

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner

v.

ISCAN2D TECHNOLOGIES, LLC,
Patent Owner

Case IPR2026-00317
U.S. Patent No. 12,230,394

**DECLARATION OF DR. PRASHANT SHENOY IN SUPPORT OF
PETITION FOR *INTER PARTES* REVIEW
OF U.S. PATENT NO. 12,230,394**

Mail Stop "PATENT BOARD"

Patent Trial and Appeal Board
U.S. Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

Apple EX1003
IPR2026-00317
U.S. Patent No. 12,230,394

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	MY BACKGROUND AND QUALIFICATIONS	2
III.	SUMMARY OF OPINIONS.....	6
IV.	MATERIALS CONSIDERED	8
V.	LEGAL UNDERSTANDING.....	11
A.	My Understanding of Claim Construction.....	11
B.	My Understanding of Obviousness	11
C.	A Person of Ordinary Skill in the Art	14
VI.	BACKGROUND OF THE TECHNOLOGY.....	15
A.	Barcodes are generally used to encode information, including wireless pairing information to establish wireless communications.....	15
1.	General overview of barcodes	15
2.	Color coded barcodes were known.....	19
3.	Barcodes were used to encode wireless pairing information.....	21
B.	Wearable biometric devices were known and used to share information over wireless communication links, and to generate and display barcodes	27
1.	Wearable devices were known to generate biometric data and communicate it over wireless network.....	27
2.	Wearable devices were known to include user interfaces for generating and displaying data, including barcodes encoding information	30
VII.	OVERVIEW OF THE '394 PATENT	32
VIII.	PROSECUTION HISTORY	33
IX.	LEVEL OF ORDINARY SKILL IN THE ART.....	34
X.	CLAIM CONSTRUCTION	35
XI.	GROUND 1: BISHOP IN VIEW OF LEBOEUF RENDERS OBVIOUS CLAIMS 1-3, 5-8, 11-14, AND 16-18.	35

A.	Overview of Bishop.....	35
B.	Overview of LeBoeuf.....	38
C.	Motivation to Combine	41
D.	Independent Claims.....	53
1.	Claim 1	53
2.	Claim 11	81
E.	Dependent Claims	95
1.	Claims 2 and 13.....	95
2.	Claim 3.....	96
3.	Claims 5 and 17.....	96
4.	Claims 6 and 18.....	97
5.	Claims 7 and 16.....	98
6.	Claims 8 and 12.....	98
7.	Claim 14.....	99
XII.	GROUND 2: BISHOP-LEBOEUF FURTHER IN VIEW OF WILLIAMS RENDERS OBVIOUS CLAIMS 4, 9, 10, 15, 19, AND 20.	100
1.	Williams	100
2.	Claims 4 and 15.....	101
3.	Claims 9, 10, 19, and 20	104
XIII.	GROUND 3A: BROWN IN VIEW OF WEISS RENDERS OBVIOUS CLAIMS 1-8 AND 11-18.....	106
A.	Brown	107
B.	Weiss	109
C.	Motivation to Combine	110
D.	Independent Claims.....	117
1.	Claim 1	117
2.	Claim 11	141
E.	Dependent Claims	154
1.	Claims 2 and 13.....	154

2.	Claim 3.....	155
3.	Claims 4 and 15.....	155
4.	Claims 5 and 17.....	156
5.	Claims 6 and 18.....	157
6.	Claims 7 and 16.....	158
7.	Claims 8 and 12.....	158
8.	Claim 14.....	159
XIV.	GROUND 3B: BROWN-WEISS FURTHER IN VIEW OF ORT TEACHES CLAIMS 1-8, 11-18	159
XV.	GROUND 4A AND 4B: BROWN-WEISS AND BROWN-WEISS- ORT FURTHER IN VIEW OF WILLIAMS RENDERS OBVIOUS CLAIMS 9, 10, 19, AND 20	163
1.	Claims 9, 10, 19, and 20	163
XVI.	OBJECTIVE INDICIA.....	166
XVII.	CONCLUSION.....	167

I, Prashant Shenoy, Ph.D., hereby declare as follows.

I. INTRODUCTION

1. I have been retained as an expert witness on behalf of Petitioner Apple Inc. (“Petitioner”) for the above-captioned *inter partes* review (IPR). I am being compensated for my time in connection with this IPR at my standard consulting rate.

2. I understand that this Declaration accompanies a petition for IPR involving U.S. Patent No. 12,230,394 (“the ’394 patent”) (EX1001), which resulted from U.S. Patent Application No. 18/320,937 (“the ’937 application”), filed on May 19, 2023. Based on Provisional Application No. 61/515,728, I understand that the ’394 patent alleges a priority date of August 5, 2011. Although I have not performed an analysis as to whether the ’394 patent is actually entitled to this date, I refer to this date as the priority date throughout this Declaration. My opinions would not change if the ’394 patent is entitled to a different priority date.

3. In preparing this Declaration, I have reviewed the ’394 patent and each of the documents cited herein, in light of general knowledge in the art before August 5, 2011. In formulating my opinions, I have relied upon my experience, education, and knowledge in the relevant art. In formulating my opinions, I have also considered the viewpoint of a person of ordinary skill in the art at the time of the invention (“POSA”).

II. MY BACKGROUND AND QUALIFICATIONS

4. My complete qualifications and professional experience are described in my Curriculum Vitae, a copy of which can be found in Exhibit 1033. The following is a brief summary of my relevant qualifications and professional experience.

5. Over the years, I have led research and industry collaboration projects in areas such as storage and file systems, Web and Internet systems, content distribution, streaming media, database systems, cloud computing, virtualization, RFID and sensor networks, and energy systems. During that time, I have consulted with both large companies and startups in a technical advisory role related to product architecture, IP issues, and applied research.

6. I am a tenured professor in the College of Information and Computer Sciences at the University of Massachusetts Amherst ("UMass"), where I currently hold the position of Distinguished Professor of Computer Science. I also served as an Associate Dean in the College of Information and Computer Sciences from 2016 to 2025. I have been a faculty member at UMass since 1998. I also hold a visiting appointment at UCLA where I am presently on sabbatical from UMass.

7. I received my Bachelor of Technology (B.Tech.) degree in 1993 from the Department of Computer Science and Engineering at The Indian Institute of Technology ("IIT"), Mumbai, India. IIT awarded me the Institute Medal for being

the top-ranking undergraduate student. In 1994, I received my Master of Science (M.S.) degree in Computer Sciences from The University of Texas at Austin. In 1998, I received my Doctor of Philosophy (Ph.D.), also from the Department of Computer Sciences at The University of Texas at Austin. My dissertation, which was in the area of file systems, was recognized by the department as the Best Doctoral Dissertation of 1998-1999.

8. I have been involved in the research and development of distributed computing systems for more than 30 years. At UMass, I perform research and teach in the areas of distributed systems, operating systems, computer networking, data management, and multimedia systems, among others.

9. A major focus of my research has been the design of large-scale distributed computing systems. Over the years, I have led research and industry collaboration projects in areas such as computer networking, distributed systems, storage and file systems, Web and Internet systems, content distribution, streaming media, database systems, cloud computing, virtualization, RFID and sensor networks, and energy systems. During that time, I have consulted with both large companies and startups in a technical advisory role related to product architecture, IP issues, and applied research.

10. For example, starting in the early 1990s, my research focused on the development of storage and file systems. During that time, I developed multimedia

file system and data management technologies that were designed for efficient storage and retrieval of large amounts of video and audio data. I collaborated with AT&T Bell Laboratories to design a new media server for video streaming. These efforts resulted in U.S. Patent No. 6,079,028 on fault-tolerant architectures for continuous media servers.

11. In the late 1990s, I led the design of a new operating system called QLinux, that was based on the open-source Linux operating system. As part of this research, I developed resource management and scheduling techniques that provide isolation and service guarantees to applications. This technology provided the underpinnings for fair resource management and isolation techniques used in OS virtualization. It was adopted by a startup company for providing resource isolation in its web hosting products.

12. In the early 2000s, I led several projects on web systems and cloud computing. For example, I led research projects on web technologies such as web caching and scaling web applications. I also led research projects on cloud computing platforms (which were known as web hosting platforms at the time) involving virtualization, dynamic resource management, replication, fault tolerance, and storage. My group at UMass collaborated with technology companies such as IBM, AT&T, Sprint, Intel, and many others as part of this research.

13. My research on virtualization has involved design of technologies for virtual machines and container resource management and their deployment in cloud computing systems and data centers. I am co-inventor on U.S. Patent No. 8,473,557, jointly assigned to AT&T and UMass, on virtual machine migration.

14. Over the years, I have authored or co-authored more than 300 articles in peer-reviewed journals and conference proceedings that have been cited over 27,000 times. Seventeen papers authored by myself and members of my research group on this project won awards for their technical contributions. Two papers have won Test-of-Time awards, an award given to a publication that has had the most impact over a ten-year period since its publication.

15. I have served as an Editor for six leading journals and have served as the Technical Program Chair for twenty conferences and workshops in my field. I founded the ACM Special Interest Group on Energy Systems and also served on steering committee of conferences and journals.

16. I am also a Fellow of the ACM, IEEE, AAAS, and AAIA, four professional societies in computing and science.

17. I am a named inventor on three U.S. Patents and one published application (Nos. 2014/0040206, 8,510,596, 8,473,557, and 6,079,028). These documents are generally related to distributed and operating systems, virtualization, and cloud data centers.

18. As a faculty member at UMass, I have also taught undergraduate and graduate courses in operating systems, distributed systems, networking, and related topics for more than twenty-five years.

19. These courses teach concepts related to operating systems, virtual machines, containers, cloud computing, file systems, and distributed systems. They also involve hands-on course projects on these topics.

III. SUMMARY OF OPINIONS

20. In forming my opinions about the '394 patent, I have considered the following grounds of unpatentability based on obviousness. Based on my review of the prior art references that form the basis of these grounds, it is my opinion that claims 1-20 of the '394 patent would have been obvious to a POSA prior to August 5, 2011. The prior art references I rely on are:

- U.S. 2011/0072263 (“Bishop”), which was filed September 23, 2009, and published March 24, 2011.
- U.S. 2008/0146892 (“LeBoeuf”), which published June 19, 2008.
- U.S. 2010/0012715 (“Williams”), which published January 21, 2010.
- U.S. 2011/0081860 (“Brown”), which was filed on October 2, 2009, and published April 7, 2011.
- WO 2010/144626 (“Weiss”), which published on December 16, 2020.
- U.S. 2012/0198531 (“Ort”), which was filed January 31, 2011, and

published August 2, 2012.

21. I understand that each of these references constitutes prior art to the '394 patent because they were filed and/or published before the '394 patent's earliest priority date. I apply the following grounds of unpatentability applying these prior art references:

Ground	Claims	References
1	1-3, 5-8, 11-14, 16-18	Bishop in view of LeBoeuf
2	4, 9, 10, 15, 19, 20	Bishop in view of LeBoeuf and further in view of Williams
3A	1-8, 11-18	Brown in view of Weiss
3B	1-8, 11-18	Brown in view of Weiss and further in view of Ort
4A	9, 10, 19, 20	Brown in view of Weiss and further in view of Williams
4B	9, 10, 19, 20	Brown in view of Weiss and further in view of Ort and Williams

22. I have been asked to consider how a POSA would have understood the challenged claims in light of the disclosures of the '394 patent. I have also been asked to consider how a POSA would have understood the prior art references listed in the table above.

23. Further, I have been asked to consider and provide my technical review, analysis, insights, and opinions regarding whether a POSA would have

understood that the combinations of the prior art references listed in the table above render obvious claims 1-20 of the '394 patent.

IV. MATERIALS CONSIDERED

24. In formulating my opinions, I have relied upon my training, knowledge, and experience that are relevant to the '394 patent. I have also reviewed and am familiar with the following documents and materials in addition to any other documents cited in this declaration:

Exhibit No.	Description
1001	U.S. Patent No. 12,230,394 to McKirdy
1002	File History of U.S. Patent No. 12,230,394
1003	Declaration of Dr. Prashant Shenoy in Support of Petition for <i>Inter Partes</i> Review of U.S. Patent No. 12,230,394
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 Pub. No. WO 2010/144626 to 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")

Exhibit No.	Description
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)
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”)

Exhibit No.	Description
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”)
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”)

25. To the best of my knowledge, the above-mentioned documents and materials are true and accurate copies of what they purport to be. An expert in the field would reasonably rely on them to formulate opinions such as those set forth in this declaration.

V. LEGAL UNDERSTANDING

26. I have also relied upon various legal principles (as explained to me by Apple's counsel) in formulating my opinions. My understanding of these principles is summarized below.

A. My Understanding of Claim Construction

27. I understand that during an *inter partes* review proceeding, claims are to be construed in light of the specification as would be read by a person of ordinary skill in the relevant art at the time the application was filed. I understand that claim terms are given their ordinary and customary meaning as would be understood by a person of ordinary skill in the relevant art in the context of the entire disclosure. A claim term, however, will not receive its ordinary meaning if the patentee acted as his own lexicographer and clearly set forth a definition of the claim term in the specification. In this case, the claim term will receive the definition set forth in the patent.

B. My Understanding of Obviousness

28. I understand that a patent claim is invalid if the claimed invention would have been obvious to a POSA at the time the application was filed. This

means that even if all of the requirements of the claim cannot be found in a single prior art reference that would anticipate the claim, the claim can still be invalid.

29. To obtain a patent, a claimed invention must have, as of the priority date, been nonobvious in view of the prior art in the field. I understand that an invention is obvious when the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious to a POSA at the time the invention was made.

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

(1) identify the particular references that, singly or in combination, render the patent obvious;

(2) specifically identify which elements of the patent claim appear in each of the asserted references; and

(3) explain how the prior art references would have been combined or modified in order to create the inventions claimed in the asserted claim.

30. I also understand that prior art references can be combined under several different circumstances. For example, it is my understanding that one such circumstance is when a proposed combination of prior art references results in a system that represents a predictable variation, which is achieved using prior art elements according to their established functions.

31. I also understand that when considering the obviousness of a patent claim, one should consider whether a teaching, suggestion, or motivation to combine the references exists so as to avoid impermissibly applying hindsight when considering the prior art. I understand this test should not be rigidly applied, but that the test can be important to avoid such hindsight. I also understand that, when combining references, characterizing the references as “primary” and “secondary” is merely a matter of presentation with no legal significance. For instance, whether a combination is presented as reference A in view of reference B or reference B in view of reference A does not affect the underlying obviousness considerations for a patent claim.

32. I understand that certain objective indicia can be important evidence as to whether a patent is obvious or nonobvious. Such indicia include:

(1) commercial success of products covered by the patent claims; (2) a long-felt need for the invention; (3) failed attempts by others to make the invention; (4) copying of the invention by others in the field; (5) unexpected results achieved by the invention as compared to the closest prior art; (6) praise of the invention by the infringer or others in the field; (7) the taking of licenses under the patent by others; (8) expressions of surprise by experts and those skilled in the art at the making of the invention; and (9) the patentee proceeded contrary to the accepted wisdom of the prior art.

33. I also understand that “obviousness” is a legal conclusion based on the underlying factual issues of the scope and content of the prior art, the differences between the claimed invention and the prior art, the level of ordinary skill in the prior art, and any objective indicia of non-obviousness.

34. For that reason, I am not rendering a legal opinion on the ultimate legal question of obviousness. Rather, my testimony addresses the underlying facts and factual analysis that would support a legal conclusion of obviousness or non-obviousness, and when I use the term obvious, I am referring to the perspective of one of ordinary skill in the art at the time of invention.

C. A Person of Ordinary Skill in the Art

35. I understand that a person of ordinary skill in the relevant art (“POSA”) is presumed to be aware of all pertinent art, thinks along conventional wisdom in the art, and is a person of ordinary creativity—not an automaton.

36. I have been asked to consider the level of ordinary skill in the field that someone would have had at the time the claimed invention was made. In deciding the level of ordinary skill, I considered the following:

- the levels of education and experience of persons working in the field;
- the types of problems encountered in the field; and
- the sophistication of the technology.

37. My opinion below explains how a POSA would have understood the technology described in the references I have identified herein around the August 5, 2011 timeframe, which I have been advised is the earliest possible effective filing date for the '394 patent. However, my opinions herein would not be affected if the '394 patent is found to only be entitled to a later effective filing date.

38. Regardless of whether I use “I” or a “POSA” during my technical analysis below, all of my statements and opinions are to be understood to be based on how a POSA would have understood or read a document at the time of the alleged invention.

VI. BACKGROUND OF THE TECHNOLOGY

39. As I further explain in Section VII, the '394 patent describes establishing wireless communication links by encoding wireless pairing data in barcodes. The claims of the '394 patent broadly recite a wearable activity tracking device and a mobile device that implement this pairing process to communicate and display biometric or activity related data of a user. These concepts, however, were well known before the '394 patent's earliest possible priority date.

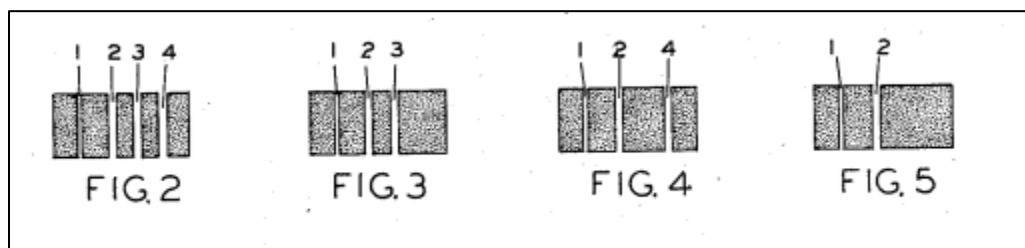
A. Barcodes are generally used to encode information, including wireless pairing information to establish wireless communications

1. General overview of barcodes

40. Barcodes are visual representations of machine-readable data. Barcodes encode such data into patterns, such as patterns of vertical bars, dots,

squares, or other arrangement. Barcodes have been known for decades. In fact, they are described in U.S. Patent No. 2,612,994 to Woodland et al., which issued in 1952 and is thought to be the first patent describing barcodes. *See* EX1012.

Woodland describes a “pattern of white lines... on a dark background,” where the lines have fixed places. EX1012, 2:16-50. Line 1 represents a “datum line” while subsequent lines (e.g., Lines 2-4) represent “information lines” such that the presence of an information line at its designated place represents a “numeral one (1)” and the absence of an information line at its designated place represents “zero (0).” *Id.* The barcodes are thus visual representations of binary numbers. *Id.* For instance, Figure 2 represents the binary number 111 because lines 2, 3, and 4 are present. *Id.* Similarly, Figure 3 represents the binary number 110 because information lines 2 and 3 are present but information line 4 is not, and Figure 4 represents the binary number 101 because line 3 is vacant. *Id.*

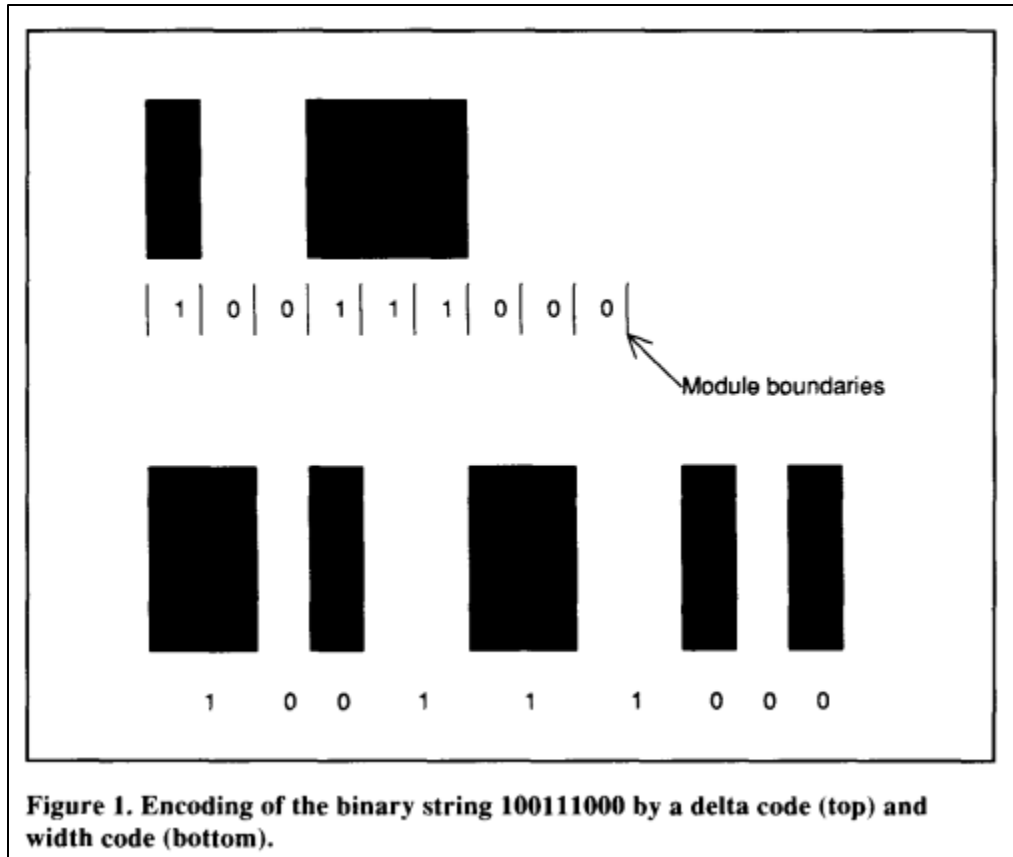


EX1012, FIGs. 2-5.

