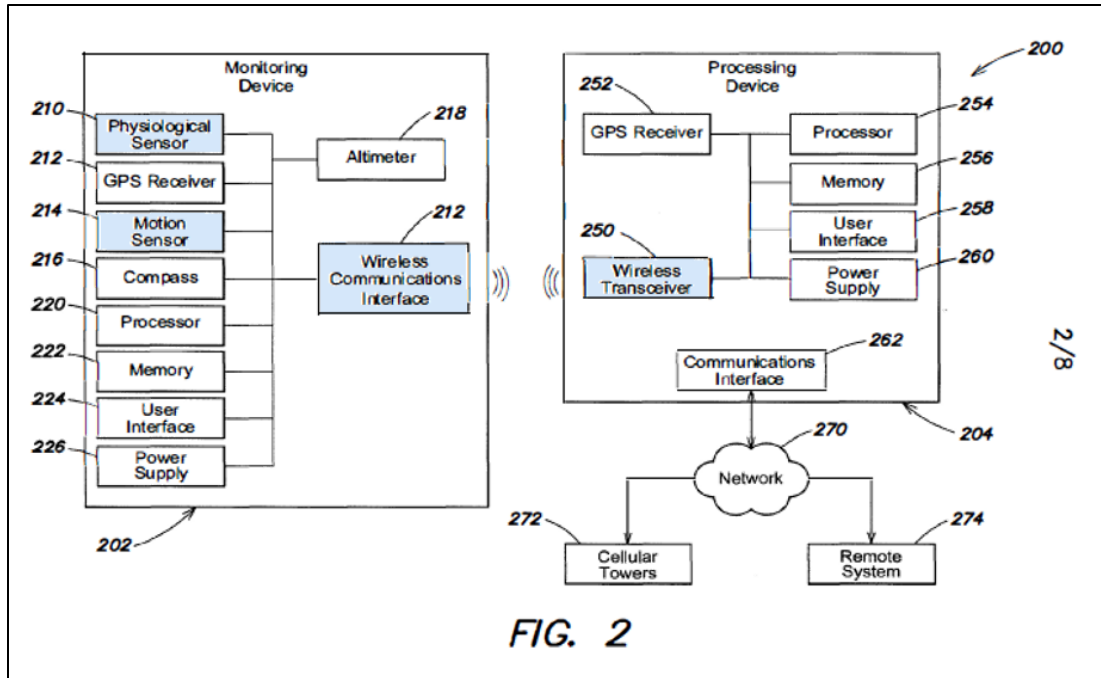
The Brown-Weiss monitoring device would generate such physiological attributes and location/motion data using the embedded sensors. EX1007, 7:21-23 ("Each sensor 112 can detect and measure, for example, one or a plurality of

physiological attributes”), 12:3-4 (“monitoring device [] is adapted to determine a location and/or a movement of the user”); EX1003, ¶¶228-30. It would do so using the *processor software* taught by the combination of Brown and Weiss. *See, e.g.*, EX1006, ¶¶57, 70, 106.

I. [1.11]

The combination of Brown and Weiss teaches this element. EX1003, ¶231. Weiss’s “monitoring device” (*wearable activity device*) communicates with the “processing device” (*mobile device*) through a “wireless communications interface” that is a “Bluetooth™-compatible transmitter.” EX1007, 11:10-12, 12:10-11; *see also* 7:30-8:2 (monitoring device includes a “wireless transmitter 114, such as a Bluetooth™ transmitter, for transmitting data acquired from one or more of the sensors 112 to the processing device 120”).

The monitoring device transmits data to the processing device, such as “data or information provided by” the physiological sensors or motion sensor of the monitoring device “and/or other data associated with the physiological attributes, the location and/or activities of an individual using the monitoring device.” EX1007, 13:1-5, *see also* 14:2-5 (“the monitoring device [] communicates one or more of the following to the processing device []: sensor data (e.g., physiological data), location data, motion data... etc.”).



EX1007, Fig. 2.

The monitoring device thus communicates *bio-metric information and activity tracking information* in the form of physiological sensor data, which includes “pulse, blood oxygen level, temperature, respiration, heart waveform, heart-rate, galvanic skin response, activity, perspiration, body fluid chemistry, and other such detectable attributes.” EX1007, 2:11-15, *see also* 21:30-22:5; EX1003, ¶¶232-33. The monitoring device also transmits additional *activity tracking information* in the form of, for instance, “motion data” and data relating to “activities of an individual,” etc. EX1007, 13:1-5, *see also* 12:2-9, 14:2-5; EX1003, ¶233.