41. Barcodes were ubiquitous long before the priority date of the '394 patent, and were used to encode information for a range of industries, such as retail, publishing, factories, military, healthcare, grocery, healthcare, apparel,

merchandise, etc. EX1013, 74; EX1014, 1. There are many different types of barcodes, each having different encoding schemes, or symbologies. EX1013, 74. Early codes were one-dimensional (1D) such as the Universal Product Code (UPC), which was commonly used for tracking trade items in stores, and Code 39, which was used in the Department of Defense. EX1013, 74-77. These codes were generally black-and-white, and stored data in the form of parallel lines, including black “bars” and white “spaces.” EX1013, 75.

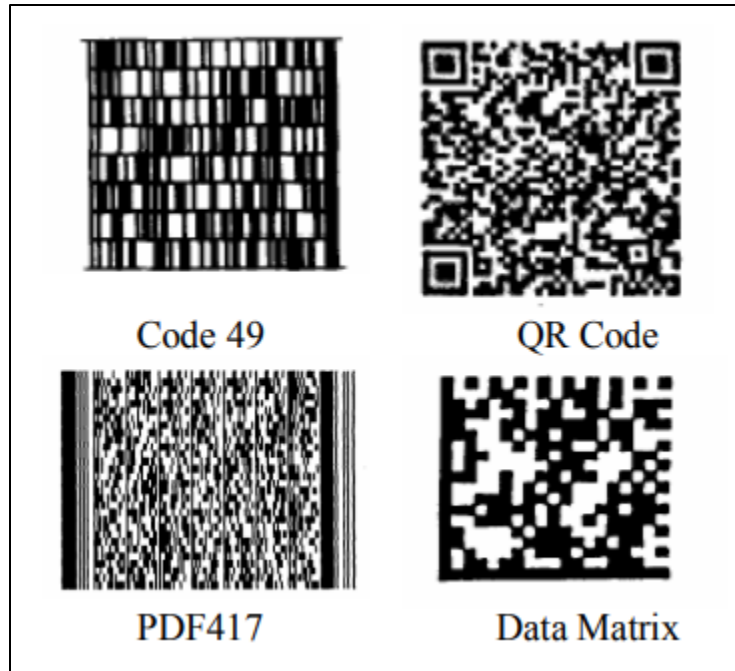
42. There are two fundamental ways of encoding information in a 1D manner. The first is to assign 1’s and 0’s to “modules,” with black bars representing the 1’s and white spaces representing the 0’s. EX1013, 2. These are called “delta codes,” but can also be referred to as “color codes” because the data is encoded in the different colors (e.g., black and white) of the bars and spaces. EX1013, 75. The other fundamental way of encoding one-dimensional codes is to encode data based on the widths of the bars and spaces, such that wider elements represent 1’s and narrower elements represent 0’s. EX1013, 75. These are called “width codes.” EX1013, 75. Example delta and width codes are shown in the below figure. As shown, the delta code (top) encodes 1’s as black bars and 0’s as white spaces. Both of these codes encode the number 100111000. The width code encodes 1’s as wider elements (either bars or spaces) and 0’s as narrower elements.



EX1013, FIG. 1.

43. As the use of barcodes increased, people sought to increase the amount of data that could be stored in barcodes. This led to the development of two-dimensional (2D) barcodes that store a large amount of data in a small area.

EX1014, 1. Unlike 1D barcodes, 2D barcodes were also capable of encoding alphanumeric data. Examples of 2D barcodes include Quick Response (QR), PDF417, Micro PDF417, Code 49, and DataMatrix codes. EX1014, p. 2.



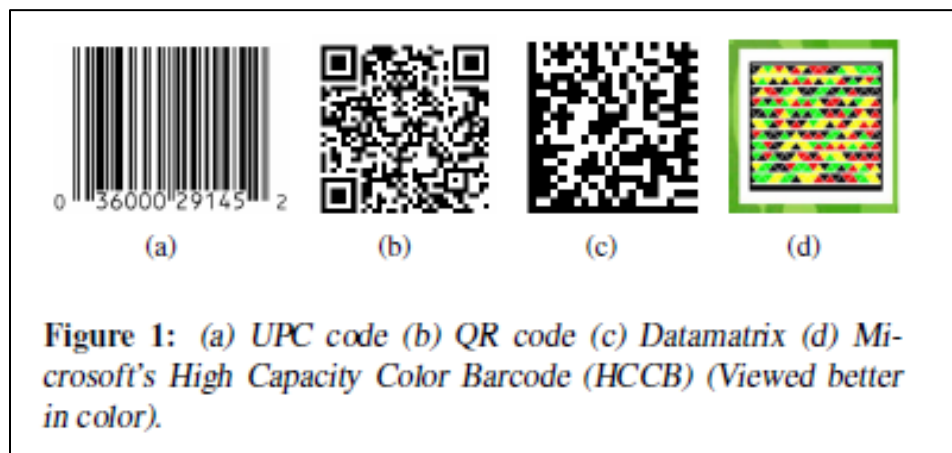
EX1014, 2.

44. 2D barcodes can hold a large amount of information. For instance, QR codes can hold up to 7,089 digits, 4296 letters, and 2953 binary data. EX1014, 2. As the name suggests, they achieve this higher data density by encoding data in horizontal and vertical dimensions. There are two general categories of 2D barcodes: stacked barcodes and matrix barcodes. EX1014, 2. For instance, Data Matrix and QR Code are examples of 2D matrix barcodes. In these barcodes, data is encoded in 2D “cells” depending on the color of the cell, for instance, with dark (black) cells representing 1’s and light cells representing 0’s. EX1015, 47-48; EX1016, ¶21.

2. Color coded barcodes were known

45. As I explained above, increasing the data density of barcodes has been a continuing goal in the field of barcodes. One way of doing this is to encode data

using multiple colors. 2D color barcodes hold much more information in the same physical size as a black-and-white barcode. For instance, Microsoft introduced a High Capacity Color Barcode (HCCB) in 2007 and commercialized it in its “Microsoft Tag” product. EX1017, 1; EX1018, 806. An HCCB has rows of strings of symbols (triangles) that can be one of four colors, such as black, red, green and yellow, each of which encodes different data. EX1017, 1; EX1018, 806.



EX1017, FIG. 1.

46. Using different colored symbols enables each symbol to encode more data. EX1018, 807; EX1019, 710. For instance, where black-and-white barcodes encode one bit per symbol (either 0 or 1), a color barcode having four colors can represent two bits per symbol (00, 01, 10, or 11). This doubles the data density compared to black-and-white barcodes. Similarly, an 8-color barcode encodes three bits per symbol (000, 001, 010, etc.), which triples the data density compared to black-and-white barcodes. This allows the same amount of information to be represented in fewer symbols and thus allows the physical size of the barcode to be

smaller.

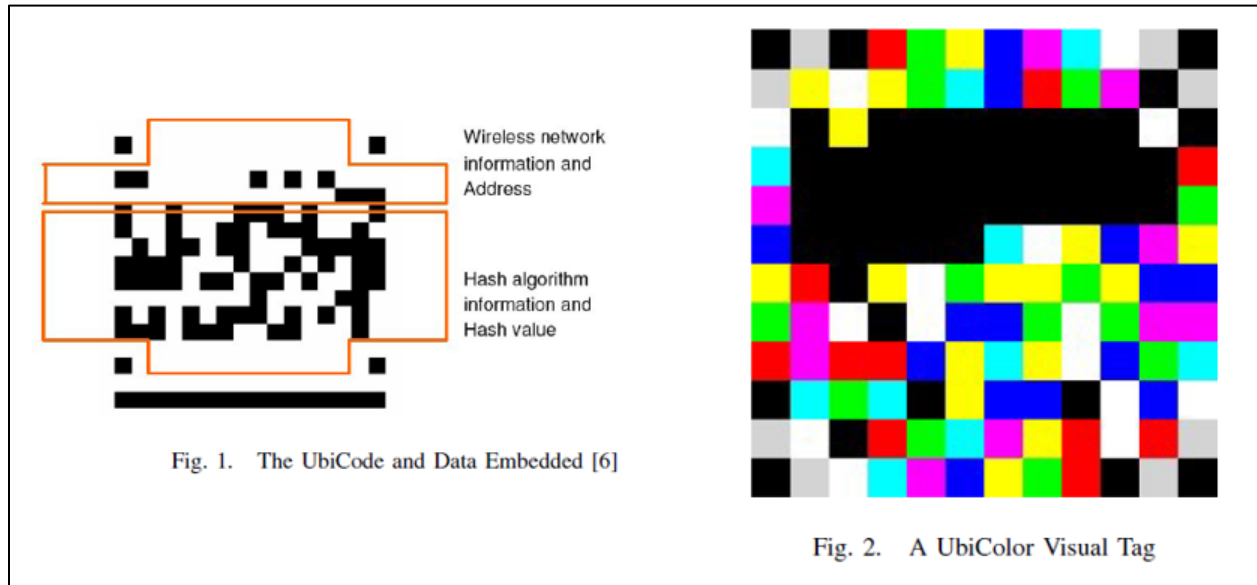
47. In 2011, Microsoft's HCCB was perhaps the best-known color coded barcode, but other color-coded barcodes were known. For instance, the Color Bar Code System from Imageid Ltd. and ColorCode from Colorzip Media were two other types of commercialized color-coded barcodes. EX1018, 808; EX1019, 710. Others proposed similar color-coded barcodes in academic literature. *See generally, e.g.,* EX1017; EX1018; EX1019.

3. Barcodes were used to encode wireless pairing information

48. As I explained above, by 2011, the use of barcodes was widespread to encode many different types of information across many industries. One such known use case for barcodes was to encode information used for establishing wireless communication links between devices.

49. One such solution, called UbiCode, used black-and-white barcode images called "visual tags" to encode a network address and a hash of a public key. EX1020, 173. The visual tag was displayed on one device and captured by the other using a digital camera. EX1020, 173. Using the information contained in the visual tag, secure communication could be established. EX1020, 1. Another solution, called UbiColor, extended UbiCode to use color coded barcodes. EX1020, 173, 175. The use of color-coded barcodes in UbiColor allowed "each region of the visual tag to convey more information within the same space,

allowing for a significant reduction in the number of regions needed to convey the necessary information.” EX1020, 173. This made it easier for the reading device (camera) to recognize and extract information. EX1020, 173.

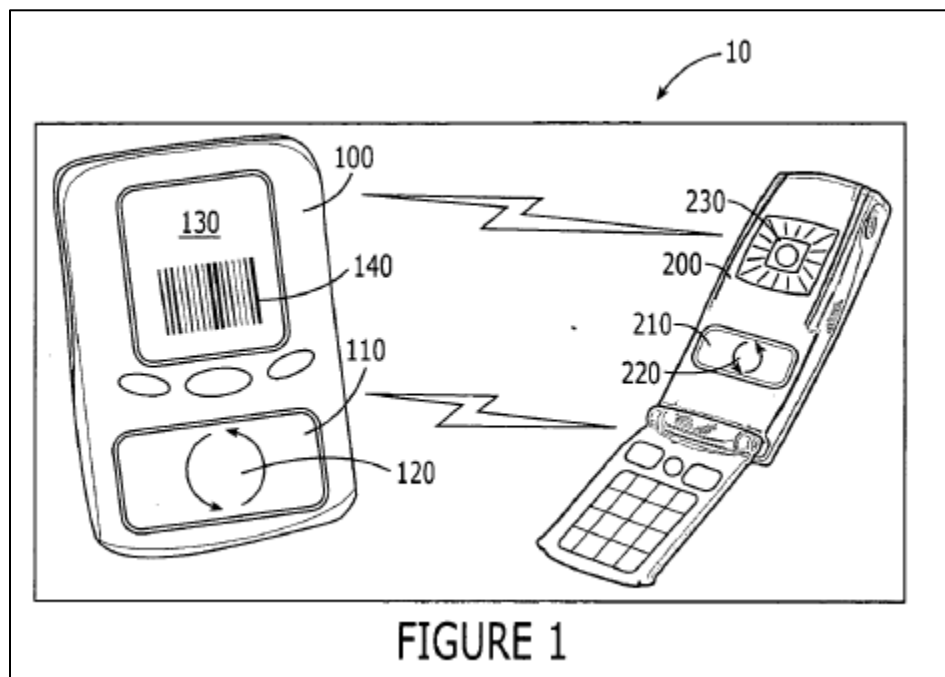


EX1020, FIGs. 1-2.

50. Numerous patents also disclosed techniques for using barcodes, including color-coded barcodes, to establish wireless communication links. For instance, as I explain below, the prior art references asserted herein, including Brown, Bishop, Williams, and Ort, teach techniques for encoding wireless pairing information in barcodes and scanning these barcodes to set up wireless communication links.

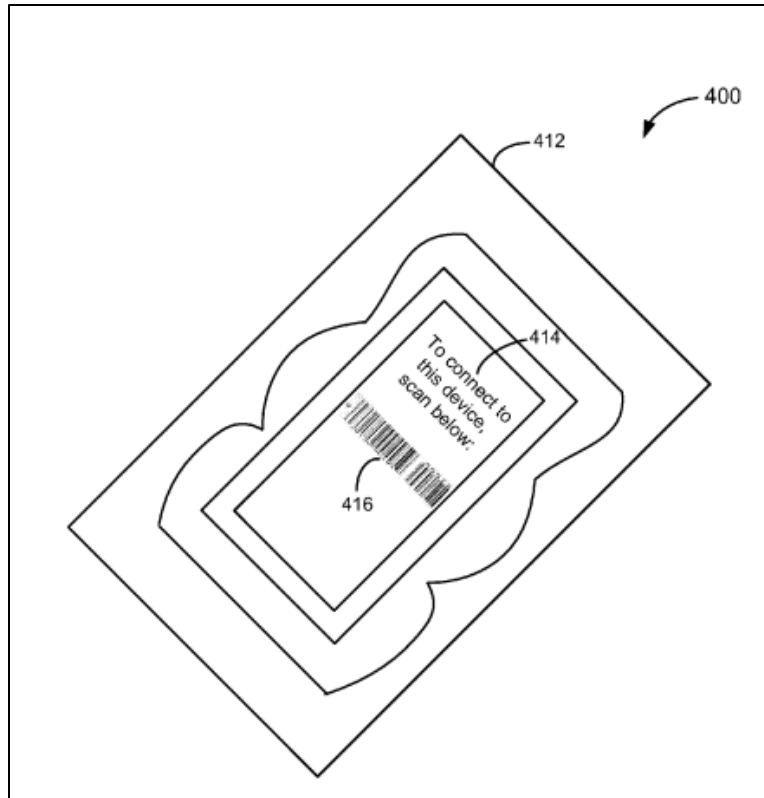
51. As another example, Anttila, filed in 2003, teaches techniques for “establishing a short-range communication link between digital devices for the purpose of transferring data between the devices.” EX1023, Abstract. “The first

device generates and displays a visual code that encodes the address of the first device and the location of data element desired to be transferred.” EX1023, Abstract. The visual code is a barcode that includes a “terminal address of the first [] device and a data identifier for the selected data element” to be transferred. EX1023, ¶28. The “terminal address may be a Bluetooth® device address, an Internet Protocol (IP) address, a Uniform Resource Locator (URL) or the like.” EX1023, ¶28. “A second device, which implements image capture capability, captures the visual code and decodes such to determine the address of the first device and the location of the data element.” EX1023, Abstract. “Upon decoding, the second device will automatically initiate the short-range communication link between the first and second digital devices and the transfer of the data element from the first device to the second device will ensue.” EX1023, Abstract.



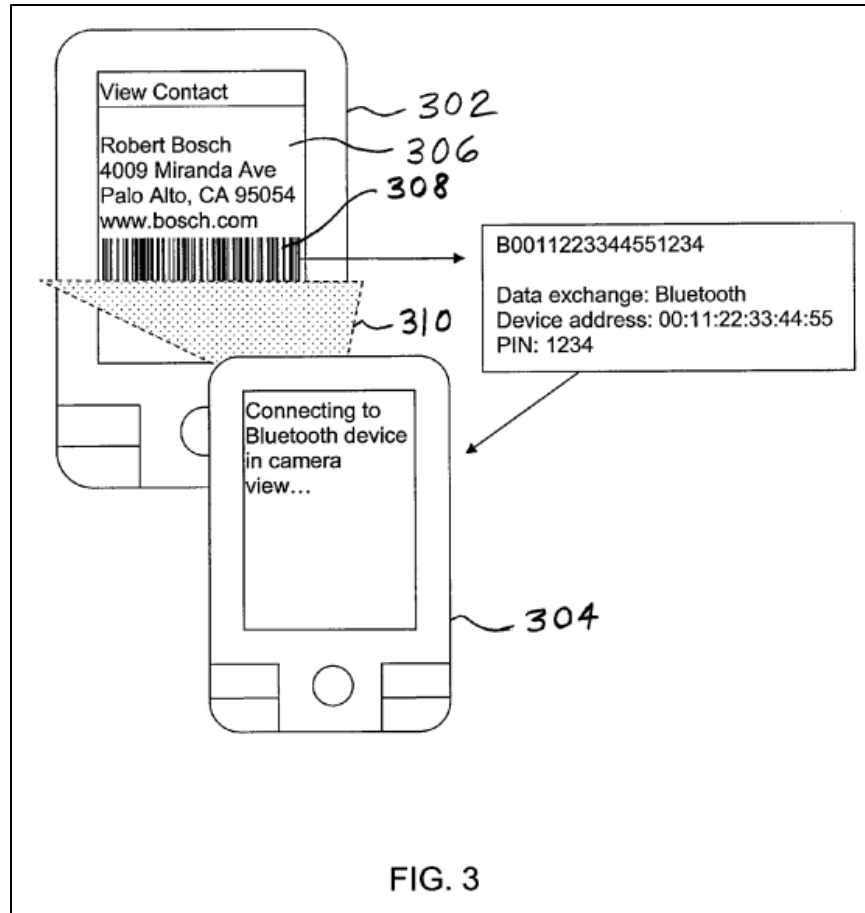
EX1023, FIG. 1.

52. Kovitz similarly teaches “automatic device connection or pairing” using barcodes. EX1021, 3:20-33. “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, among other things, “network addresses” of the devices to be paired, such as MAC addresses, BSSIDs, Bluetooth addresses, IP addresses, etc., depending on the protocol used. EX1021, 6:50-58, 12:9-15.



EX1021, FIG. 4C.

53. Faenger similarly teaches a process for “pairing... devices and authorizing a data exchange” using “visual tags” in the form of barcodes. EX1022, ¶40. For instance, a first device encodes a Bluetooth address and personal identification number (PIN) in a barcode, and a second device captures an image of the barcode to facilitate Bluetooth pairing. EX1022, ¶67-68.



EX1022, FIG. 3.

54. Thus, using barcodes to encode wireless pairing data for establishing wireless communications was well known before the priority date of the '394 patent. Indeed, with the rise of mobile devices that included image capture and wireless networking capabilities, this was a natural use of barcode technology. For instance, these similar processes were efficient because they enabled quick, hassle-free wireless communications, and obviated the need for manual inputs, thus eliminating human error. *See* EX1023, ¶10.

55. Moreover, these processes gave users greater control and knowledge over which devices they paired with. Conventional pairing processes required users

to select a desired device in a long list of discovered nearby devices. Consequently, users were often unsure of the correct device. These barcode pairing processes improved upon this by ensuring that devices paired with the corresponding device that captured the barcode image. EX1023, ¶¶10-11; EX1021, 2:66-3:11.

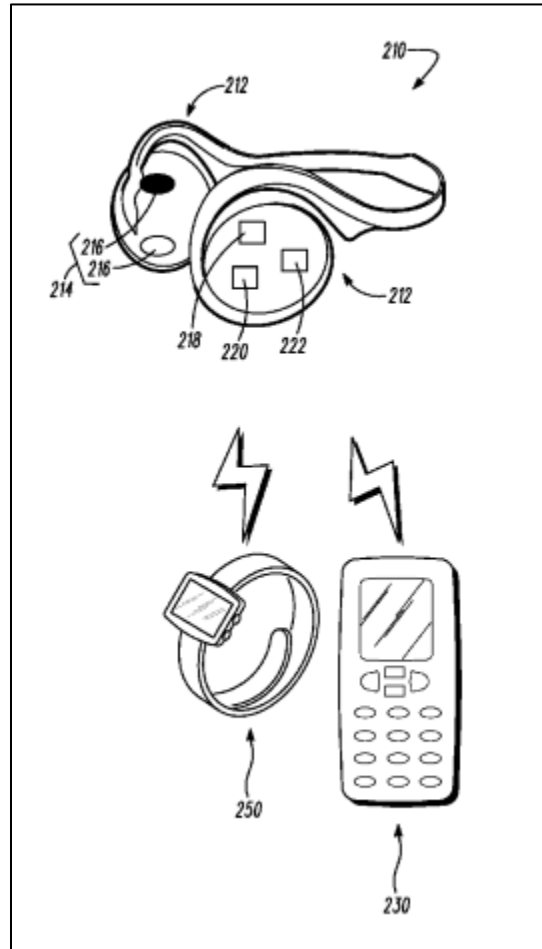
B. Wearable biometric devices were known and used to share information over wireless communication links, and to generate and display barcodes

1. Wearable devices were known to generate biometric data and communicate it over wireless network

56. As I explained above, the '394 patent claims require a wearable activity tracking device to establish a wireless communication link with a mobile device in order to communicate biometric or activity related data to the mobile device. It is my opinion that this was well known before the priority date of the '394 patent. For instance, in addition to the prior art asserted herein, which I describe in detail below, numerous patent references disclosed such systems before the priority date of the '394 patent. Such systems generally fall under two categories: systems for monitoring health, and systems for monitoring athletic performance.

57. For instance, Hong discloses a “multi-functional wireless headset [that includes] a heart rate sensing assembly configured to detect heart rate data of a wearer of the headset, and a wireless communication unit configured to communicate heart rate data” to a mobile device. EX1024, Abstract. The mobile

device is then “configured to display information associated with the sensed heart rate data.” EX1024, ¶54. The wireless communication unit “may be configured to communicate via one or more wireless protocols, such as, for example, Bluetooth, ZigBee, and the like.” EX1024, ¶19.



EX1024, FIG. 2.

58. Moon similarly discloses a “body-worn monitor” that includes a “wrist-worn transceiver 72” that “continuously determines vital signs (e.g. blood pressure, SpO₂, heart rate, respiratory rate, and temperature) and motion-related properties (e.g. posture, arm height, activity level, and degree of motion) for an

ambulatory patient in a hospital.” EX1025, ¶54. The wrist-worn transceiver 72

“wirelessly communicate[s]” with a medical professional’s portable device

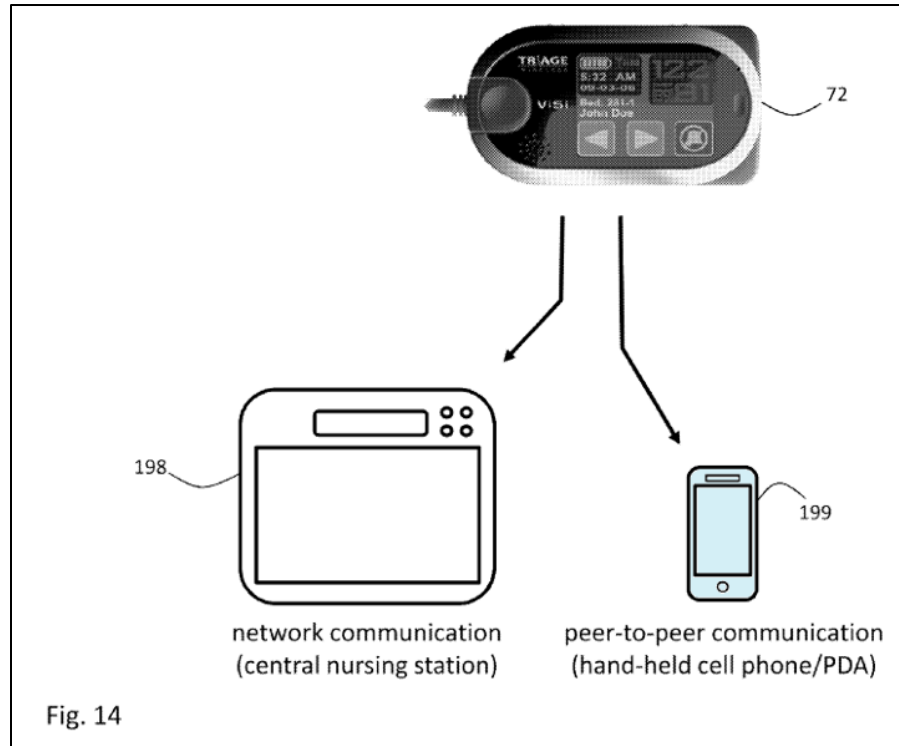
(cellular phone) using “a peer-to-peer communication protocol.” EX1025, ¶109.

For instance, Moon teaches a process that “‘pairs’ the portable device with the

patient’s wrist-worn transceiver” so that “the transceiver [can send] information for

the particular patient to the portable device [], which then displays it for the

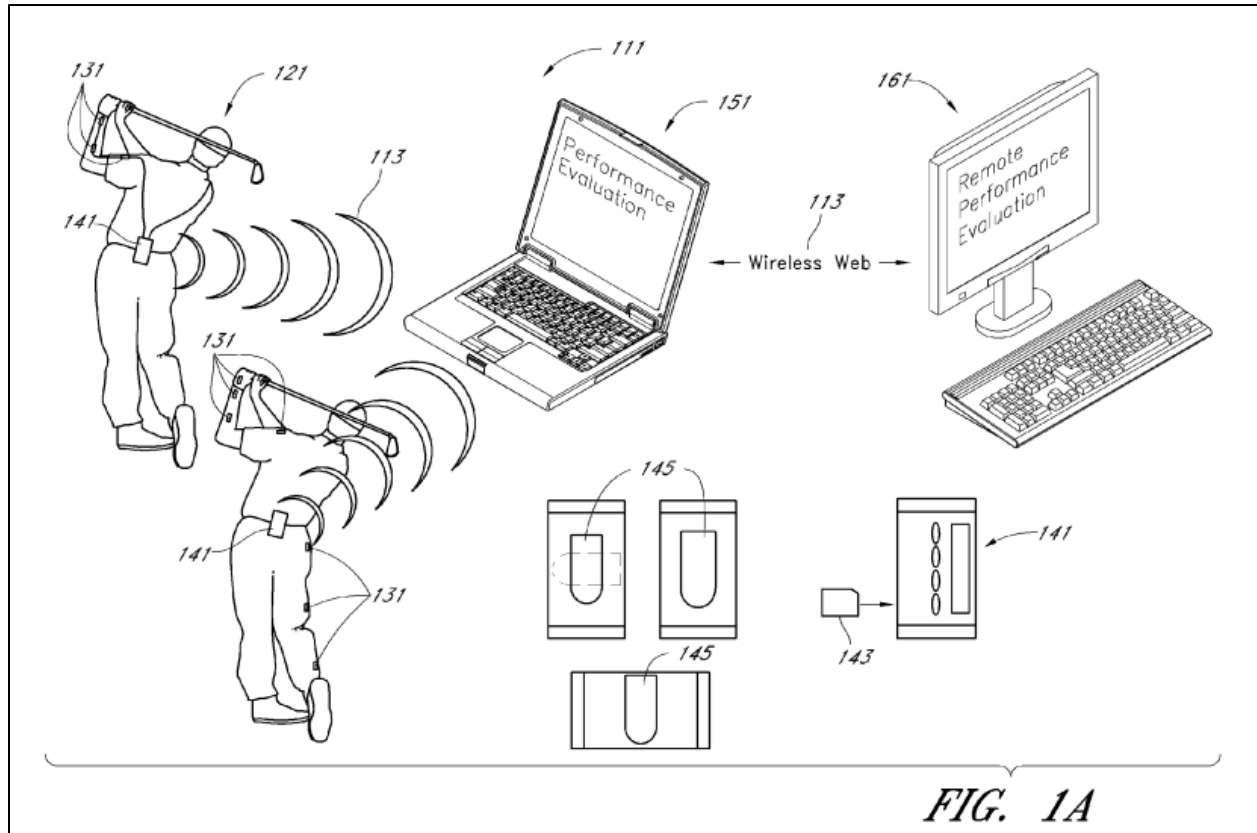
medical professional.” EX1025, ¶109.



EX1025, FIG. 14 (annotated).

59. As yet another example, Stirling teaches techniques for “measuring and analyzing movements of a body and for communicating information related to such body movements over a network.” EX1026, Abstract. In particular, Stirling

discloses a “body movement sensor system” that “gather[s] data relating to positions and movements of various body parts, such as those movements performed in sports activities.” EX1025, ¶¶71. The system transmits such data over a wireless connection (e.g., Bluetooth, TCP/IP, 802.11b, 802.11a, 802.11g, 802.11e, etc.) to, for instance, the user’s cell phone so that “a user can perceive the data (e.g., in the form of a graphic representation, histogram, and/or listing of numerical parameters) and evaluate the movement.” EX1025, ¶¶71, 79.

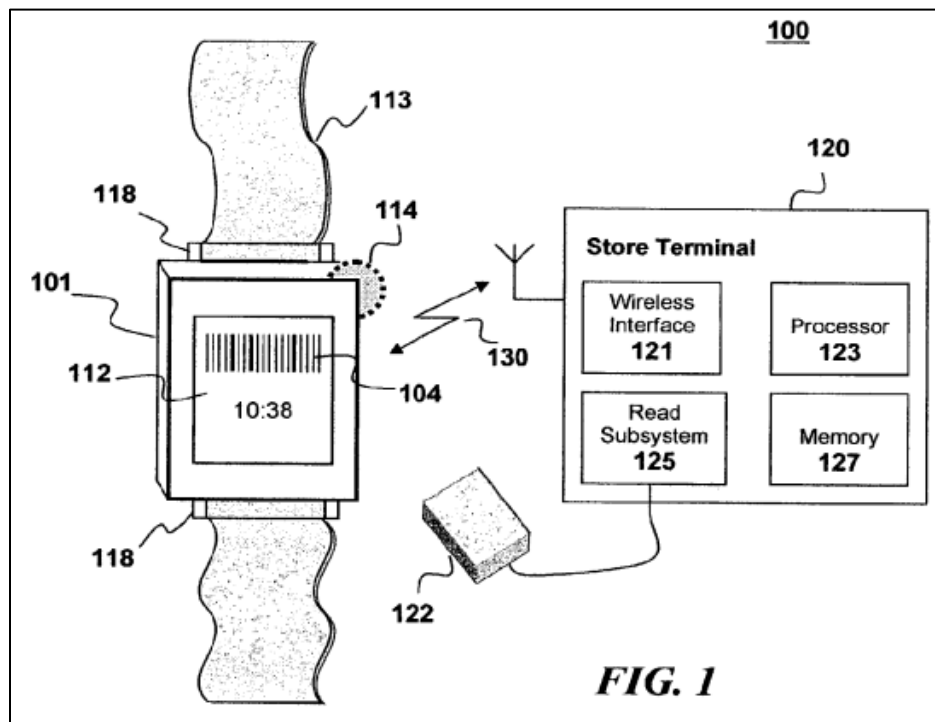


EX1025, FIG. 1A.

2. Wearable devices were known to include user interfaces for generating and displaying data, including barcodes encoding information

60. Before the priority date of the '394 patent, wearable devices were also

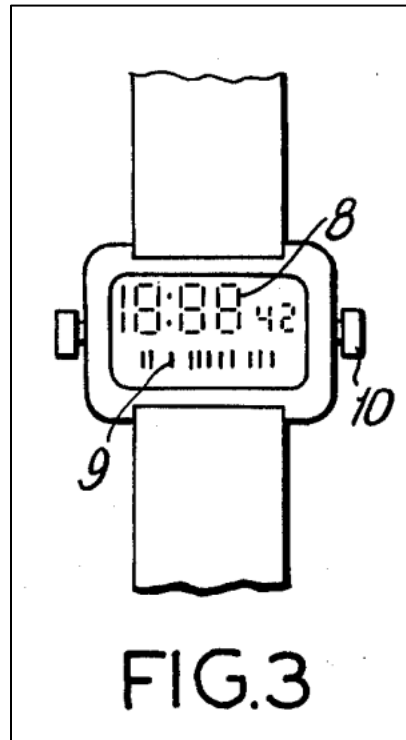
used to generate and display information via user interfaces presented on digital displays. For instance, wearable devices were configured to generate barcodes encoding various types of information. For instance, Narayanaswami discloses a “Portable Shopping Device (PSD)” is implemented as a “wrist watch” with a “high definition display” configured to “convey a large amount of information on a screen using a 2D barcode.” EX1010, ¶¶38, 49. In particular, the PSD is configured to “encode[] a payment message and shopper’s certificate, preferably as a 2-dimensional bar code 104 for display on the PSD 101 display screen 112.” EX1010, ¶49. A sales clerk at the store scans the barcode to verify the purchase. EX1010, ¶52.



EX1010, FIG. 1.

61. As another example, Crutcher discloses a “timepiece” having an

“electro-optic display” that displays a “bar code” that encodes “identification code” “information in a binary coded machine-readable format.” EX1011, 2:58-63, 3:51-53, 9:19-21.



EX1011, FIG. 3.

VII. OVERVIEW OF THE '394 PATENT

62. The '394 patent is titled “Barcode Generation And Implementation Method And System For Processing Information.” EX1001, Title. The '394 patent teaches a “general system 100 for obtaining, communicating and processing information via a barcode.” EX1001, 3:60-66. 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.*, 4:9-24. The

mobile device then “scan[s] the barcode... processes the barcode data and if necessary, operates in response to the barcode data.” *Id.*, 4:24-29.

63. In the claims, the data generation device is a *wearable activity tracking 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 activity tracking device. The mobile device then receives and displays *activity related information* or *the bio-metric information* generated by the activity tracking device.

VIII. PROSECUTION HISTORY

64. I have reviewed the prosecution history of the '394 patent and understand that the application that issued as the '394 patent was allowed without rejection. In the Notice of Allowance, the Examiner acknowledged that Brown “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.” EX1002, 185. The Examiner also acknowledged that “[t]he prior art teaches encoding pairing information as color information that is displayed by a color-coding device where a color decoding device decodes the encoded pairing information to establish wireless communication with the color-coding device.” *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.*

65. But as I explained above, and as I further explain below, it was well-known for wearable biometric devices to communicate biometric data to mobile devices via wireless communication links. And as I further explain below, it is my opinion that a POSA would have found it obvious to adapt such systems to establish the wireless communication links by encoding wireless pairing information in barcodes.

IX. LEVEL OF ORDINARY SKILL IN THE ART

66. A person of ordinary skill in the art (POSA) at the time of the '394 patent was filed would have had a bachelor's degree in Computer or Electrical Engineering or equivalent discipline, and approximately two years' experience in telecommunications or computer networking. Additional education could substitute for professional experience, and significant work experience could substitute for formal education.

67. I am well qualified to determine the level of ordinary skill in the art. I am very familiar with the technology of the '394 patent during the August 5, 2011 timeframe. As mentioned above, by 2011, I had obtained a Ph. D. in Computer Science and had acquired extensive experience relating to, for instance, computer networking, distributed systems, multimedia systems, streaming media, and cloud

computing.

X. CLAIM CONSTRUCTION

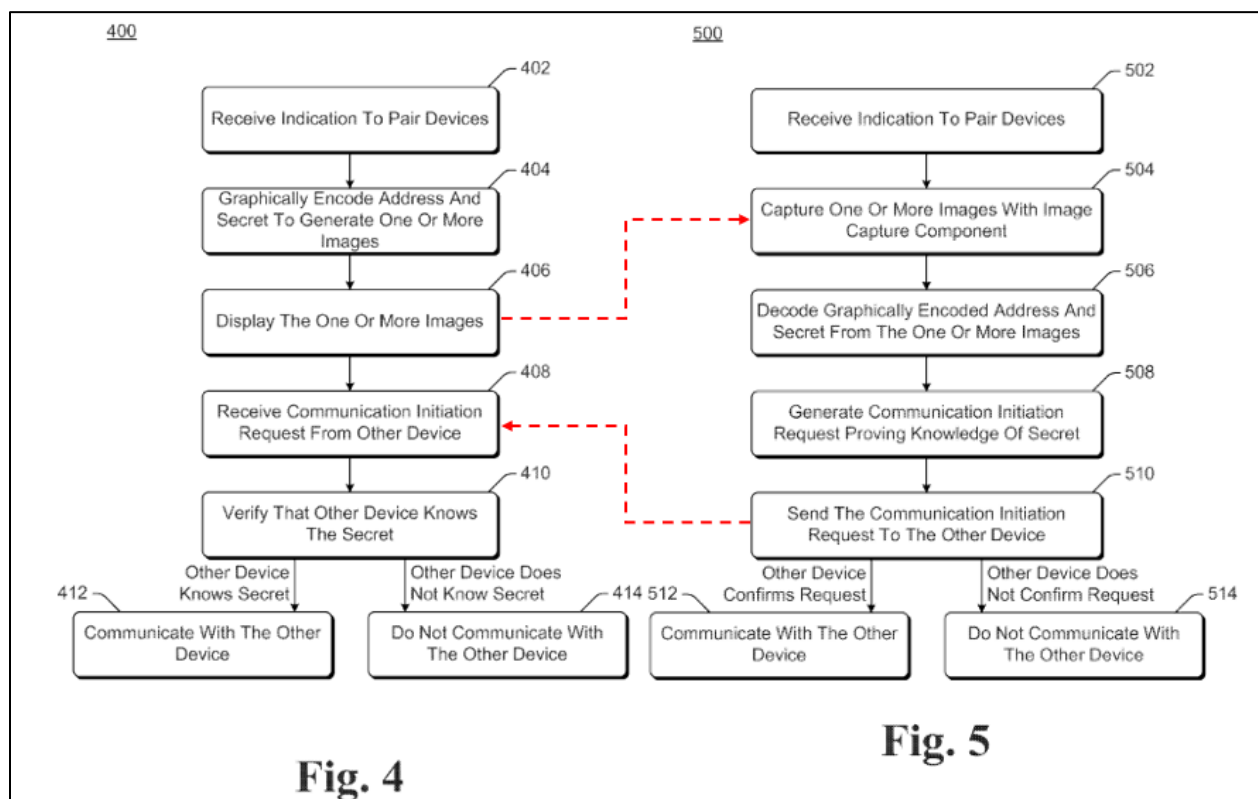
68. I have been informed that the challenged claims of the '394 patent are to be given their plain and ordinary meaning as understood by one of ordinary skill in the art at the time of the invention in light of the specification and the prosecution history pertaining to the patent. Based on my review of the challenged claims, it is my opinion that all claim terms should receive their plain and ordinary meaning in the context of the '394 patent specification. For instance, it is my opinion that the plain and ordinary meaning of the term “color coded” is: “having color other than ‘black-white’ that encodes data.” *See* EX1001, 28:38-65. Moreover, it is my opinion that no other claim terms need to be explicitly construed to render all claims of the '394 patent obvious.

XI. GROUND 1: BISHOP IN VIEW OF LEBOEUF RENDERS OBVIOUS CLAIMS 1-3, 5-8, 11-14, AND 16-18.

A. Overview of Bishop

69. Bishop teaches a technique in which “two devices can be easily paired by a user.” EX1004, ¶57. 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).

70. As shown, Bishop’s device 400 receives an indication (e.g., user request) to “pair devices,” and in response, generates one or more images that graphically encodes “an address of [the] device and a secret.” EX1004, ¶¶60-61. The image can be implemented as an HCCB, such as those I describe above.

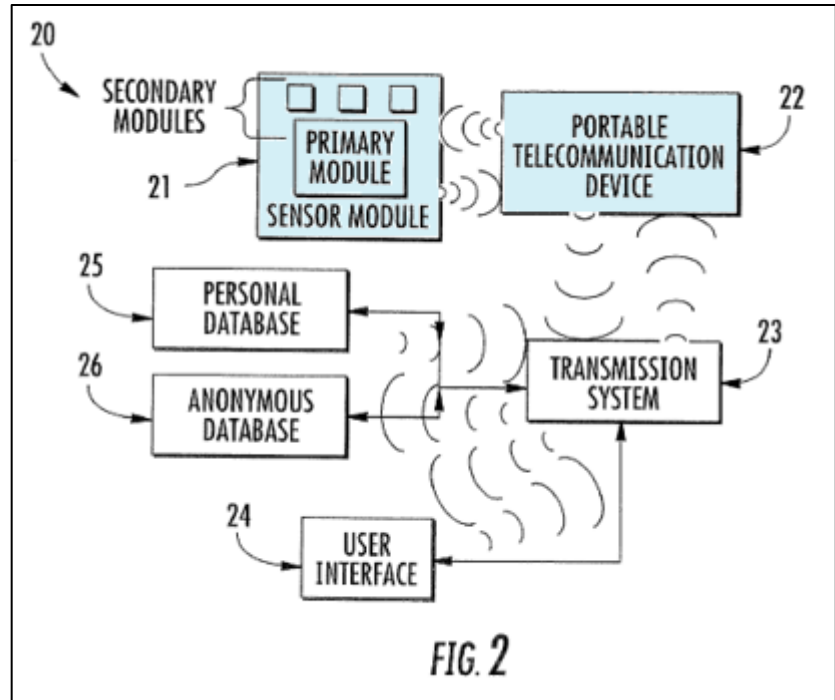
EX1004, ¶23. The device 400 displays the image so that the device 500 can capture the image. EX1004, ¶¶62, 69. The device 500 then decodes the “graphically encoded data” from the image and provides a “communication initiation request” to the device 400. EX1004, ¶70. The request is addressed to the device 400 using the address decoded from the image and includes the secret “to prove that device [500] has knowledge of the secret.” EX1004, ¶¶40, 70-71. Upon receiving the request, the device 400 “verifies that the device [500] knows the secret” and then “proceed[s] with communicating with that other device.” EX1004, ¶¶63-64.

71. Bishop’s pairing process is not particular to a specific network but can be used for “variety of different networks.” EX1004, ¶18. The devices can implement different types of graphically encoded information depending on the network. For instance, the address used to identify the requesting device “can vary based on the protocol used by communication network 108.” EX1004, ¶24. Because the address “identifies device 102 on communication network 108,” and enables “other devices on network 108 can send messages to device 102,” a POSA would have readily understood the types of addresses to be used to establish wireless communication links over different known networks. EX1004, ¶18. A POSA would have also understood how to use these addresses to pair the devices based on Bishop’s teachings.

B. Overview of LeBoeuf

72. LeBoeuf teaches techniques for “monitoring various physiological and environmental factors.” EX1005, Abstract. It discloses a “wearable monitoring device”¹ that implements “at least one physiological sensor 11.” EX1005, ¶79. The device can be implemented, for instance, as a variety of wearable devices, such as an “earpiece” or a “wrist-watch, belt, article of clothing, necklace,” etc. EX1005, ¶141. Using the sensors, the wearable monitoring device “monitor[s] the physiological functioning of the body, such as, but not limited to... heart rate, pulse rate, breathing rate, blood flow, heartbeat signatures,” etc. EX1005, ¶80.

¹ LeBoeuf uses the terms “wearable monitoring device” and “sensor module” interchangeably. EX1005, ¶99.