As explained in Section VIII.C, in the Brown-Weiss system, Weiss’s monitoring device would generate such sensor information and wirelessly transmit

it to the mobile device over the *wireless communications link* established using Brown's communication initiation procedures. EX1003, ¶234. It would do so using the *processor software* taught by the combination of Brown and Weiss. *See, e.g.*, EX1006, ¶¶57, 70, 106. Thus, the combination of Brown and Weiss teaches this element.

2. Claim 11

a. [11.P]

The combination of Brown and Weiss teaches this element. EX1003, ¶235. As explained in Section VIII.C, and for claim 1, Brown teaches a *method for establishing a wireless communications link between two mobile devices*. EX1006, Abstract. Weiss teaches a method in which a monitoring device (*wearable activity device*) communicates wirelessly with a processing device (*mobile device*). EX1007, 2:8-20. In the combined system, Brown's wireless communication link establishment process would be used to establish the wireless communications link between Weiss's monitoring device and a mobile device, as taught by the combination of Brown and Weiss. EX1003, ¶235.

b. [11.1]

The combination of Brown and Weiss teaches this element for the reasons provided for element [1.5]. EX1003, ¶236. For instance, Brown-Weiss's monitoring device stores Bluetooth pairing data (comprising *wireless pairing information*) in memory. *See, e.g.*, EX1006, ¶¶40, 72, 75.

c. [11.2]

The combination of Brown and Weiss teaches this element for the reasons provided for element [1.6]. EX1003, ¶237. For instance, Brown-Weiss's monitoring device's *processor* receives or obtains from memory the Bluetooth pairing data (comprising *wireless pairing information*) to generate a barcode encoding the pairing data. *See, e.g.*, EX1006, ¶¶40, 70, 72, 75.

d. [11.3]

The combination of Brown and Weiss teaches or renders obvious this element for the reasons provided for element [1.7]. EX1003, ¶238. For instance, Brown-Weiss's monitoring device's *processor* generates a color-coded barcode (*color coded digital scannable media*) encoding the pairing data. *See, e.g.*, EX1006, ¶¶2, 75-76.

e. [11.4]

The combination of Brown and Weiss teaches this element for the reasons provided for element [1.8]. EX1003, ¶239. For instance, Brown-Weiss's monitoring device displays the color-coded barcode (*color coded digital scannable media*) on a display device. *See, e.g.*, EX1006, ¶¶2, 75-76, 79.

f. [11.5]

The combination of Brown and Weiss teaches this element for the reasons provided for element [1.9]. EX1003, ¶240. For instance, Brown-Weiss's *mobile device* “scan[s] (e.g., using a camera associated with the device) [the] barcode that

encodes pairing data.” EX1006, ¶¶82, 91, *see also* ¶93.

g. [11.6]

The combination of Brown and Weiss teaches this element for the reasons provided for element [1.9]. EX1003, ¶241. For instance, Brown-Weiss’s *mobile device* “process[es] the Bluetooth pairing data” (comprising wireless pairing information), and “decodes the barcode to obtain the Bluetooth pairing data.” EX1006, ¶¶83-84, 95.

h. [11.7]

The combination of Brown and Weiss teaches this element for the reasons provided for element [1.9]. EX1003, ¶242. For instance, Brown-Weiss’s *mobile device* “establish[es] a communication link” with the second device (*establish a wireless communications link*) using the processed (and decoded) Bluetooth pairing data. EX1006, ¶¶43, 84-85.

i. [11.8]

The combination of Brown and Weiss teaches this element for the reasons provided for element [1.10]. EX1003, ¶243. For instance, Brown-Weiss’s monitoring device’s *processor* generates physiological attributes and location/motion data (*activity information and bio-metric information*) using the embedded sensors. *See, e.g.*, EX1007, 7:21-23, 12:3-4.