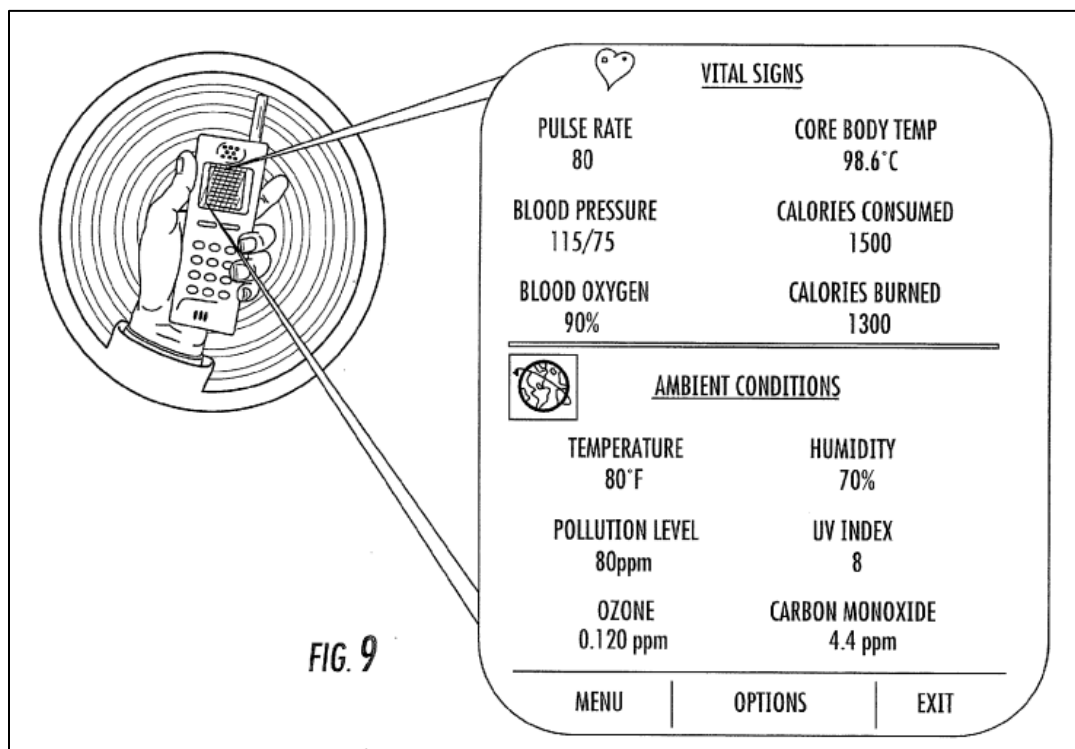
EX1005, FIG. 2 (annotated).

73. 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.

74. In particular, sensor data from the wearable monitoring device can be “stored, analyzed, summarized, and displayed on the portable telecommunication device 22.” EX1005, ¶102. “For example, charts relating health and environment, as well as real-time biofeedback and the like, can be displayed” on the device.

EX1005, ¶102. The sensor data is “measur[ed] and transmit[ed]... in real-time” to enable the user to view such health parameters in real-time or “over a duration of time.” EX1005, ¶85, *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, such as charts.”), 77 (“performing near-real-time personal health and environmental monitoring”).

Figure 9 shows an example interface for displaying such sensor data on the portable telecommunications device (e.g., cell phone).



EX1005, FIG. 9.

75. The wearable monitoring device can send data to the portable telecommunication device in “[r]aw or processed” form. EX1005, ¶141. For instance, the wearable monitoring device may implement “algorithms for

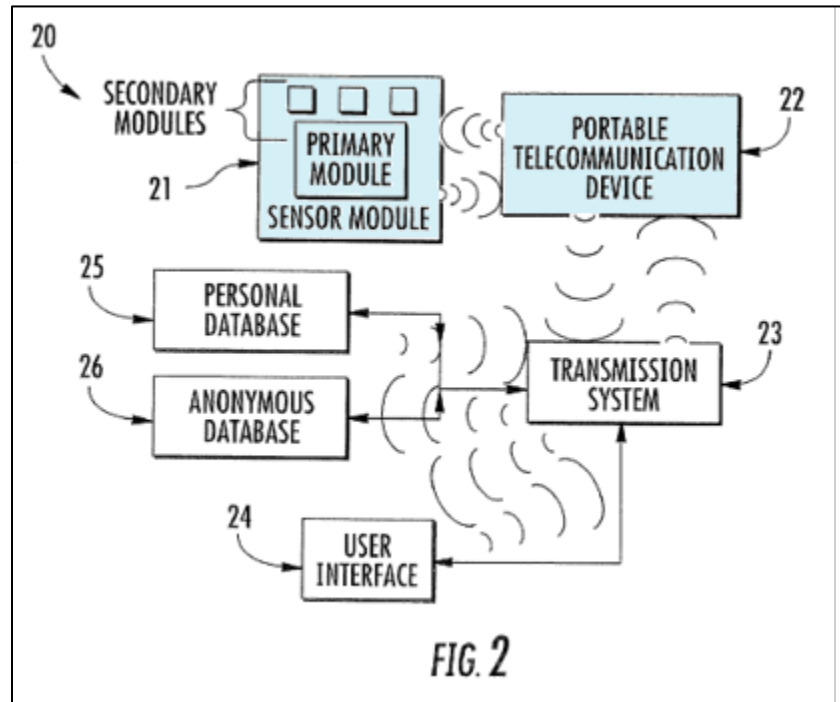
processing personal health and environmental data, diagnosing medical conditions, assessing health states, and the like.” EX1005, ¶113, *see also* ¶11 (“physiological information... may be analyzed locally via the monitoring device”). In such implementations, the wearable monitoring device collects raw sensor data and processes it based on such algorithms. EX1005, ¶113.

76. In some implementations, the wearable monitoring device includes algorithms for “combining information from various sensors 11, 12 into a meaningful real-time personal health and environmental exposure assessment.” EX1005, ¶129. Such algorithms are used to “convert the raw sensor data (from one or more sensors) into a meaningful assessment for the user... without the need for processing in the telecommunication device 22.” EX1005, ¶129. “The output from these algorithms can be viewed as charts, graphs, figures, photos, or other formats for the user to view and analyze.” EX1005, ¶129. “Preferably, these formats display various health factors over time with respect to a particular environment, with health factor intensity on the dependent axis and time or environmental factor intensity on the independent axis.” EX1005, ¶129.

C. Motivation to Combine

77. A POSA would have found it obvious to combine Bishop and LeBoeuf to arrive at the claims of the ’394 patent. As I explained above, LeBoeuf’s wearable monitoring device is configured to “communicate[] wirelessly

with the portable telecommunication device 22, preferably in an open architecture configuration, such as Bluetooth® or ZigBee.” 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).

78. A POSA would have sought to minimize the difficulties in wirelessly pairing LeBoeuf’s devices. As I explained above, conventional wireless pairing processes required users to “manually select a desired second [] device to pair with from a menu or list of available [] devices in range of the first [] device.” EX1021, 2:25-28, *see also* 2:66-3:1 (“[M]anual intervention may be required to pair Bluetooth devices or connect to an AP, particularly when connecting for the first time.”); *see also* EX1023, ¶8 (“This type of manual input of data is inefficient and

is prone to human error.”); EX1006, ¶42 (“[T]here may be many discoverable devices within range, requiring a user to select the desired device from a long list.”). In such implementations, users may select and thereby attempt to pair with the wrong device. EX1021, 3:1-11. A POSA would have recognized this and would have sought to implement an intuitive and user-friendly pairing process for LeBoeuf’s devices.

79. This would have led a POSA to Bishop, which discloses a technique in which “two devices can be easily paired by a user.” EX1004, ¶57. Bishop sought to improve upon conventional pairing processes, which were “cumbersome,” and required “numerous settings or other configuration changes [to be] made by the users of the devices.” EX1004, ¶¶1, 57. As I explained above, Bishop thus describes a technique in which “two devices can be easily paired” using “graphically encoded data” such as a barcode that stores information needed to establish communications between the two devices. EX1004, ¶57.

80. A POSA would have found it obvious to adapt LeBoeuf’s devices to establish a wireless communication link using Bishop’s pairing process. Bishop provides motivation for this combination by teaching that its technique avoids the “cumbersome processes for configuring the devices to be able to communicate” found in conventional pairing processes. EX1004, ¶57. Indeed, such conventional processes could be “time consuming and cumbersome on the part of the user,

reducing the user friendliness of the devices.” EX1004, ¶1. Bishop’s process, on the other hand, 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.

81. This is consistent with my explanation above. It was known that wireless pairing of devices could be unintuitive and inefficient in part due to the need for manual intervention by the user. A POSA would have recognized the utility of Bishop’s process and 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. Indeed, a POSA would have recognized that Bishop’s barcode pairing process simplifies the pairing process and provides a straight-forward, intuitive manner of selecting devices with which to pair.

82. Bishop’s process also provides strong security through use of its “shared secret.” EX1004, ¶40. In particular, 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, 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. That is, for a second device to know a first device’s secret, it must have scanned the first device’s barcode. Ensuring that devices are

only able to pair in this manner prevents “malicious device[s]” from “provid[ing] a verifiable communication initiation request to [the first device] claiming to be [the second device] because such a malicious device would not have the secret that was encoded in the displayed image.” EX1004, ¶45. Bishop’s process thus enables users to ensure that the devices being paired are the correct devices, and not malicious actors.

83. A POSA would have thus been further motivated to combine Bishop and LeBoeuf to implement a *secure* pairing process. This is particularly so because LeBoeuf’s wearable monitoring device collects “personal and private [] information” regarding user health. EX1005, ¶17. A POSA would have thus recognized the importance of a secure pairing process in LeBoeuf to prevent malicious actors from pairing with the monitoring device to obtain such information. Bishop provides such security by giving users complete control over which devices are to be paired and ensuring that only devices with knowledge of the secret can be paired.

84. The combination of Bishop and LeBoeuf thus teaches a wearable monitoring device that generates and communicates biometric and activity-related data to a mobile device over a wireless communications link established by a pairing process initiated by encoding pairing information in a barcode. *See, e.g.*, EX1004, ¶12; EX1005, ¶¶79, 102. In particular, Bishop teaches a wireless pairing

process that establishes a wireless communications link between various types of mobile devices. EX1004, ¶¶12, 57-58. Once this communications link is established, the devices can communicate data (e.g., “a report, song, or other data”) and/or control data (e.g., “so images or other files from one device can be displayed on another, so that one device can change the operation of the other, and so forth”) to each other over the link. EX1004, ¶58. LeBoeuf teaches a usage scenario for Bishop’s wireless pairing process. For instance, LeBoeuf teaches a wearable monitoring device that senses and generates data related to “basic vital signs” and communicates this data over a wireless communications link (e.g., Bluetooth) to a portable telecommunications device for display by the portable device. EX1005, ¶¶79, 97, 101-102.

85. The combined Bishop-LeBoeuf system would include a monitoring device and mobile device, as taught by the combination of Bishop and LeBoeuf, which would each be adapted to implement Bishop’s communication initiation techniques. For instance, the monitoring device would assume the role of Bishop’s device 102 in the pairing process and would initiate the process by generating and displaying an image of graphically encoded data to establish wireless communications between itself and the portable telecommunication device. The mobile device would assume the role of Bishop’s device 104 and would be configured to capture the displayed image and to generate and send a

communication initiation request to the monitoring device. The devices would then each be configured to establish the wireless communication link based on the combined teachings of Bishop and LeBeouf. For instance, the device pairing process would be used to implement LeBoeuf's wireless communication link, such as using the Bluetooth, ZigBee, or Wi-Fi protocols taught by LeBoeuf. EX1005, ¶¶5, 58, 101.

86. To this end, the monitoring device would be adapted as necessary to implement hardware and software to generate and display graphically encoded data, as taught by the combination of Bishop and Leboeuf. Similarly, the mobile device would be adapted as necessary to implement hardware and software to capture an image of an decode the graphically encoded data, and to generate a communication initiation request for establishing the wireless communication link, as also taught by the combination of Bishop and LeBoeuf. For instance, a POSA would have found it obvious to adapt LeBoeuf's devices to implement componentry taught by Bishop, such as the "device pairing module," "screen," "image capture component," "processors or processing units," and "memory and/or storage components" to the extent necessary for implementing the pairing process. *See* EX1004, ¶¶20, 24, 31, 59, 73-74, 76. Such implementations would merely amount to a simple substitution of known elements into LeBoeuf's devices in a known manner to achieve predictable results. That is, the resulting devices would

be configured to implement Bishop's pairing processes to establish a wireless communications link, and to share biometric and activity-related data over that link.

87. A POSA would have had a reasonable expectation of success in combining the references in this manner. For instance, Bishop explains that its techniques are "platform-independent, meaning that the techniques can be implemented on a variety of commercial computing platforms having a variety of processors." In particular, Bishop's techniques can be implemented using "a variety of different types of devices," even on "low-resource device[s] with limited memory and/or processing resources." EX1004, ¶15. Bishop's technique applies to "various usage scenarios," and can be implemented "[a]nywhere communication between two devices is desired." EX1004, ¶58.

88. Moreover, as I explained above, Bishop's pairing process can be implemented using "a variety of different networks." EX1004, ¶18. Bishop's devices can implement different types of graphically encoded information for pairing, depending on the network. For instance, the address used to identify the requesting device "can vary based on the protocol used by communication network 108." EX1004, ¶24. Because the address "identifies device 102 on communication network 108," and enables "other devices on network 108 can send messages to device 102," a POSA would have readily understood how to implement different

addresses used by different known networks. EX1004, ¶18. A POSA would have also understood how to use these addresses to pair the devices based on Bishop's teachings and known network pairing procedures. For instance, a POSA would have recognized that Bishop's "pairing" technique is applicable to Bluetooth because Bluetooth also implements a "pairing" process. *See, e.g.*, EX1021, 2:4-43 ("Bluetooth uses a process called pairing... to establish wireless connection parameters between two devices."); EX1006, ¶¶41-43. A POSA would have also readily known how to implement Bluetooth pairing procedures in Bishop because Bluetooth was widespread and commonly implemented in mobile devices.

89. For instance, as I explained above, it was well known to use similar barcode pairing processes to establish Bluetooth or other wireless communication links. Like Bishop, such processes encoded the network (e.g., Bluetooth) address of the requesting device in the barcode and used that address to pair the devices in accordance with the known Bluetooth pairing process. *See, e.g.*, Section VI.A.3 *supra* (discussing EX1020-EX1023); *see also* EX1006, ¶¶47 ("the network address of the first device may also be encoded in the barcode"), 49 ("pairing data comprising a Bluetooth address"); EX1009, ¶42 ("pairing message may contain the device address associated with the initiating device").

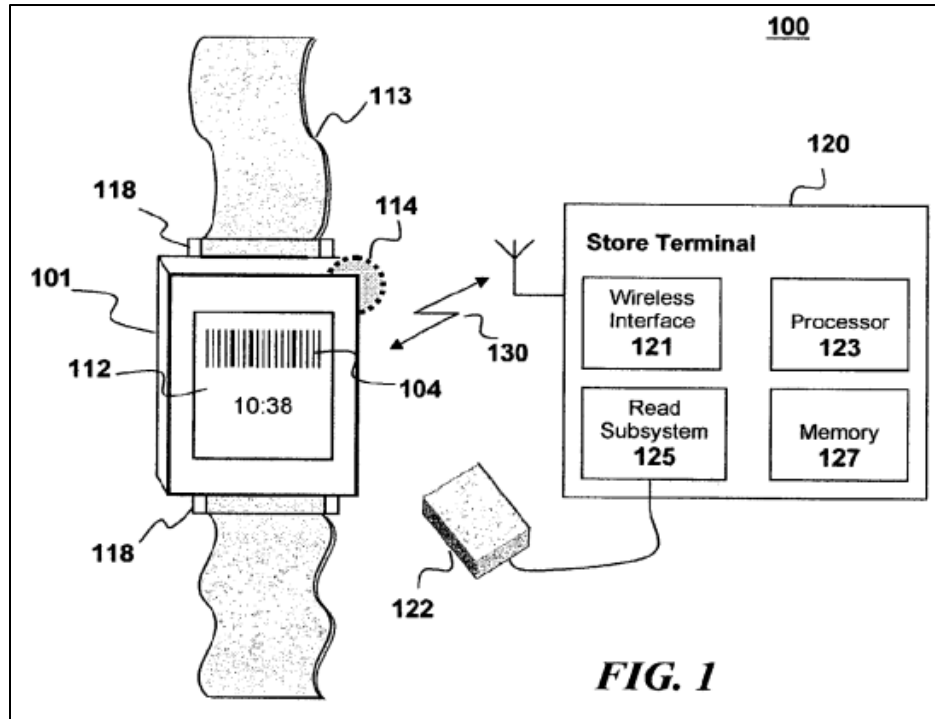
90. Thus, based on the disclosures of Bishop and knowledge of those skilled in the art, it is my opinion that such barcode pairing processes were well

known for establishing wireless communication links in a variety of types of networks. A POSA would have readily recognized that Bishop's pairing process could be used to pair LeBoeuf's devices, and a POSA would have had a reasonable expectation of success in implementing such pairing process between a wearable and mobile device, as taught by LeBoeuf.

91. LeBoeuf also teaches flexibility in the devices used to implement its system. For instance, the 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, another earpiece, or other portable, telemetric device." EX1005, ¶¶101, 141. A POSA would have thus had no problem implementing Bishop's techniques in LeBoeuf's devices because Bishop teaches similar devices, and explains that the barcode pairing process can be implemented by a "low-resource device with limited memory and/or processing resources." EX1004, ¶15. In other words, it is my opinion that Bishop's pairing process was intended for devices like LeBoeuf's.

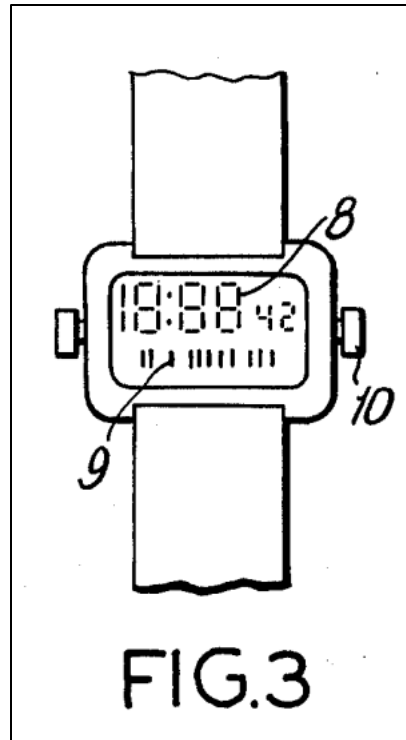
92. For instance, LeBoeuf's wearable monitoring device includes a display in the form of a "visual monitor." EX1005, ¶105. A POSA would have had readily been able to adapt the monitoring device to implement a display that displays graphically encoded data, as taught by Bishop. EX1004, ¶¶23, 30. A

POSA would have also been able to adapt the monitoring device to encode the address and secret in a barcode as taught by Bishop. Indeed, as I explained above in Section XII.B, it was well known for wearable electronic devices, including watches, to generate and display barcodes that encoded information. For instance, Narayanaswami discloses a “Portable Shopping Device (PSD)” is implemented as a “wrist watch” with a “high definition display” configured to “convey a large amount of information on a screen using a 2D barcode.” EX1010, ¶¶38, 49.



EX1010, FIG. 1.

93. In another instance, Crutcher discloses a “timepiece” having an “electro-optic display” that displays a “bar code” that encodes “identification code” “information in a binary coded machine-readable format.” EX1011, 2:58-63, 3:51-53, 9:19-21.



EX1011, FIG. 3.

94. Indeed, a wearable device, such as disclosed by LeBoeuf, is just a certain type of mobile device configured to be attached to or otherwise worn by a user. LeBoeuf discloses many different types of wearable devices. EX1005, ¶141. A POSA would have readily been able to implement a display, such as an LCD display, for displaying barcodes in LeBoeuf's wearable device. For instance, it was well within the skill of a POSA to adapt the size and configuration of such display for displaying barcodes (including color-coded barcodes).

95. Moreover, as I explained above, a POSA would have also readily been able to make any other adaptations in LeBoeuf's devices necessary to implement Bishop's pairing process. For instance, Bishop teaches conventional hardware and software components, such as the device pairing modules, display

screens, processing units, image capture component, and “memory and/or storage components” that configure its devices to implement the pairing process. *See* EX1004, ¶¶20, 24, 31, 59, 73-74, 76. These components are conventional hardware and software elements that are compatible with LeBoeuf’s devices. It was within a POSA’s skill to implement such components as necessary to achieve the predictable result of implementing Bishop’s pairing process.

96. A POSA would have thus recognized that these adaptations would have been straightforward and would be implemented without undue burden. Indeed, as explained, Bishop’s disclosures “support[] 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 a known technique (encoding wireless pairing information in barcodes) to improve similar devices (Bishop and LeBoeuf’s mobile devices) in the same way (to efficiently and securely establish wireless communications).

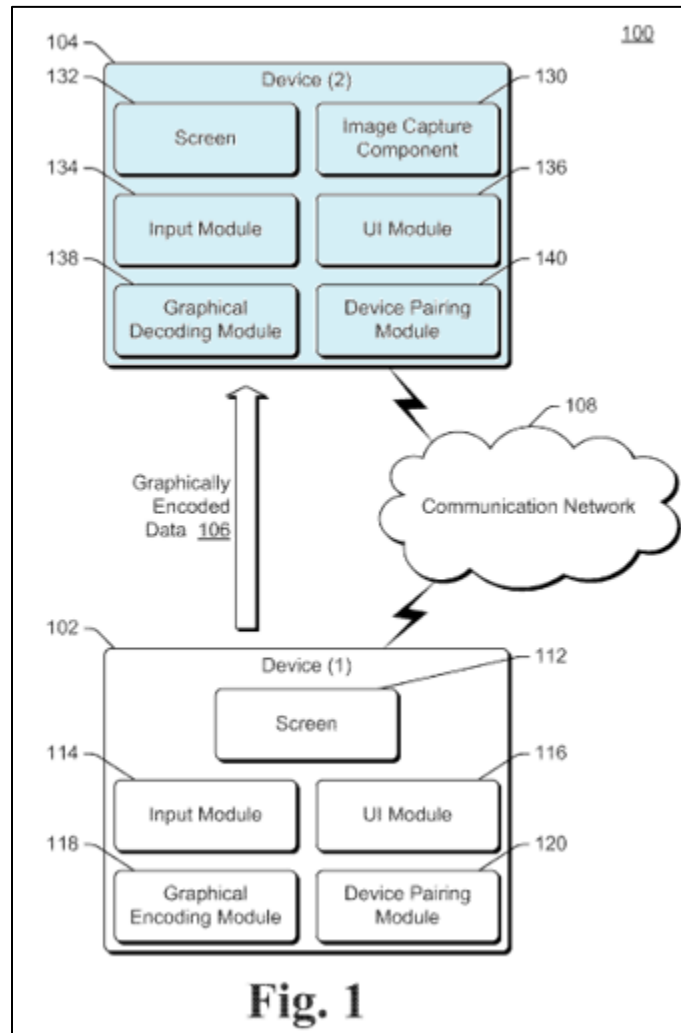
D. Independent Claims

1. Claim 1

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

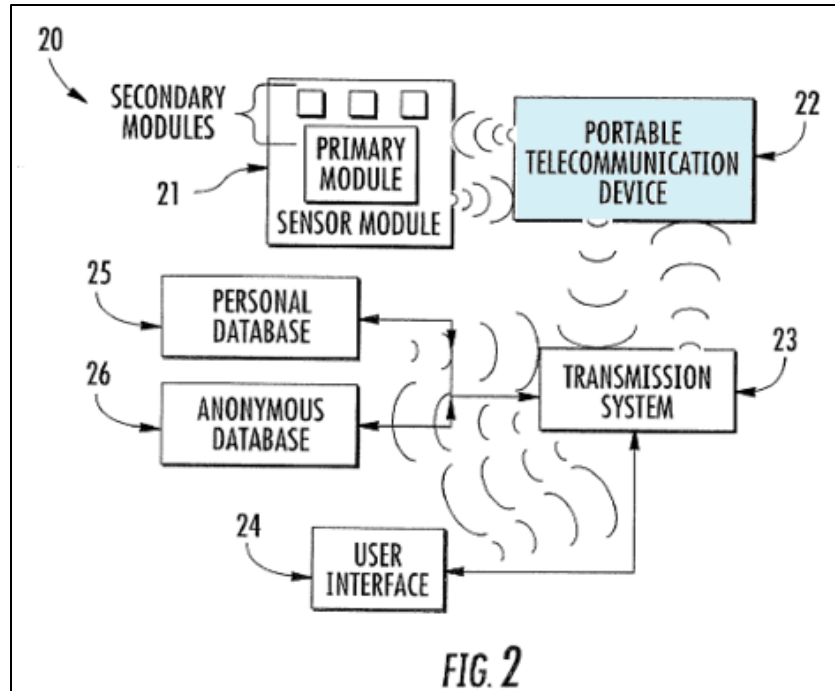
97. Bishop discloses a “device 104” (*mobile device*), which can be, for instance, a “handheld computer,” a “personal digital assistant (PDA),” a “mobile

station,” or a “cellular or other wireless phone.” EX1004, ¶15.



EX1004, FIG. 1 (annotated).

98. LeBoeuf teaches a “portable telecommunication device 22” (*mobile device*), which can be “a cell phone (which includes a ‘smartphone’), PDA, laptop computer, Blackberry,” etc. EX1005, ¶101.



EX1005, FIG. 2 (annotated).

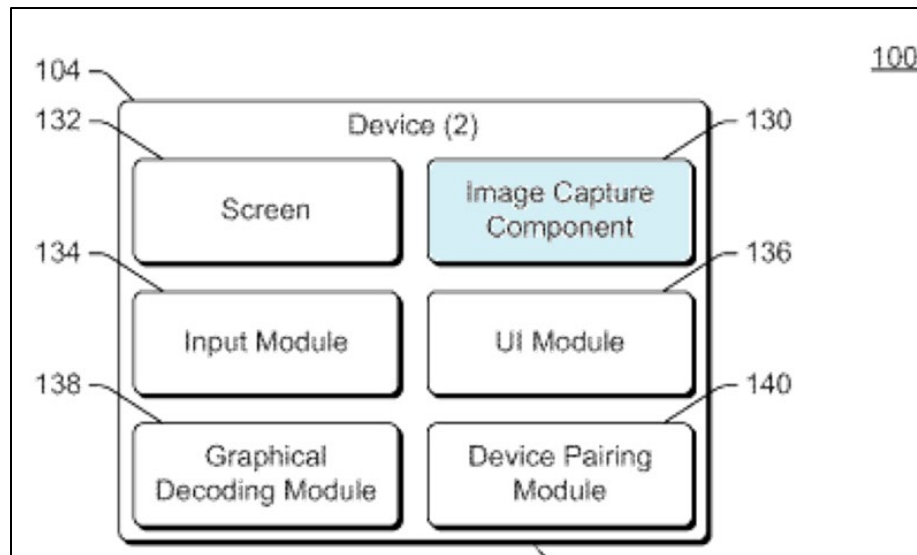
99. As explained in Section XI.C, the combined Bishop-LeBoeuf system includes a mobile device taught by the combination of Bishop (e.g., mobile device 104) and LeBoeuf (e.g., telecommunication device 22) that communicates wirelessly with LeBoeuf’s wearable sensor module 21². As explained below, the combined mobile device teaches the componentry and functionality of the claimed *mobile device*. For instance, the combined mobile device is adapted to implement Bishop’s barcode pairing process to establish a wireless communication link, and also to receive and display biometric and activity related information, as taught by

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

LeBoeuf.

b. [1.1] at least one camera sensor, included within the mobile device;

100. Bishop-LeBoeuf's mobile device 104 includes an internal "image capture component" (*camera sensor*) that "captures images." EX1004, ¶33. The image capture component is "a camera or digital camera" implemented using, for instance, "CCD (charge coupled device) technology, CMOS (complementary metal oxide semiconductor) technology, and so forth." EX1004, ¶33.



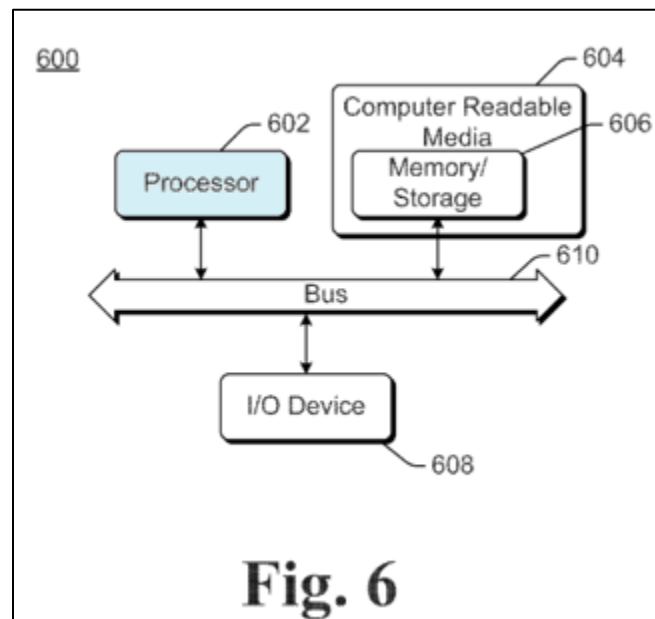
EX1004, FIG. 1 (excerpt, annotated).

101. Thus, it is my opinion that the combination of Bishop and LeBoeuf teaches this element.

c. [1.2] at least one processor in signal communication with the at least one camera sensor;

102. Bishop-LeBoeuf's mobile device 104 includes "one or more processing units 602" that execute "instructions" for implementing the mobile

device's functionality. EX1004, ¶¶74, 76 ("The techniques discussed herein can be implemented in software, with instructions being executed by one or more processing units 602."). These processors cause the image capture component (*camera sensor*) to "capture[] images for use by device 104," and are thus *in signal communication with* the image capture component. EX1004, ¶¶31 (modules for implementing the barcode scanning process are implemented by "one or more instructions that are executed by one or more processors or controllers"), 33, 69, 74. Indeed, the processor instructs the image capture component to capture images, which are then used by the processor to carry out Bishop's pairing process.

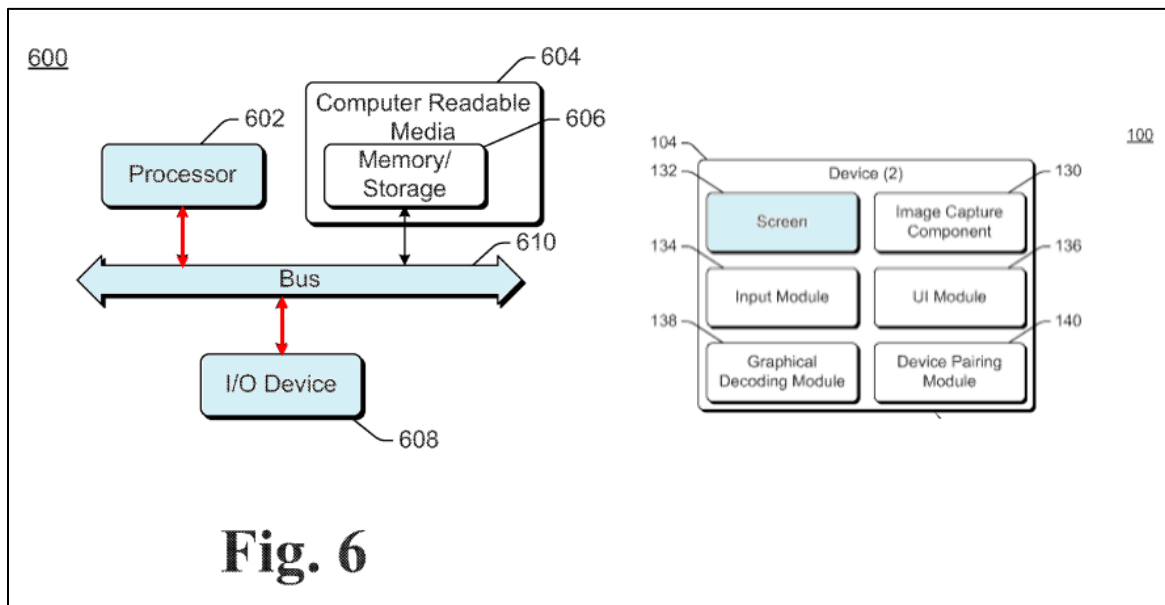


EX1004, FIG. 6 (annotated).

103. Thus, it is my opinion that the combination of Bishop and LeBoeuf teaches this element.

d. [1.3] a display in signal communication with the at least one processor;

104. Bishop-LeBoeuf's mobile device 104 includes a "screen 132," which is a "display component." EX1004, ¶¶20, 31-32. The screen 132 is *in signal communication* with the one or more processing units 602 (*at least one processor*) because the one or more processing units cause the screen to, for instance, display a "user interface." EX1004, ¶¶31 (UI module 136 implemented by "one or more instructions that are executed by one or more processors or controllers"), 32, 74, 77 (I/O devices 608 include a "display device (e.g., a monitor or projector)").



EX1004, FIGs. 6, 1 (excerpt) (annotated).

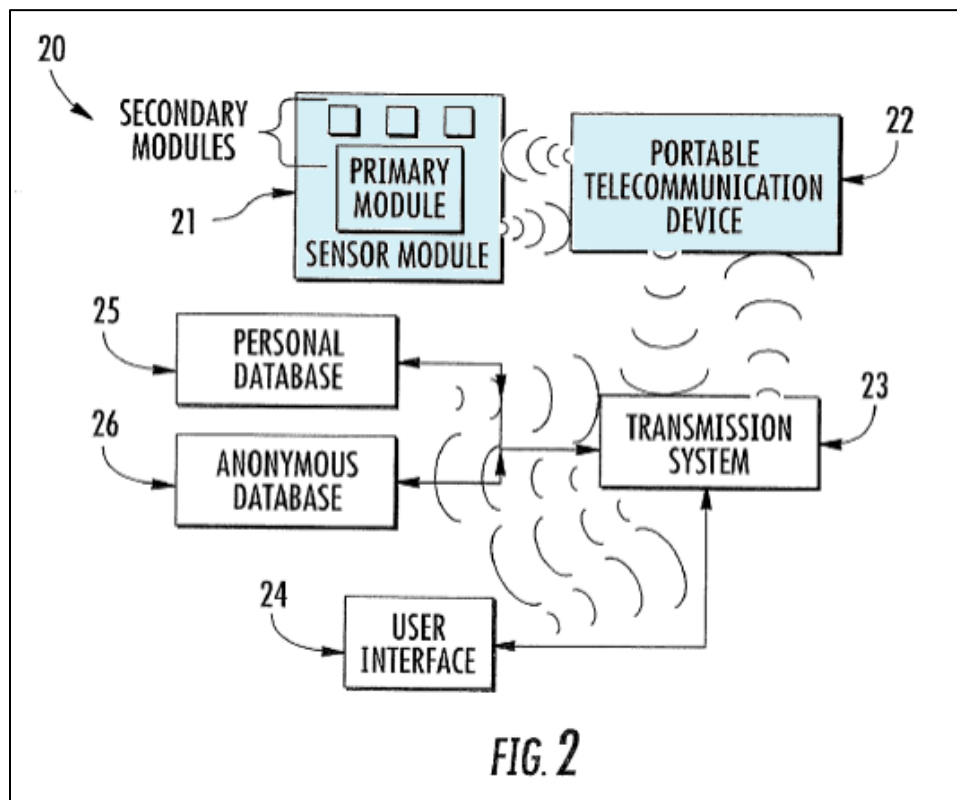
105. Thus, it is my opinion that the combination of Bishop and LeBoeuf teaches this element.

e. **[1.4] communication circuitry configured for wireless communication with an external wearable activity tracking device;**

106. Bishop-LeBoeuf's mobile device 104 includes a "device pairing module 140" that "manages... the pairing or initiation of communication between devices." EX1004, ¶39, *see* ¶¶31, 67, 81. The device 104 also includes "communications [] modules for wirelessly sending data to and/or receiving data from other devices." EX1004, ¶17, *see also* ¶18. Modules in Bishop are implemented as a combination of software and "hardware (e.g., fixed logic circuitry)." EX1004, ¶81. The device 104 also includes a "network card." EX1004, ¶77. Moreover, LeBoeuf's portable telecommunications device includes *communication circuitry* for communicating with the wearable monitoring device using an "open architecture configuration, such as Bluetooth® or ZigBee." EX1005, ¶¶101-02. The combined mobile device thus comprises *communication circuitry* as claimed.

107. As explained in Section XI.C, in the Bishop-LeBoeuf system, the combined mobile device communicates with a wearable monitoring device/sensor module, as taught by LeBoeuf. *See* EX1005, ¶101. The wearable monitoring device is an *external wearable activity tracking device* as claimed because 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. 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. The wearable monitoring device is *wearable* because it is “configured to be worn by a” user, and can be implemented as, for instance, an earpiece or “wrist-watch.” EX1005, ¶¶14, 141.

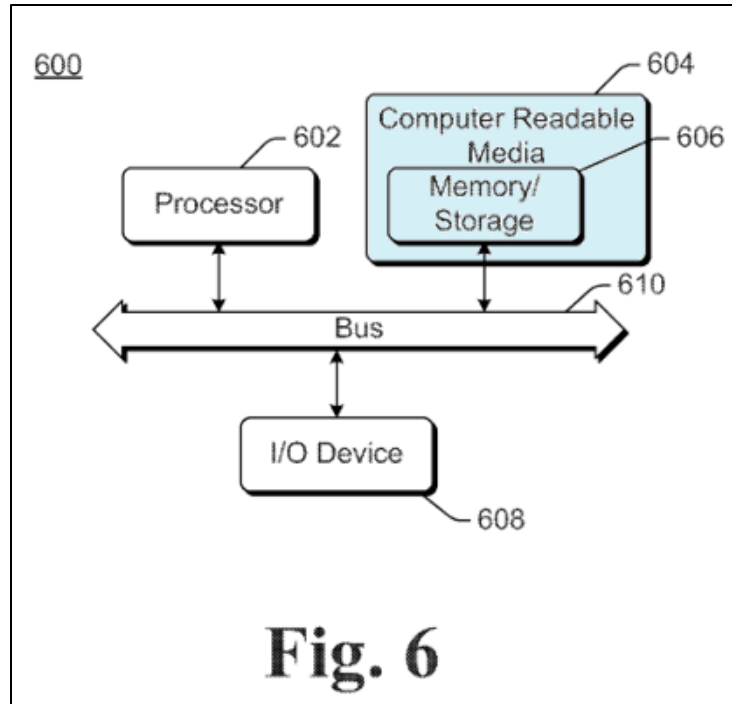


EX1005, FIG. 2 (annotated).

108. In the combined system, the Bishop-LeBoeuf mobile device would wirelessly communicate with the wearable monitoring device via the device pairing module and/or communications modules (*communication circuitry*). Thus, the combination of Bishop and Leboeuf teaches this element.

- f. **[1.5] memory, included within the mobile device, associated with one or more processors and configured to store software instructions, which, when executed by the one or more processors, cause the one or more processors to perform operations comprising;**

109. Bishop-LeBoeuf's mobile device includes "one or more 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, ¶¶31, *see also* ¶¶74, 76, 81 (disclosing "program code that performs specified tasks when executed on a processor (e.g., CPU or CPUs)," and is "stored in one or more computer readable memory devices"). When *executed by the one or more processors* 602 of the device, these *software instructions* cause the processors to implement the claimed wireless pairing process, as described in the following sections.



EX1004, FIG. 6 (annotated).

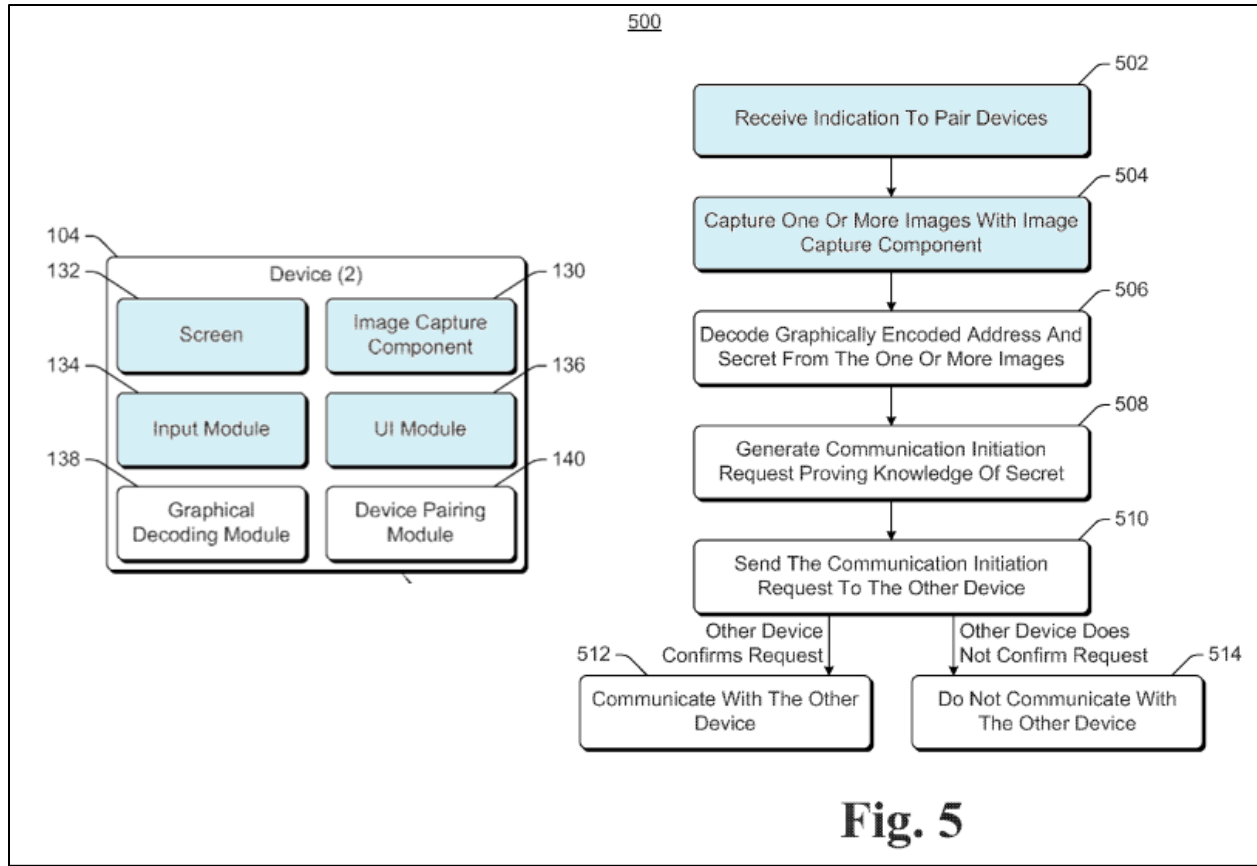
110. Thus, it is my opinion that the combination of Bishop and LeBoeuf teaches this element.