Moreover, the monitoring device stores this *activity information and bio-metric information* in its *memory device*. EX1003, ¶244. As explained for element

[1.4], Weiss’s monitoring device includes “memory 222” (*memory device*), which “may be, for example, static RAM, dynamic RAM, ROM, EPROM, EEPROM, or flash memory.” EX1007, 11:14-19. For instance, Weiss’s monitoring device “stores data collected by, for example, the physiological sensor 210, in the memory 222.” EX1006, 13:10-12. A POSA would have understood that data collected by the other sensors (e.g., motion sensor, GPS, compass, etc.) is similarly stored in the memory 222. EX1003, ¶244.

j. [11.9]

The combination of Brown and Weiss teaches this element for the reasons provided for element [1.11]. EX1003, ¶245. For instance, Brown-Weiss’s monitoring device “communicates one or more of the following to the processing device []: sensor data (e.g., physiological data), location data, motion data... etc.” EX1007, 13:1-5, 14:2-5.

E. Dependent Claims

1. Claims 2 and 12

Weiss’s monitoring device (*wearable activity device*) is a wearable health monitoring device because it is “designed to be easily wearable and include one or a plurality of sensors for detecting one or more physiological attributes, including, but not limited to, pulse, blood oxygen level, temperature, respiration, heart waveform, heart-rate, galvanic skin response, activity, perspiration, body fluid chemistry, and other such detectable attributes.” EX1007, 2:8-15; *see also*

EX1007, 2:16-3:4. It is also a *smartwatch* because it can be “integrated into... a wristwatch.” EX1007, 7:26-29. In such configuration, the monitoring device is a *smartwatch* because it includes a “processor” for determining user vital signs, and a “wireless communications interface” for establishing wireless connections with other devices. EX1007, 11:7-12:18; EX1003, ¶247.

2. Claim 3 and 13

Brown-Weiss’s *wireless communication circuitry* is configured to implement a Bluetooth wireless connection link, which, as Dr. Shenoy explains, is a *personal area network communications link*. See EX1006, ¶¶22, 40, 70; EX1003, ¶249.

3. Claims 4 and 14

Brown’s mobile device is a “two-way communication device with advanced data communication capabilities,” such as “a cellular telephone with data messaging capabilities.” EX1006, ¶11. A POSA would have understood that this is a *smartphone* because it includes software application(s) to “manage data items of interest to a subscriber, such as, but not limited to, e-mail, calendar events, voice mails, appointments, and task items.” EX1006, ¶19, *see also* ¶17 (mobile device implements “web browsing and messaging such as e-mail, voice mail, Short Message Service (SMS), and Multimedia Messaging Services (MMS)”); EX1003, ¶251.

Moreover, Weiss's processing device (*mobile device*) can be "smartphone," such as an "iPhone" or "Blackberry." EX1007, 12:14-18. Thus, the combination of Brown and Weiss teaches this claim. EX1003, ¶252.

4. Claims 5 and 15

Brown's Bluetooth pairing data includes a MAC address of the device 401 (*wireless pairing information*). EX1006, ¶75, *see also* ¶40. In the combined Brown-Weiss system, the MAC address would be associated with Weiss's monitoring device (*wearable activity device*). A POSA would have understood that this MAC address is also an *identification identifier/number* because the device is a "unique network address" that "identifie[s]" the device. EX1006, ¶40; EX1003, ¶254.

5. Claims 9 and 19

As explained for element [1.7], Brown teaches or renders obvious the claimed *color coded digital scannable media*. As Dr. Shenoy explains, Brown's "color barcode" is *a representation of non-human readable information using colored pixels* and can be a "2-dimensional barcode" (*2D Matrix code*), such as a QR code. EX1006, ¶75, *see also* ¶36; EX1003, ¶¶256-57.

6. Claims 10 and 20

As explained in Section VIII.C, Brown-Weiss's monitoring device implements a display device as taught by Brown. *See supra* Section VIII.C (citing EX1006, ¶¶23, 75, 79). A POSA would have found it obvious to implement the

Brown-Weiss display as a touchscreen display, LED display, or LCD display.

EX1003, ¶259.

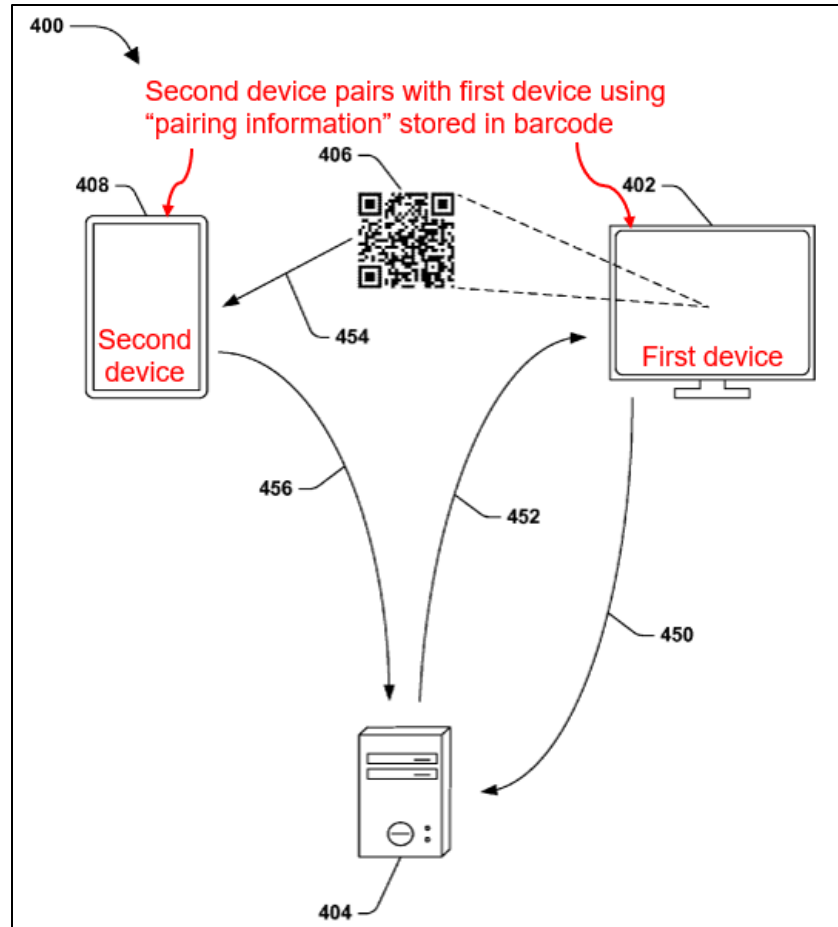
For instance, Brown's device 401 includes a "touch screen." EX1006, ¶¶12-13, 23. A POSA would have found it obvious to adapt Weiss's monitoring device to implement such a touch screen display. Indeed, as Dr. Shenoy explains, in 2011, cellular phone displays commonly included touch screens. EX1003, ¶260. A POSA would have thus recognized that such implementation would merely amount to a simple substitution of a known display component (Brown's touch screen) to achieve predictable results. *Id.*

Moreover, as Dr. Shenoy further explains, a POSA would have found it obvious to implement Brown-Weiss's display as an LED or LCD display because such displays were used for the overwhelming majority of cellular phones and mobile devices in 2011. EX1003, ¶261. As explained for claims 4 and 14, Brown's mobile device displays software applications for "e-mail, calendar events, voice mails, appointments, and task items," as well as "web browsing." EX1006, ¶¶17, 19. A POSA would have sought to include an LCD or LED display for displaying such applications and would have recognized that such implementation would merely amount to a simple substitution of display devices (an LED or LCD display for Brown-Weiss's combined display) to obtain predictable results. EX1003, ¶261. Moreover, as there were a limited number of display options for mobile phones at

the time, and because LED and LCD displays made up the vast majority of such displays, a POSA would have found it obvious to implement such LED or LCD display as merely choosing from a finite number of identified, predictable solutions, with a reasonable expectation of success. EX1003, ¶261-62.

**IX. GROUND 4B: BROWN-WEISS FURTHER IN VIEW OF ORT
TEACHES CLAIMS 1-5, 9-15, AND 19-20**

As explained in Section VIII, Brown-Weiss renders obvious all elements of claims 1-5, 9-15, and 19-20. EX1003, ¶263. However, to the extent that Brown’s color barcode is not *color coded* as claimed, a POSA would have found it obvious to implement such a color-coded barcode. *Id.* For instance, Ort discloses techniques “for joining two or more devices in a multi-device communication session.” EX1008, Abstract. In Ort, a first device displays to a second device a “visual tag” in the form of an HCCB that comprises “pairing information” that is “used to join a plurality of devices in a shared communication session.” EX1008, ¶6, *see also* ¶20. The second device “capture[s] the image of the tag displayed by the first device,” “retrieve[s] the device-session pairing information from the tag, and use[s] the information... to... join the session initiated by the first device.” EX1008, ¶23.