- g. [1.6] Generate, via the mobile device processor, an optical scanning user interface on the mobile device display;**

111. Bishop-LeBoeuf's mobile device 104 is configured to, via its processor, capture an image of "graphically encoded data" that is displayed on the screen 112 of corresponding device 102. EX1004, ¶¶16, 23, 39 ("[I]mages displayed on screen 112 as graphically encoded data 106 are captured by image capture component 130" of device 104). That is, the device 104 generates and displays a barcode image encoding the device address and secret. EX1004, ¶27. The device 102 captures an image of this image using its image capture component

(camera), and by generating an *optical scanning user interface on the mobile device display*. See EX1004, ¶34.

112. In particular, device 104 generates a user interface corresponding to a “camera mode” (*optical scanning user interface*) in response to a “capture request input by a user via input module 134” of the device. EX1004, ¶34. This is performed via the device’s processor 602. EX1004, ¶¶31 (functionality implemented by “one or more instructions that are executed by one or more processors or controllers”), 76. The camera mode interface presents on the display of device 104 “a view being seen by image capture component 130,” which enables the user to “position device 104 appropriately” to capture the image. EX1004, ¶34. For instance, “[t]he user can [] position device 104 appropriately so that the image on screen 112 is being seen by image capture component 130, and then input a capture request.” EX1004, ¶34.



EX1004, FIGs. 1 (excerpt), 5 (annotated).

113. Thus, it is my opinion that the combination of Bishop and LeBoeuf teaches this element.

- h. [1.7] Detect, via the at least one mobile device camera sensor and the optical scanning user interface, a color coded digital scannable media from a display included within the external wearable activity tracking device,**

114. As explained for element [1.6], Bishop-LeBoeuf’s mobile device 104 captures an image of “graphically encoded data” that is displayed on the screen of corresponding device 102. EX1004, ¶¶16, 34, 39. The graphically encoded data is a “high capacity color barcode (HCCB),” which as I explained above, is a *color coded digital scannable media* as claimed because it encodes data via different

colors, such that the colors themselves encode data. EX1004, ¶¶23, 30; *see also* Sections VI.A.2-3 *supra*. In particular, an HCCB has rows of strings of symbols (triangles) that can be one of, for instance, four colors, such as black, red, green, and yellow, each of which encodes different data. EX1017, 1; EX1018, 806. Each color is used to encode a different binary value. As I explained, this allows for greater data density compared to traditional black-and-white barcodes.

115. The device 104 *detects* the HCCB that is being displayed on the display of the device 102, for instance, by determining that the image contains graphically encoded data. The device 104 can “distinguish images that graphically encode data from images that do not graphically encode data,” for instance, “based on a known signature or other value encoded into each graphically encoded image.” EX1004, ¶35, *see also* ¶36. In other words, the device determines that an image depicts an HCCB by identifying the known signature in the image. This detection occurs via the image capture component (*camera sensor*), which captures the image, and the camera mode user interface (*optical scanning user interface*), which displays the view seen by the image capture component and enables the user to instruct the device to capture the image. EX1004, ¶34 (“[D]isplaying on screen 132 a view being seen by image capture component 130.”).

116. As explained in Section XI.C, in the combined system, Bishop-LeBoeuf’s mobile device establishes communication with the wearable monitoring

device (*external wearable activity tracking device*) using Bishop's barcode scanning process. The monitoring device initiates the process by generating and displaying the HCCB that is captured by the mobile device. The mobile device then captures the image and sends the communication initiation request to the monitoring device to establish the wireless communication link between the devices. *See* Sections VI.A-C.

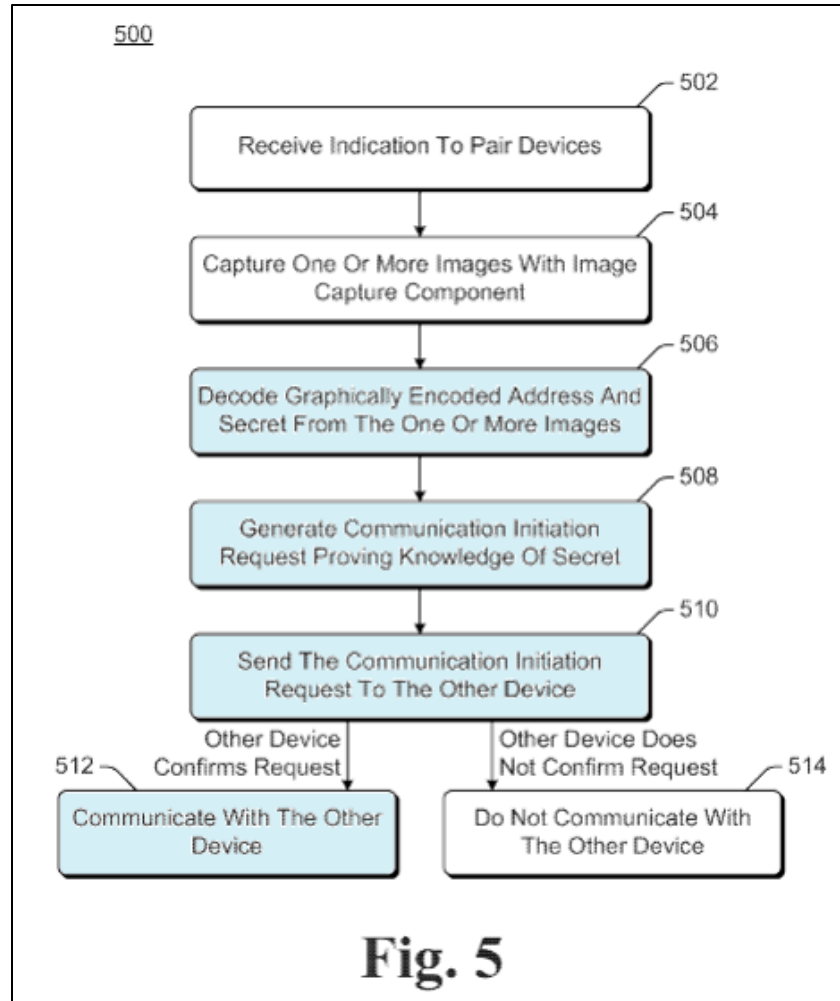
117. Thus, it is my opinion that the combination of Bishop and LeBoeuf teaches this element.

- i. **[1.8] wherein the color coded digital scannable media contains wireless pairing information associated with the external wearable activity tracking device;**

118. Bishop's HCCB encodes and contains *wireless pairing information* in the form of "an address of device 102." EX1004, ¶¶24, 56. The address is "an IP (Internet Protocol) address" or other address depending "on the protocol used by communication network 108." EX1004, ¶24. It comprises *wireless pairing information* because it "identifies device 102 on communication network 108," and enables "other devices on network 108 [to] send messages to device 102." EX1004, ¶18. The address is thus "used to initiate communication between devices 102 and 104." EX1004, ¶23.

119. The address is thus *wireless pairing information* because it is used to pair the devices. EX1004, ¶¶15 ("device pairing based on graphically encoded

data”), 18 (“This initiation of communication is also referred to as pairing devices 102 and 104 because devices 102 and 104 are paired together and able to communicate with one another after the initiation process.”). In particular, the HCCB encodes the address and (optionally) a “secret.” EX1004, ¶¶24, 56. When the device 104 obtains and decodes the address and secret, it “generates a communication initiation request that targets (e.g., is addressed to) device 102.” EX1004, ¶40. The communication initiation request includes the secret to “prove that device 104 has knowledge of the secret.” EX1004, ¶40. It also includes device 104’s address (e.g., IP address). EX1004, ¶41. Upon receiving the communication initiation request, the device 102 “verifies that the communication initiation request proves that device 104 has knowledge of the secret,” and then “proceed[s] with communicating with device 104.” EX1004, ¶¶43-44. At this point, the devices are paired. EX1004, ¶57, *see also* ¶18 (“[D]evices 102 and 104 are paired together and able to communicate with one another after the initiation process”).



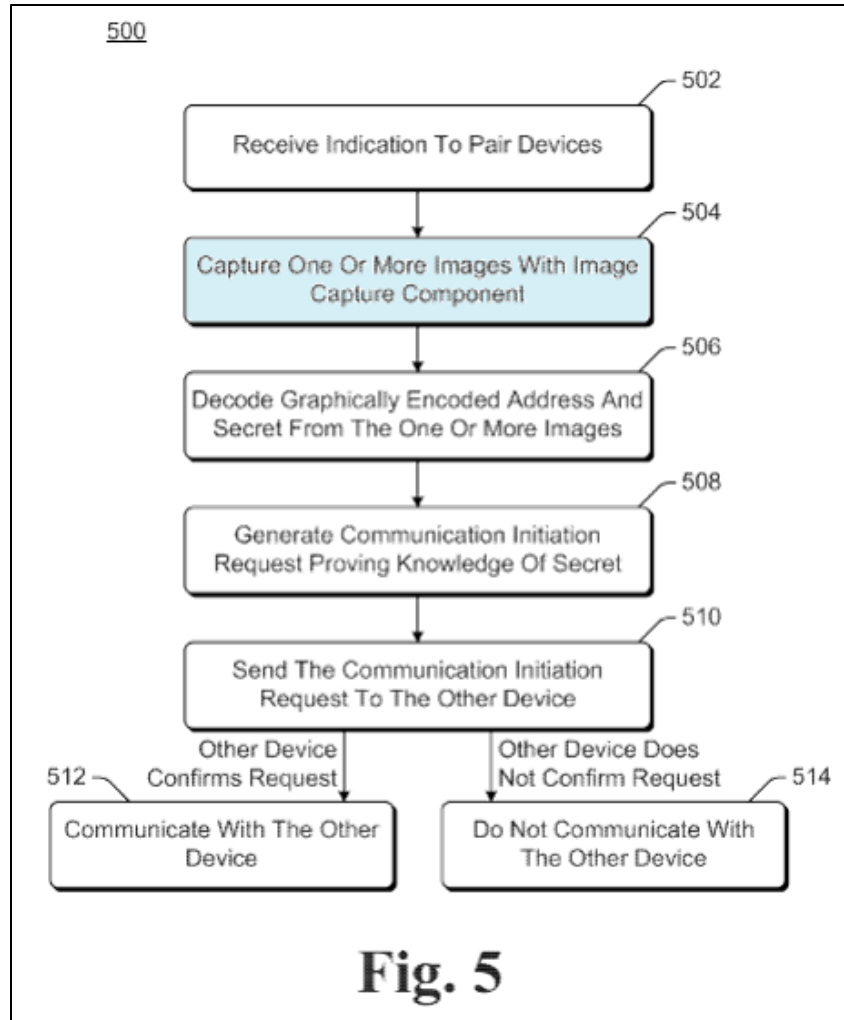
EX1004, FIG. 5 (annotated).

120. Thus, the address encoded in the HCCB comprises *wireless pairing information* associated with the device 102. As explained in Section XI.C, in the combined Bishop-LeBoeuf system, the address and secret are encoded and displayed by the wearable monitoring device (*external wearable activity tracking device*) in order to wirelessly pair the mobile device with the wearable monitoring device. In this system, the address is an address of the wearable monitoring device to initiate communications between the wearable monitoring device and the device 104. EX1004, ¶23.

121. Thus, it is my opinion that the combination of Bishop and LeBoeuf teaches this element.

- j. **[1.9] Optically obtain, via the at least one mobile device camera sensor, the wireless pairing information from the color coded digital scannable media;**

122. As explained for element [1.8], Bishop-LeBoeuf's device 104 captures an image depicting the HCCB displayed by device 112 using the image capture component (camera). EX1004, ¶¶33-36. The device further determines that the image "graphically encode[s] data," for instance, "based on a known signature or other value encoded into [the] graphically encoded image." EX1004, ¶¶35, 69. In one implementation, the device "captur[es] the images until one or more images that graphically encode data are captured." EX1004, ¶36. This process comprises *optically obtaining the wireless pairing information from the color coded digital scannable media* because the device 104 uses the image capture component (*camera sensor*) to capture (*optically obtain*) the encoded address (*wireless pairing information*) and secret that is stored in the HCCB (*color coded digital scannable media*).



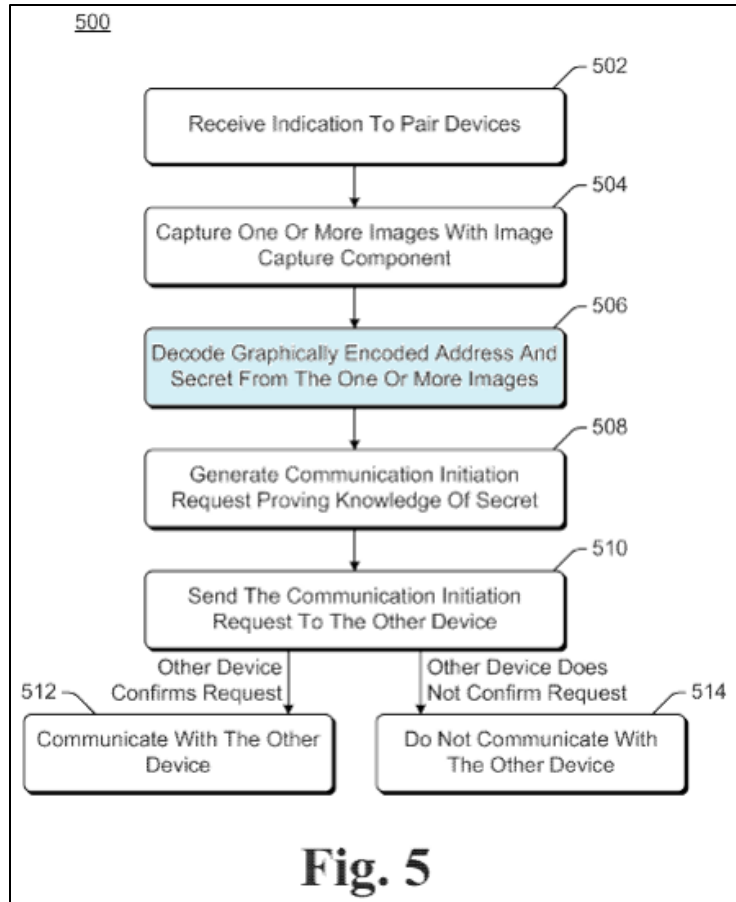
EX1004, ¶FIG. 5 (annotated).

123. Thus, it is my opinion that the combination of Bishop and LeBoeuf teaches this element.

k. [1.10] Process, via the at least one mobile device processor, the wireless pairing information;

124. Once Bishop-LeBoeuf's mobile device 104 captures the image depicting the HCCB, it *processes*, via its processor, the information encoded in the HCCB (*wireless pairing information*). It processes the *wireless pairing information* in multiple ways.

125. First, the device *processes the wireless pairing information* by determining the proper “graphical decoding technique” that it should use to decode the data. To do this, it determines the “the graphical encoding technique” used to encode the data “based on characteristics of the image... in which the data is encoded.” EX1004, ¶37. For instance, the device 104 determines “whether the image is black and white or includes color, whether symbols in the image are triangles or other shapes, etc.” EX1004, ¶37. Second, the device *processes the wireless pairing information* by “decod[ing] the data encoded in the images[]” (i.e., in the HCCB) using the selected “graphical decoding technique[.]” EX1004, ¶¶37, 39, *see also* ¶70 (“The graphically encoded data from the one or more images is decoded (act 506), resulting in a decoded address and a decoded secret.”). This processing is performed via the device’s processor 602. EX1004, ¶¶31 (functionality implemented by “one or more instructions that are executed by one or more processors or controllers”), 76.



EX1004, FIG. 5 (annotated).

126. Thus, it is my opinion that the combination of Bishop and LeBoeuf teaches this element.

- I. [1.11] Establish, via the at least one mobile device processor, a wireless communications link with the external wearable activity tracking device responsive to the processing of the wireless pairing information;

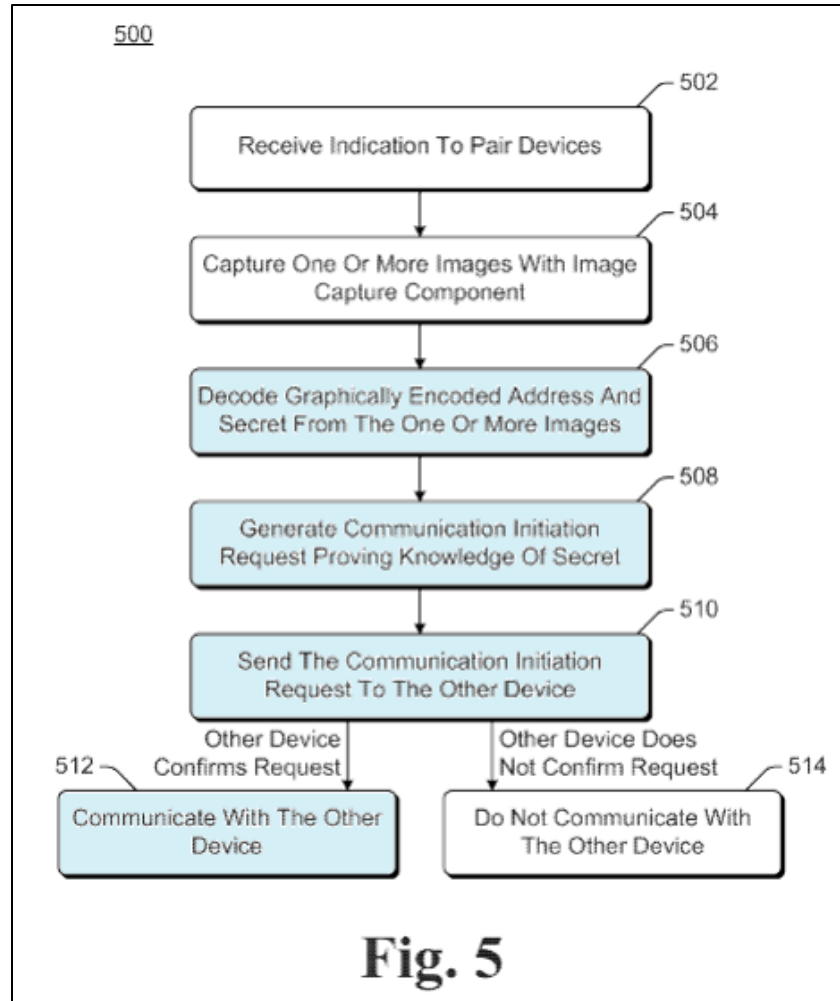
127. As explained above, in Bishop, when the device 104 obtains and decodes (*processes*) the address and secret, it “generates [via its processor] a communication initiation request that targets (e.g., is addressed to) device 102.”

EX1004, ¶40. The communication initiation request includes the secret to “prove

that device 104 has knowledge of the secret.” EX1004, ¶40. It also includes device 104’s address (e.g., IP address). EX1004, ¶41. Upon receiving the communication initiation request, the device 102 “verifies that the communication initiation request proves that device 104 has knowledge of the secret,” and then “proceed[s] with communicating with device 104.” EX1004, ¶¶43-44. At this point, the devices are “paired.” EX1004, ¶57.

128. The address is thus “used to initiate communication between devices 102 and 104” (*establish a wireless communications link*). EX1004, ¶23. Once established, the devices “wirelessly send[] data to and/or receiv[e] data from” one another. EX1004, ¶17, *see also* ¶¶44, 58, 80. The communication between devices is established via the one or more processing units 602 of device 104 (*via the at least one mobile device processor*), and using the graphically encoded data stored in the HCCB (*responsive to the processing of the wireless pairing information*). Indeed, the device 104 uses the address to generate a “communication initiation request” in order to “pair” devices 102 and 104. EX1004, ¶¶18, 76. Once the devices are “paired together,” they are “able to communicate with one another” via communications network 108. EX1004, ¶18 (“This initiation of communication is also referred to as pairing devices 102 and 104 because devices 102 and 104 are paired together and able to communicate with one another after the initiation process.”).

129. Bishop's pairing process is thus used to *establish a wireless communication link* because it initiates communication between the devices. The devices are not configured to communicate prior to the pairing process. The device address that is encoded in the HCCB is used to "identif[y] device 102 on communication network 108" so that "other devices on network 108 can send messages to device 102." EX1004, ¶18. The establishment of the wireless communication link thus enables the devices 102 and 104 to "transfer data (e.g., a report, song, or other data from one device to another)" and/or control information "(e.g., so images or other files from one device can be displayed on another, so that one device can change the operation of the other, and so forth)" to each other. EX1004, ¶58.



EX1004, FIG. 5 (annotated).

130. As explained in Section XI.C, in the combined Bishop-LeBoeuf system, the mobile device would be paired with the wearable monitoring device (*external wearable activity tracking device*). As described, the mobile device would capture an image of the graphically encoded data (HCCB) displayed by the wearable monitoring device and would generate and send the communication initiation request to the wearable monitoring device to establish the wireless connection between the devices. The wireless communication link would be, for instance, a Bluetooth link, as taught by LeBoeuf. EX1005, ¶¶101-02. Thus, the

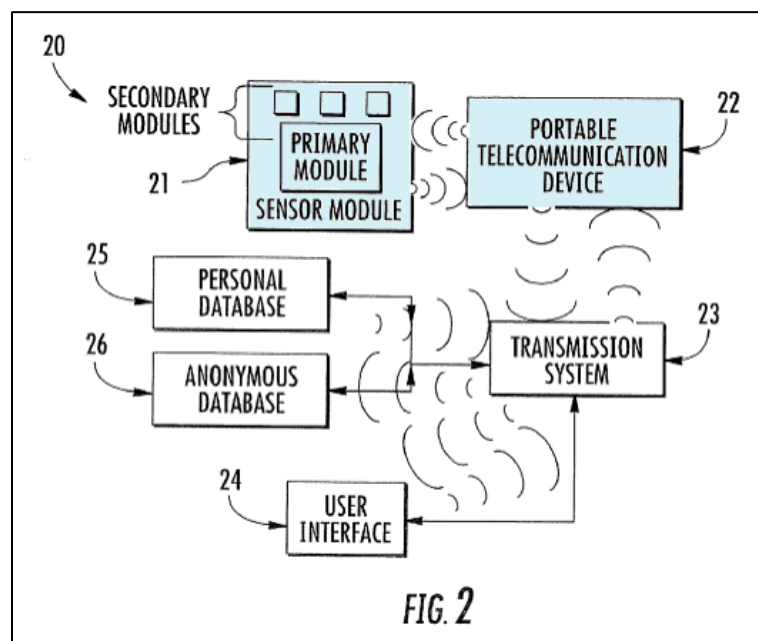
combination of Bishop and LeBoeuf teaches this element.