EX1008, Fig. 4 (annotated).

A POSA would have recognized the similarities between Brown and Ort, and thus the applicability of using Ort's HCCB to encode Brown's device pairing information. EX1003, ¶264. As explained, Brown teaches color coded barcodes through its disclosure of a "color barcode." *See* EX1006, ¶¶2, 76, *see also* ¶¶36, 75. However, to the extent that Brown's color barcode is not the color-coded barcode as claimed, Ort's HCCB is. *See* Section V.D.1.h.

As Dr. Shenoy explains, Microsoft commercialized its HCCB in 2007, well before the priority date of the '123 patent. EX1003, ¶264. HCCBs are

advantageous over black and white barcodes because they provide a higher data density. EX1003, ¶265. A POSA would have thus recognized the benefits and applicability of implementing Ort's HCCB in Brown-Weiss. EX1003, ¶266. Moreover, simply changing the type of barcode used in the Brown-Weiss system, as taught by Ort, would not have otherwise impacted the Brown-Weiss combination beyond software changes necessary to implement the HCCB, and a POSA would not have had any trouble implementing Ort's disclosures in Brown-Weiss. EX1003, ¶¶266-67. A POSA would have found it obvious to implement Brown's "color barcode" as an HCCB as merely a simple substitution of one known element (Ort's HCCB) for another (Brown's barcode) to obtain predictable results (encoding device pairing data). *Id.*

Thus, the combination of Brown, Weiss, and Ort renders obvious the claimed *color coded digital scannable media*. EX1003, ¶268. As Dr. Shenoy explains, when implemented as an HCCB, the barcode is also a *representation of non-human readable information using colored pixels* and a *2D Matrix code*, as required by claims 9 and 19. *Id.* Brown-Weiss-Ort renders obvious all other elements of claims 1-5, 9-15, 19-20 for the reasons provided for Brown-Weiss in Section VIII. *Id.*

X. GROUNDS 5A AND 5B: BROWN-WEISS AND BROWN-WEISS-ORT FURTHER IN VIEW OF WILLIAMS RENDERS OBVIOUS CLAIMS 6 AND 16

As explained in Section VI, Williams teaches a Bluetooth pairing process in which a first device encrypts wireless pairing information that is encoded in a barcode image. EX1009, ¶¶26-28, 29. A POSA would have found it obvious to implement these techniques in Brown-Weiss (and Brown-Weiss-Ort) to provide increased security of the device pairing process. EX1003, ¶271.

Brown's process implements a "secure" pairing process by encoding Bluetooth pairing data in barcodes. A POSA would have recognized that Williams's technique provides improved security by encrypting similar pairing data. *Id.* Indeed, encrypting the data encoded in Brown's barcode would ensure that only parties with the relevant encryption key would be able to decipher the pairing data and pair with the device.

Indeed, as Dr. Shenoy explains, encryption was a well-known technique for implementing secure communications. EX1003, ¶272. Furthermore, it was well known to encrypt information encoded in barcodes. *Id.* A POSA would have thus found it obvious to encrypt Brown-Weiss and Brown-Weiss-Ort's graphically encoded data, as taught by Williams, and would have had a reasonable expectation of success in doing so. EX1003, ¶273. Indeed, encryption was commonly performed to secure data and a POSA would have readily understood how to

implement William’s encryption techniques. *Id.* For instance, a POSA would have readily understood how to implement and communicate suitable keys for encrypting and decrypting the data in accordance with well-established and conventional techniques. *See, .g.,* EX1009, ¶¶9, 43. This would have been obvious as merely requiring the use of a known technique (encrypted barcode images) to improve similar processes (wireless pairing processes) in the same way (provide enhanced security). EX1003, ¶273.

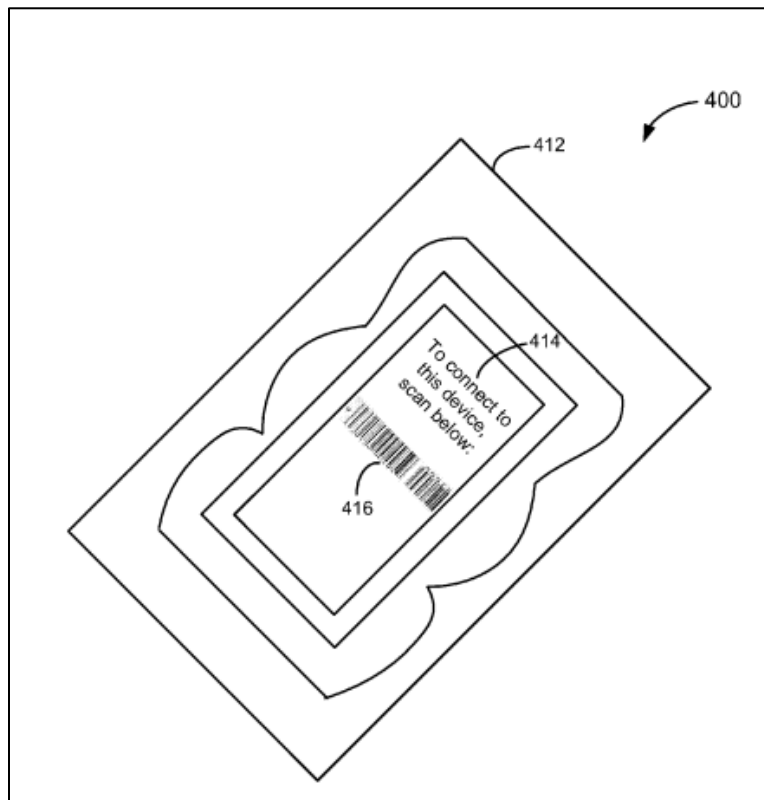
Thus, the combination of Brown, Weiss, and Williams, and the combination of Brown, Weiss, Ort, and Williams renders obvious claims 6 and 16. EX1003, ¶274.

XI. GROUNDS 6A AND 6B: BROWN-WEISS AND BROWN-WEISS-ORT FURTHER IN VIEW OF KOVITZ RENDERS OBVIOUS CLAIMS 7-8 AND 17-18

As explained in Section VIII.D, Brown teaches *wireless pairing information* comprising a MAC address used to establish wireless communications between devices. The MAC address is *wireless communication circuitry information* because it is a “unique network address that is assigned to each device (i.e., when it is manufactured).” EX1006, ¶40. To the extent Brown does not disclose *wireless pairing information that comprises* the wearable activity device information required by claims 7-8 and 17-18, Kovitz does. EX1003, ¶275.

As explained in Section VII, Kovitz teaches techniques for “wireless device

connection and pairing” using barcodes. EX1021, Abstract. The barcodes encode, among other things, *wearable activity device information*, such as software “applications supported or required by a device” (*device software information*) and “usage requirements, power requirements, current battery levels” of the device (*device utilization information*). EX1021, 11:40-45, 12:36-13:14.



EX1021, Fig. 4C.

A POSA would have found it obvious to implement Kovitz’s *device software information* and *device utilization information* in Brown-Weiss and Brown-Weiss-Ort’s Bluetooth pairing data. EX1003, ¶¶276-77.

Kovitz teaches that specific application identifiers in the pairing data would inform the pairing device of particular “applications supported or required by a

device,” such as “software or code [] necessary to enable or configure communication with the device.” EX1021, 12:36-51. This would enable the pairing device to determine if it “has all required applications installed,” and if not, to download such applications. EX1021, 12:56-13:14; EX1003, ¶277. As another example, including the *utilization information* in the pairing data would enable the devices to “negotiate” a suitable protocol to use based on this information, as taught by Kovitz. EX1021, 16:13-17:11; EX1003, ¶278; *see also* EX1006, ¶105.

A POSA would have sought to implement these features in Brown-Weiss and Brown-Weiss-Ort to enhance the pairing process, and to tailor it to the specific requirements of the devices being paired. EX1003, ¶279. As Brown already teaches a wireless pairing process using barcodes, a POSA would have readily been able to implement Kovitz’s techniques in Brown-Weiss and Brown-Weiss-Ort. *Id.* Indeed, a POSA would have recognized that this would merely amount to the use of a known technique (encoding device utilization and software information in barcodes) to improve similar devices in the same way (an enhanced pairing process that accounts for device requirements or capabilities). *Id.*

XII. CERTIFICATION UNDER RULE 42.104(A)

Petitioner certifies that the ’123 patent is available for IPR and Petitioner is not barred or estopped from requesting IPR of any claim.