- m. **[1.12] Receive, via the wireless communications link, at least one of activity related information and bio-metric information generated by the external wearable activity monitoring device;**

131. The combination of Bishop and LeBoeuf teaches this element. Bishop teaches that, once communication is established between devices 102 and 104, the devices can “transfer data (e.g., a report, song, or other data [])” and “control information, and so forth to one another.” EX1004, ¶¶44, 58. The device 104 receives this information *via the wireless communication link* established using Bishop’s process.

132. LeBoeuf’s wearable monitoring device/sensor module (*external wearable activity monitoring 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. In LeBoeuf, the portable telecommunication device receives, from the wearable monitoring 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 (“[S]ignals from the sensors 11, 12 [] can be transmitted wirelessly by the transmitter 14.”), 119

("[W]earable sensor module 21 [records] psychological and physiological stress," which is sent to and "displayed on a portable telecommunication device 22."), 129 ("[R]aw or preprocessed data from the sensor module 21 is transmitted wirelessly to the telecommunication device 22."), 141 ("Raw or processed data 46 from these sensors can be wirelessly transferred to a recording device or a portable telecommunication device 22 (FIG. 2).").



EX1005, FIG. 2 (annotated).

133. This transmitted sensor data includes *activity related information and bio-metric information generated by the wearable monitoring device*. 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” (*bio-metric information*).

EX1005, ¶97.

134. The physiological sensors are also configured to generate *activity related 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 “gage 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 (“[A]ccelerometer-based pedometers” used to “measure the number of steps walked during a day.”).

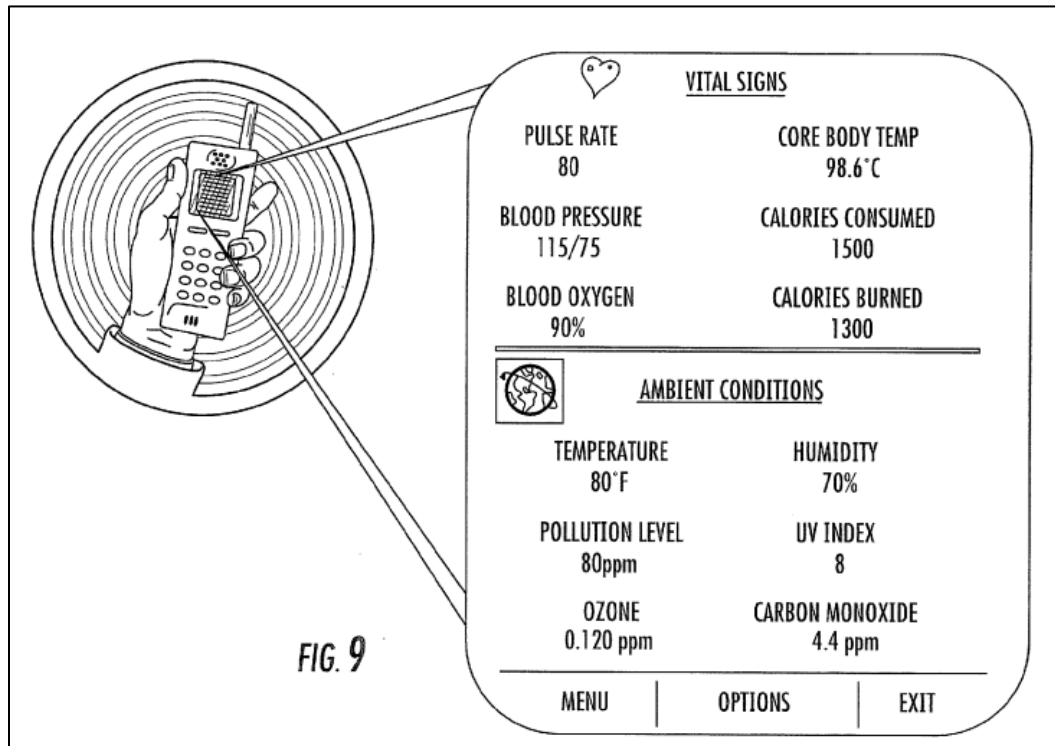
135. As explained in Section XI.C, in the Bishop-LeBoeuf system, the wearable monitoring device would generate such information and wirelessly transmit it to the mobile device. In the combined system, this information would be transmitted over the *wireless communications link* established using Bishop’s communication initiation procedures. Thus, the combination of Bishop and LeBoeuf teaches this element.

- n. **[1.13] Display, via the mobile device display, at least one of the activity related information and the biometric information.**

136. LeBoeuf's portable telecommunication device 22 (*mobile device*) includes "an end-user graphical interface... such that data from the wearable sensor module 21 can be stored, analyzed, summarized, and displayed on the portable telecommunication device 22." EX1005, ¶102. "For example, charts relating [to] health and environment, as well as real-time biofeedback and the like, can be displayed on" the user interface of the portable telecommunication device. 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, such as charts."), 119 ("[P]sychological and physiological stress" recorded by wearable sensor module is "displayed on a portable telecommunication device 22."), 129 ("[P]ortable telecommunication device" "display[s] various health factors over time with respect to a particular environment.").

137. An example user interface displayed on the portable telecommunication device is shown in Figure 9. EX1005, ¶¶41, 97. Figures 3 and 10 show other example user interfaces for displaying similar data. EX1005, ¶¶105-106. As shown in Figure 9, the user interface displays "vital signs" including pulse rate, core body temperature, blood pressure, caloric intake, calories burned, etc. As

explained above, these “vital signs” were measured by the “physiological sensors” of the wearable monitoring device, and transmitted to the portable telecommunication device, in “raw or processed” form, for display by the portable telecommunication device. EX1005, ¶¶79, 101-102, 129, 141.



EX1005, FIG. 9.

138. As explained in Section XI.C, in the Bishop-LeBoeuf system, the wearable monitoring device would collect and generate basic vital signs and would transmit them to the mobile device for display by the mobile device. This would include displaying, via its processor, a user interface similar to that shown in LeBoeuf’s Figure 9 depicting “vital signs collected by” the monitoring device. EX1005, ¶97. Thus, the combination of Bishop and LeBoeuf teaches this element.

2. Claim 11

- a. [11.P] A system for establishing a wireless communications link between a wearable activity tracking device and a mobile device, the system comprised of:**

139. The combination of Bishop and LeBoeuf teaches this element. As explained in Section XI.C, and for claim 1, Bishop teaches a *system for establishing a wireless communications link between two mobile devices*. EX1004,

¶12. LeBoeuf teaches a system in which a wearable monitoring device (*wearable activity tracking device*) communicates wirelessly with a portable telecommunication device (*mobile device*). EX1005, ¶101. In the combined system, Bishop's wireless communication link establishment process is used to establish the wireless communications link between the wearable monitoring device a mobile device, as taught by the combination of LeBoeuf and Bishop.

- b. [11.A.1] The wearable activity tracking device, wherein the wearable activity tracking device is comprised of;**

140. The combination of Bishop and LeBoeuf teaches this element for the reasons provided for element [1.4]. EX1005, ¶¶14, 79, 97.

- c. [11.A.2] A display device;**

141. Bishop-LeBoeuf's wearable monitoring device includes a "visual monitor" for displaying a user interface. EX1005, ¶105. Moreover, as I explained in Section XI.C, in the combined Bishop-LeBoeuf system, the wearable monitoring

device would include 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; *see also* discussion for element [1.7]. Thus, it is my opinion that the combination of Bishop and LeBoeuf teaches this element.

d. [11.A.3] At least one of an activity tracking capability and an embedded bio-metric monitoring sensor associated with the wearable activity tracking device;

142. As explained for elements [1.4] and [1.12], Bishop-LeBoeuf’s wearable monitoring device 10 comprises *embedded bio-metric monitoring sensors* in the form of “physiological sensor[s] 11... for monitoring the physiological functioning of the body.” EX1005, ¶¶79-80. LeBoeuf provides a long list of example physiological sensors, including, for instance, “sensors for monitoring: heart rate, pulse rate, breathing rate, blood flow, heartbeat signatures,” etc. EX1005, ¶80.

143. The monitoring device also comprises *an activity tracking capability* via sensors that are configured to monitor, 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* ¶¶14, 79, 97, 110, 112, 163. For instance, the wearable monitoring device can “track the caloric intake, health, and physical activity of dieters,” as well as “the diet, physical activity, health, and environment of athletes.” EX1005, ¶110, *see*

also ¶163 (“Caloric intake, physical activity, and metabolism can be monitored using a core temperature sensor, an accelerometer, a sound extraction methodology, a pulse oximeter, a hydration sensor, and the like.”). As another example, the wearable monitoring device includes “one or more accelerometers” that “measur[e] body motion in real-time,” and “gauge the distance a person has traveled.” EX1005, ¶¶120, 170, *see also* ¶159 (“[A]ccelerometer-based pedometers” used to “measure the number of steps walked during a day.”).

144. As another example, the wearable monitoring device comprises *an activity tracking capability* by executing “algorithms” that “combin[e] information from various sensors 11, 12 into a meaningful real-time personal health and environmental exposure assessment.” EX1005, ¶129, *see also* ¶113 (“Various algorithms can also be integrated into the wearable sensor module 21.”).

145. Thus, it is my opinion that the combination of Bishop and LeBoeuf teaches this element.

- e. **[11.A.4] Wireless communication circuitry, wherein the wireless communication circuitry is configured to establish a wireless communications link with the mobile device;**

146. Bishop-LeBoeuf’s wearable monitoring device includes “telemetric modules” (*wireless communication circuitry*), such as a Bluetooth module comprising a “Bluetooth chip.” EX1005, ¶148, FIG. 8, *see also* ¶146 (“telemetric circuitry”). The device also includes a transmitter/receiver 14 that includes

“electromagnetic transmitters,” such as one or more antennas. EX1005, ¶88.

147. Using such telemetric modules and antenna, 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® or ZigBee.” EX1005, ¶101, *see also* ¶58 (“[A] wireless connection [is] established for the duration of one session without the need for a base station.”).

148. Moreover, as explained for element [1.4], Bishop’s device includes *wireless communication* circuitry in the form of a “device pairing module,” “network card,” and “communications... modules” for establishing wireless communications links. EX1004, ¶¶17, 19, 24, 77.

149. As explained in Section XI.C, in the Bishop-LeBoeuf system, the wearable monitoring device establishes the *wireless communications link* with the mobile device using Bishop’s communication initiation process. Thus, the combination of Bishop and LeBoeuf teaches this element.

- f. **[11.A.5] at least one processor with software, wherein the at least one 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;**

150. As explained in Section XI.C, the Bishop-LeBoeuf system adapts

LeBoeuf's wearable monitoring device to implement Bishop's device pairing process. In the combined system, the wearable monitoring device comprises *at least one processor with software*. 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 executes "software" comprising instructions for implementing Bishop's communication initiation process, such as the process 400 of Figure 4. EX1004, ¶¶59, 73-74, 76.

151. The processor(s) of the combined 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. 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, ¶¶19 (Functionality of device 102 implemented by "one or more instructions that are executed by one or more processors or controllers of device 102."), 22, 27. The processor(s) are further *in signal communication with the wireless communication circuitry* because they cause the wireless communication circuitry to communicate with the mobile device 104. EX1004, ¶44; EX1005, ¶101.

152. Thus, it is my opinion that the combination of Bishop and LeBoeuf

teaches this element.

- g. [11.A.6] the memory device, wherein the memory device is configured to store wireless pairing information associated with the wireless communication circuitry;**

153. As explained for element [1.8], Bishop teaches the claimed *wireless pairing information associated with the wireless communication circuitry* through its “address of device 102” encoded in the HCCB. EX1004, ¶¶23-24. Device 102 stores this information in “a setting or configuration store of device 102.” EX1004, ¶24. A POSA would have understood that this setting or configuration store is implemented via the *memory device* that stores data. For instance, as I explained above, the Bishop-LeBoeuf wearable device includes “one or more memory and/or storage components” configured to store data, including the device address. EX1004, ¶¶75, 79. Thus, it is my opinion that the combination of Bishop and LeBoeuf teaches this element.

- h. [11.A.7] wherein the at least one processor software is configured to; obtain, from the memory device, the wireless pairing information associated with the wireless communication circuitry;**

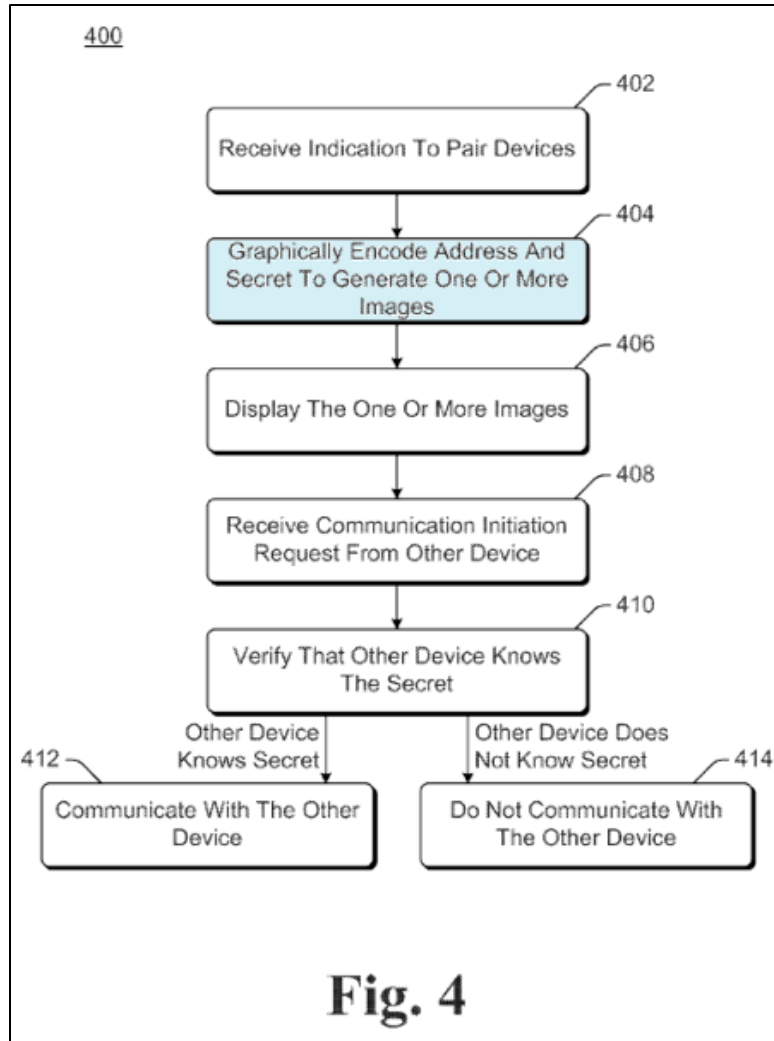
154. To encode the address (*wireless pairing* information), Bishop’s device 102 is configured to obtain it “in a variety of different manners, such as from another component or module of device 102, from a setting or configuration store of device 102” (*memory device*). EX1004, ¶24; *see also* discussion for element

[11.A.6]. This functionality is implemented via the processor software. EX1004,

¶¶19 (Functionality of device 102 implemented in software by “one or more instructions that are executed by one or more processors or controllers of device 102.”), 76. As explained in Section XI.C, the wearable monitoring device implements this functionality in the Bishop-LeBoeuf system. Thus, it is my opinion that the combination of Bishop and LeBoeuf teaches this element.

i. [11.A.8] generate a color coded digital scannable media image responsive to the wireless pairing information;

155. As explained for element [1.7], Bishop’s device 102 displays an image of “graphically encoded data” (i.e., HCCB) (*color coded digital scannable media*) that stores the address (*wireless pairing information*) and secret of device 102. EX1004, ¶¶16, 23, 30, 34, 39. To do so, the device 102 first “graphically encodes the obtained address and secret to generate one or more images.” EX1004, ¶27. As explained in Section XI.C, the wearable monitoring device implements this functionality in the Bishop-LeBoeuf system. Thus, it is my opinion that the combination of Bishop and LeBoeuf teaches this element.

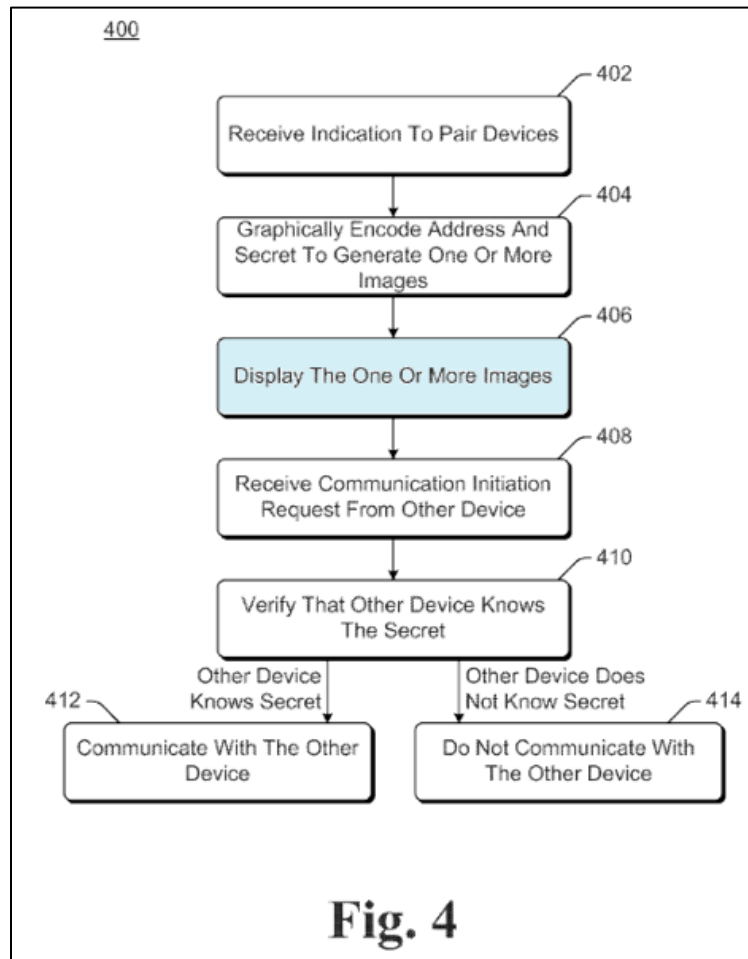


EX1004, FIG. 4 (annotated).

- j. [11.A.9] control the display device, wherein the display device is configured to display the color coded digital scannable media image;

156. Bishop's device 102 is configured to control the screen 112 (*display device*). EX1004, ¶22. As explained for element [1.7], the screen 112 is configured to display an image of "graphically encoded data" (i.e., HCCB) (*color coded digital scannable media image*). EX1004, ¶27 ("These images displayed on screen 112 are the graphically encoded data 106 being transferred to device 104."). As

explained in Section XI.C, the wearable monitoring device implements this functionality in the Bishop-LeBoeuf system. Thus, it is my opinion that the combination of Bishop and LeBoeuf teaches this element.

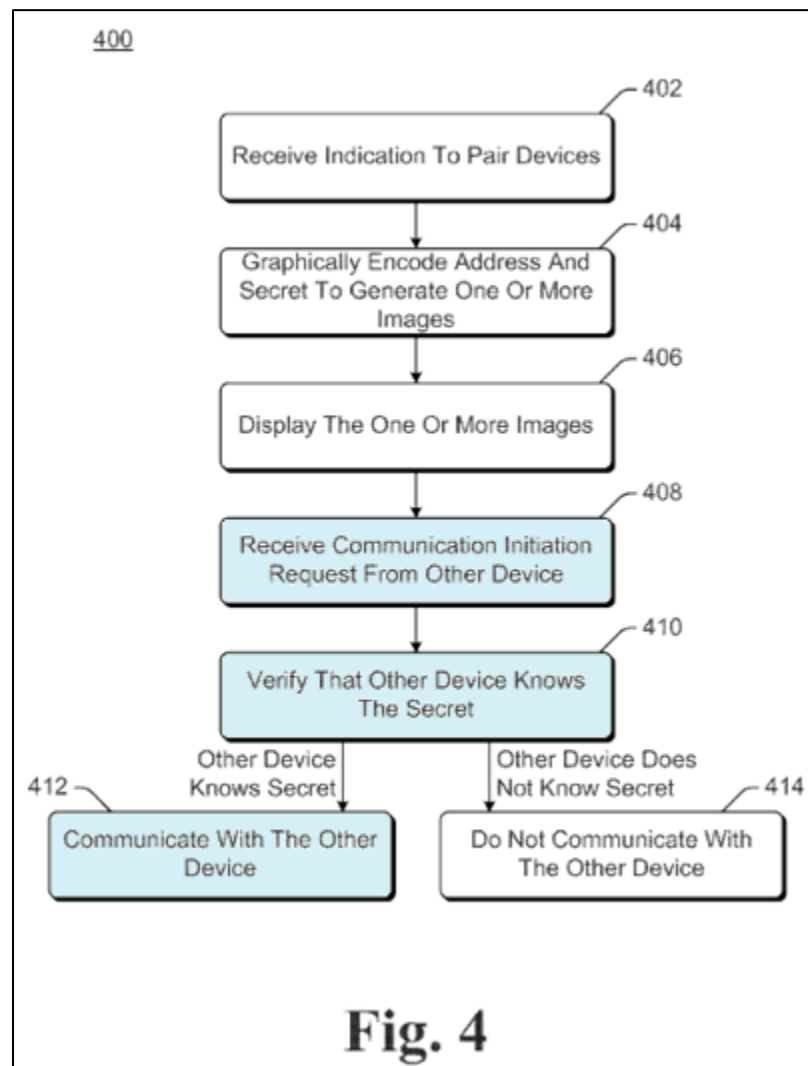


EX1004, FIG. 4 (annotated).