XIII. MANDATORY NOTICES (37 C.F.R. § 42.8(A)(1))

A. Real Party-in-Interest (37 C.F.R. § 42.8(b)(1)):

The real party-in-interest is Petitioner Apple Inc.

B. Related Matters (37 C.F.R. § 42.8(b)(2))

The '123 patent is at issue in *iScan2D Technologies, LLC v. Apple Inc.*, 1-25-cv-01794 (W.D. Tex).

C. Lead and Back-up Counsel (37 C.F.R. § 42.8(b)(3))

Lead Counsel for Petitioner is:

Richard M. Bemben (Reg. No. 68,658)
STERNE, KESSLER, GOLDSTEIN & FOX PLLC
1101 K Street, NW, 10th Floor
Washington, DC 20005
202-772-8549 (telephone)
202-371-2540 (facsimile)
rbemben-PTAB@sternekessler.com.

Back-up Counsel for Petitioner are:

David Haars (Reg. No. 73,112)
STERNE, KESSLER, GOLDSTEIN & FOX PLLC
1101 K Street, NW, 10th Floor
Washington, DC 20005
202-772-8680 (telephone)
202-371-2540 (facsimile)
dhaars-PTAB@sternekessler.com;

Robert E. Sokohl (Reg. No. 36,013)
STERNE, KESSLER, GOLDSTEIN & FOX PLLC
1101 K Street, NW, 10th Floor
Washington, DC 20005
202-772-8677 (telephone)
202-371-2540 (facsimile)
rsokohl-PTAB@sternekessler.com; and

Justin Wang (Reg. No. 81,975)
STERNE, KESSLER, GOLDSTEIN & FOX PLLC
1101 K Street, NW, 10th Floor
Washington, DC 20005
202-772-8677 (telephone)
202-371-2540 (facsimile)
jwang-PTAB@sternekessler.com

D. Service Information (37 C.F.R. § 42.8(b)(4))

Please address all correspondence to the lead and back-up counsel as shown above. Petitioner consents to electronic service by e-mail at all of the e-mail addresses listed above and PTAB@sternekessler.com.

XIV. CONCLUSION

The Board should find all claims to be unpatentable.

Respectfully submitted,

STERNE, KESSLER, GOLDSTEIN & FOX PLLC

/Richard M. Bemben/

Richard M. Bemben
Registration No. 68,658
Lead Attorney for Petitioner

Date: May 18, 2026

1101 K Street, NW
10th Floor
Washington, DC 20005
(202) 371-2600

CERTIFICATE OF WORD COUNT (37 C.F.R. § 42.24(d))

1. This Petition for *Inter Partes* Review complies with the type-volume limitation of 14,000 words, comprising 13,708 words, excluding the parts exempted by 37 C.F.R. § 42.24(a)(1).

2. This Petition for *Inter Partes* Review complies with the general format requirements of 37 C.F.R. § 42.6(a) and has been prepared using Microsoft® Word 2016 in 14-point Times New Roman font.

Respectfully submitted,

STERNE, KESSLER, GOLDSTEIN & FOX PLLC

/Richard M. Bemben/

Richard M. Bemben
Registration No. 68,658
Lead Attorney for Petitioner

Date: May 18, 2026

1101 K Street, NW
10th Floor
Washington, DC 20005
(202) 371-2600

CERTIFICATE OF SERVICE (37 C.F.R. §§ 42.6(e), 42.105(a))

I certify that the above-captioned **PETITION FOR *INTER PARTES***
REVIEW FOR U.S. PATENT NO. 11,664,123 and associated Exhibits 1001-
1034 were served in their entireties upon the Patent Owner on May 18, 2026, via
U.S.P.S. Priority Express Mail at the following addresses:

Allen D. Hertz
ALLEN D. HERTZ, P.A.
12784 Tulipwood Circle
Boca Raton, FL 33428

René A. Vazquez
DNL ZITO
1250 Connecticut Avenue, NW
Suite 700
Washington, DC 20036

Respectfully submitted,

STERNE, KESSLER, GOLDSTEIN & FOX PLLC

/Richard M. Bemben/

Richard M. Bemben
Registration No. 68,658
Lead Attorney for Petitioner

Date: May 18, 2026

1101 K Street, NW
10th Floor
Washington, DC 20005
(202) 371-2600