- k. **[11.A.10] 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;**

157. The combination of Bishop and LeBoeuf teaches this element for the reasons provided for element [1.11]. As explained, the Bishop-LeBoeuf mobile

device “generates a communication initiation request that targets (e.g., is addressed to) device 102.” EX1004, ¶40. Upon receiving the request, the wearable monitoring device “verifies that the communication initiation request proves that device 104 has knowledge of the secret,” and then “proceed[s] with communicating with device 104.” EX1004, ¶¶43-44. Thus, it is my opinion that the combination of Bishop and LeBoeuf teaches this element.



EX1004, FIG. 4 (annotated).

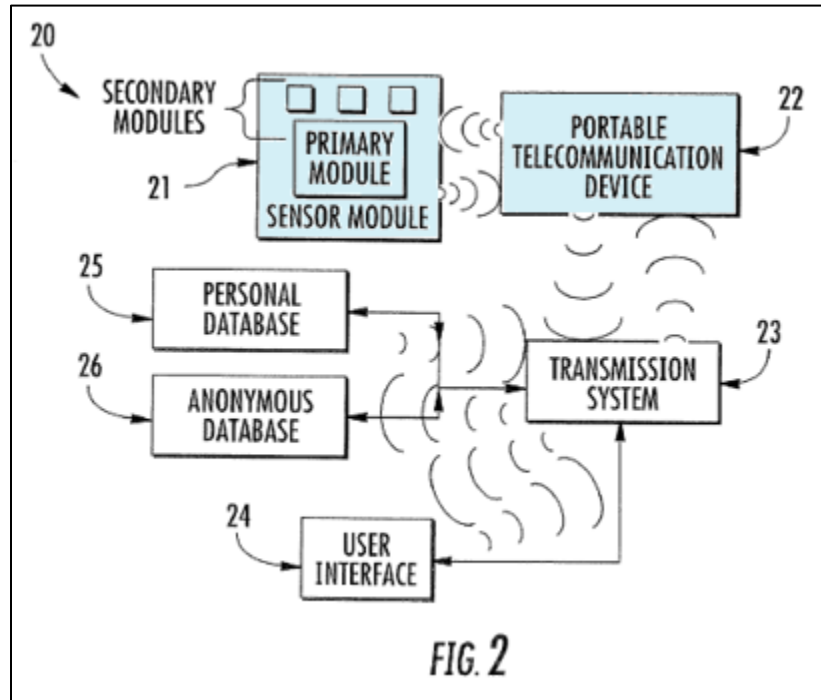
l. [11.A.11] Generate at least one of activity tracking information and bio-metric information;

158. The combination of Bishop and LeBoeuf teaches this element for the reasons provided for element [1.12] and [11.A.3]. As explained, LeBoeuf's wearable monitoring device generates information related to "basic vital signs" (*bio-metric information*) and information related to "physical activity" (*activity related information*) and transmits this information to the portable telecommunication device. 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. Thus, it is my opinion that the combination of Bishop and LeBoeuf teaches this element.

m. [11.A.12] Communicate, via the wireless communications link, at least one of the activity tracking information and the bio-metric information to the mobile device; and

159. The combination of Bishop and LeBoeuf teaches this element for the reasons provided for element [1.12]. As explained, Bishop-LeBoeuf's wearable monitoring device (*external wearable activity monitoring device*) communicates

the activity tracking information and the bio-metric information to the mobile device. EX1005, ¶¶101-02. Thus, it is my opinion that the combination of Bishop and LeBoeuf teaches this element.



EX1005, FIG. 2 (annotated).

- n. **[11.B.1] The mobile device, wherein the mobile device is comprised of; at least one camera sensor, included within the mobile device;**

160. The combination of Bishop and LeBoeuf teaches this element for the reasons provided for elements [1.P] and [1.1].

- o. **[11.B.2] at least one processor in signal communication with the at least one camera sensor;**

161. The combination of Bishop and LeBoeuf teaches this element for the reasons provided for element [1.2].

- p. [11.B.3] a display in signal communication with the at least one processor;**

162. The combination of Bishop and LeBoeuf teaches this element for the reasons provided for element [1.3].

- q. [11.B.4] communication circuitry configured for wireless communication with the wearable activity tracking device;**

163. The combination of Bishop and LeBoeuf teaches this element for the reasons provided for element [1.4].

- r. [11.B.5] memory, included within the mobile device, associated with one or more processors and configured to store software instructions, which, when executed by the one or more processors, cause the one or more processors to perform operations comprising;**

164. The combination of Bishop and LeBoeuf teaches this element for the reasons provided for element [1.5].

- s. [11.B.6] Generate, via the mobile device processor, an optical scanning user interface on the mobile device display;**

165. The combination of Bishop and LeBoeuf teaches this element for the reasons provided for element [1.6].

- t. **[11.B.7] Detect, via the at least one mobile device camera sensor and the optical scanning user interface, a color coded digital scannable media from the display included within the wearable activity tracking device, wherein the color coded digital scannable media contains wireless pairing information associated with the wearable activity tracking device;**

166. The combination of Bishop and LeBoeuf teaches this element for the reasons provided for elements [1.7] and [1.8].

- u. **[11.B.8] Optically obtain, via the at least one mobile device camera sensor, the wireless pairing information from the color coded digital scannable media;**

167. The combination of Bishop and LeBoeuf teaches this element for the reasons provided for element [1.9].

- v. **[11.B.9] Process, via the at least one mobile device processor, the wireless pairing information;**

168. The combination of Bishop and LeBoeuf teaches this element for the reasons provided for element [1.10].

- w. **[11.B.10] Establish, via the at least one mobile device processor, a wireless communications link with the wearable activity tracking device responsive to the processing of the wireless pairing information;**

169. The combination of Bishop and LeBoeuf teaches this element for the reasons provided for element [1.11].

- x. **[11.B.11] Receive, via the wireless communications link, at least one of activity related information and bio-metric information generated by the wearable activity tracking device;**

170. The combination of Bishop and LeBoeuf teaches this element for the reasons provided for element [1.12].

- y. **[11.B.12] Display, via the mobile device display, at least one of the activity related information and the bio-metric information.**

171. The combination of Bishop and LeBoeuf teaches this element for the reasons provided for element [1.13].

E. Dependent Claims

1. Claims 2 and 13

172. Claims 2 and 13 recite “wherein the mobile device is at least one of a smartphone device and a tablet device.”

173. Bishop’s device 104 can be a “cellular or other wireless phone.” EX1004, ¶15. The cellular/wireless phone comprises a smartphone because it implements “one or more applications that are run by one or more processors,” such as “communications applications or modules for wirelessly sending data to and/or receiving data from other devices, productivity applications or modules (e.g., spreadsheets, word processors), recreational applications or modules (e.g., games), resource applications or modules (e.g., databases, digital books), audio/video applications or modules (e.g., digital cameras, digital video cameras,

music playback programs), mapping or tracking applications or modules, and so forth.” EX1004, ¶17.

174. 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.

2. Claim 3

175. Claim 3 recites “wherein the wireless communications link is a two-way wireless communications link.”

176. Bishop’s wireless communications link is a *two-way wireless communications link* because it enables “two devices to be able to communicate data and/or control information between one another.” EX1004, ¶1. The devices are able to “send[] messages including data, control information, and so forth to one another.” EX1004, ¶44, *see also* ¶¶57-58. Furthermore, LeBoeuf’s *wireless communications link* is a *two-way* link because it is implemented using, for instance, Bluetooth or ZigBee, and enables “[t]he portable telecommunication device 22 and the wearable sensor module 21 [to] telemetrically communicate both to and from each other.” EX1005, ¶101. The combination of Bishop and LeBoeuf thus teaches this claim.

3. Claims 5 and 17

177. Claims 5 and 11 recite “wherein the color coded digital scannable

media [displayed by the wearable activity tracking device] 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, a augmented reality marker, a augmented reality image, and a augmented reality code.”

178. Bishop’s graphically encoded data is stored in a HCCB (*color coded digital scannable media*), which is a *2D matrix code* and a *representation of non-human readable information using colored pixels*. EX1019, 710 (HCCB is an example of a “2D barcode[]” and “use[es] colors to create more symbols, resulting in larger data capacity within the same size”); EX1017, 1 (HCCB is a “2D” barcode that implements “four colors: black, red, green and yellow” to encode machine-readable information.). The HCCB is a 2D matrix code because it encodes data using symbols in a two dimensional matrix format. It also encodes *non-human readable information using colored pixels* for the reasons I provided in Section VI.A. Indeed, a POSA would have understood that the HCCB image generated by the device 102 implements color using pixels.

4. Claims 6 and 18

179. Claims 6 and 18 recite “wherein the activity related information is generated by the [external] wearable activity tracking device from an accelerometer included within the [external] wearable activity tracking device.”

180. Bishop-LeBoeuf’s wearable monitoring device includes “one or more

accelerometers” that “measur[e] body motion in real-time,” and “gauge the distance a person has traveled.” EX1005, ¶¶120, 170, *see also* ¶¶76, 157, 163. These accelerometers are used to generate *activity-related information*, such as human motion, “[c]aloric intake, physical activity, and metabolism,” “the number of steps walked during a day,” etc. EX1005, ¶¶159 (“[A]ccelerometer-based pedometers” used to “measure the number of steps walked during a day.”), 163 (“Caloric intake, physical activity, and metabolism can be monitored using...an accelerometer.”).

5. Claims 7 and 16

181. Claims 7 and 16 recite “wherein the bio-metric information is generated by the [external] wearable activity tracking device from at least one of a blood pressure sensor, a heart rate sensor, a blood glucose sensor, a body fat sensor, and a temperature within the [external] wearable activity tracking device.”

182. As explained for element [1.12], Bishop-Leboeuf’s wearable monitoring device includes “physiological sensor[s] 11... for monitoring the physiological functioning of the body,” and generating *bio-metric information*. EX1005, ¶¶79-80. These sensors include, for instance, sensors for monitoring “heart rate, pulse rate,” “blood pressure,” “glucose,” “body fat density,” “skin and core body temperature,” etc. EX1005, ¶¶80, 151, *see also* ¶81.

6. Claims 8 and 12

183. Claim 8 recites “wherein the 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 external wearable activity tracking device.”

184. Claim 12 recites “wherein the wearable activity tracking device 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.”

185. Bishop’s communication circuitry is configured to establish a wireless connection between devices 102 and 104 over communication network 108, which can be “a variety of different networks, including the Internet,” which is a wide area network. EX1004, ¶18.

186. Moreover, 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, are personal area networks. EX1021, 1:11-24.

7. Claim 14

187. Claim 14 recites “wherein the wearable activity tracking device is at least one of a smartwatch device and a wearable health monitoring device.”

188. LeBoeuf’s wearable monitoring device is a *wearable health monitoring device* because it is a “health and environmental monitor[.]” “worn by”

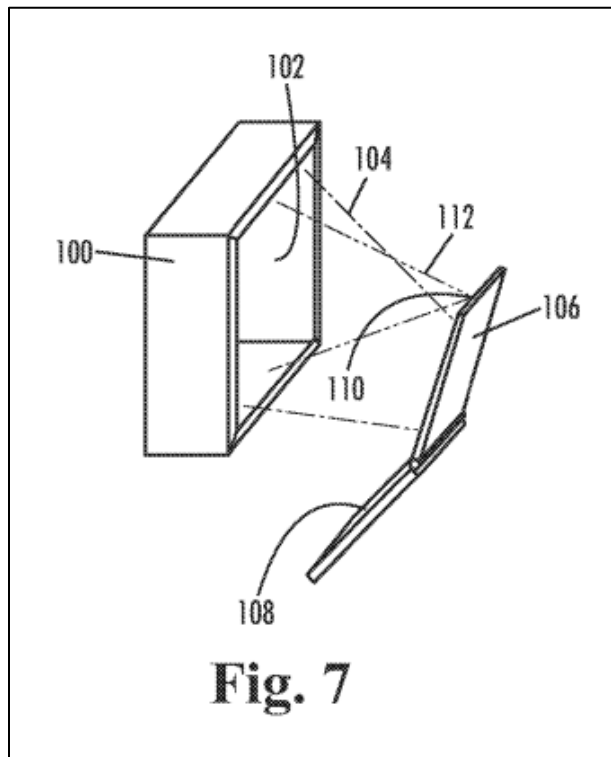
the user, and is configured to measure “basic vital signs” of the user, such as “breathing rate, pulse rate, and the like.” EX1005, ¶¶4, 79, 97, 138; *see also* discussion for element [1.4] *supra*. The wearable monitoring device can be implemented as a “wrist-watch.” EX1005, ¶141. In such configuration, the wearable monitoring device is 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. It also includes “algorithms for processing personal health and environmental data, diagnosing medical conditions, assessing health states” as well as algorithms for providing a “meaningful real-time personal health and environmental exposure assessment.” EX1005, ¶¶113, 129.

XII. GROUND 2: BISHOP-LEBOEUF FURTHER IN VIEW OF WILLIAMS RENDERS OBVIOUS CLAIMS 4, 9, 10, 15, 19, AND 20.

1. Williams

189. 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. “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 4 and 15

190. Claims 4 and 15 recite “wherein the wireless pairing information

includes at least one of a MAC address identifier associated with the external wearable activity tracking device and a unique identification number associated with the external wearable activity tracking device.”

191. As explained above, Williams’s “wireless pairing information” includes a “unique Bluetooth device address.” EX1009, ¶¶42, 45. A POSA would have understood that this address comprises a unique identification number associated with the requesting device. *See* EX1006, ¶40 (“Bluetooth devices may be identified by a unique network address that is assigned to each device (i.e., when it is manufactured).”); EX1021, 2:16-18 (“To facilitate pairing, each Bluetooth device is associated with a unique 48-bit address known as the Bluetooth Device Address or BD_ADDR.”).

192. A POSA would have found it obvious to implement Williams’s unique Bluetooth device address in the Bishop-LeBoeuf *wireless pairing information*. Indeed, as explained in Section XI.C, a POSA would have adapted Bishop’s pairing process to establish LeBoeuf’s wireless connection, which comprises a Bluetooth connection. EX1005, ¶101. Indeed, Bishop teaches various network protocols can be used, and that the encoded device address is dependent on such protocol. EX1004, ¶¶18, 24. As I also explained, when establishing such Bluetooth connection, a POSA would have found it obvious to adapt the encoded device address to be a Bluetooth address, which uniquely identifies the device.

193. The Bluetooth pairing process uses a unique Bluetooth address to address the devices. *See* EX1005, ¶¶40-43 (describing Bluetooth pairing process); EX1021, 2:16-18 (“To facilitate pairing, each Bluetooth device is associated with a unique 48-bit address known as the Bluetooth Device Address or BD_ADDR.”). And Williams provides explicit teaching of the use of such address. EX1009, ¶¶42, 45. Thus, a POSA would have found it obvious to implement Williams’s Bluetooth address in the Bishop-LeBoeuf system to establish LeBoeuf’s Bluetooth connection using Bishop’s pairing process. And a POSA would have readily been able to implement such modifications as a matter of a simple substitution of one known element for another (Bishop’s IP address for Williams’s Bluetooth address) to obtain predictable results (pairing Bluetooth devices).

194. That is, as I explained in section XI.C, a POSA would have readily understood, based on Bishop’s teachings, how to implement its pairing process for various networks, including Bluetooth. Williams confirms this by disclosing a similar pairing process for Bluetooth that encodes a unique Bluetooth address in a barcode to facilitate Bluetooth pairing between devices. *See also* Section VI.A.3 *supra* (discussing similar barcode-based Bluetooth pairing processes). In accordance with Bishop’s express instructions to encode addresses corresponding to the network protocol to be used, a POSA would have found it obvious to implement Williams’s use of a unique Bluetooth address for pairing Bluetooth

devices.

3. Claims 9, 10, 19, and 20

195. Claims 9 and 19 recite “wherein the wireless pairing information is at least partially encrypted by the [external] wearable activity tracking device.”

Claims 10 and 20 recite “wherein the processing [by the at least one mobile device] further includes decrypting the wireless pairing information after the mobile device optically detects the color coded digital scannable media displayed by the [external] wearable activity tracking device.”

196. As explained above, Williams teaches that its wireless pairing information is “encrypted” using various “encryption method[s].” EX1009, ¶¶26-28, 29. This results in an “encrypted image containing the” wireless pairing information. EX1009, ¶28. Although it does not expressly state that the pairing information is decrypted by the image-capturing device, a POSA would have understood that, when the pairing information encoded in the image is encrypted, the image-capturing device would need to decrypt it to use it for establishing the wireless link.

197. Indeed, for a device that receives encrypted data to understand that data, the device must first decrypt it. This holds true when the encrypted data is encoded in a barcode. For instance, Ross discloses encrypting medical data and “display[ing] the encrypted medical information in a machine readable format such

as a barcode.” EX1027, ¶169. The barcode is scanned “to obtain encrypted medical information,” which is “decrypt[ed]... using the decryption key.” EX1027, ¶¶170, 173, *see also* ¶91 (describing encryption/decryption process). Accordingly, a POSA would have readily understood that Williams teaches decryption as a counterpart to its expressly disclosed encryption. The decryption method is counterpart to the chosen “encryption method.” EX1009, ¶29.

198. I also note that the ’394 patent similarly does not expressly disclose decrypting data, even though it does disclose barcodes storing encrypted data. *See, e.g.*, EX1001, 4:39-46, 13:48-55, 22:35-53, 28:58-65. This confirms my opinion that a POSA would have readily understood that a reference, such as Williams, that teaches encryption techniques, also teaches corresponding decryption techniques.

199. A POSA would have found it obvious to implement Williams’s encryption/decryption techniques in Bishop-LeBoeuf to provide increased security of the device pairing process. As explained in Section XI.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 this information is not obtained by malicious actors. *See* EX1004, ¶45.

200. Indeed, encryption/decryption was a well-known technique for implementing secure communications. Furthermore, it was well known to

encrypt/decrypt information encoded in barcodes. EX1027, ¶¶91, 170, 173; EX1028, ¶39 (“The cell phone device may compute encrypted validation codes” and “display a barcode having... the computed encrypted validation code.”).

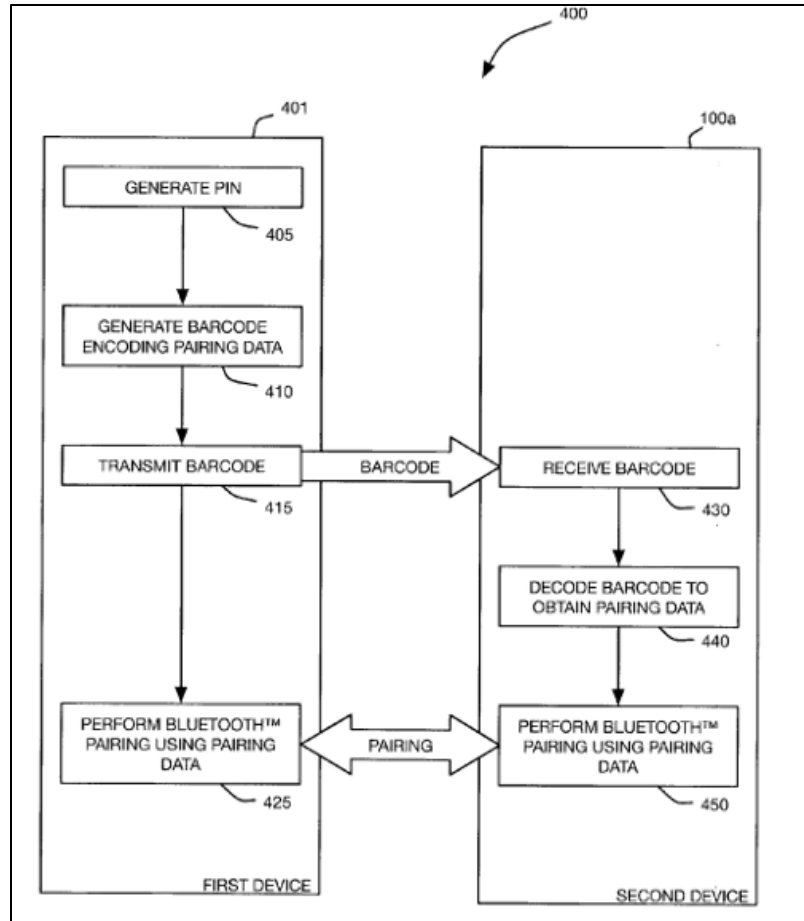
201. A POSA would have thus found it obvious to encrypt/decrypt Bishop-LeBoeuf’s graphically encoded data and would have had a reasonable expectation of success in doing so. Indeed, encryption was commonly performed to secure data and a POSA would have readily understood how to implement Williams’s encryption techniques. A POSA would have readily understood how to encode encrypted data in a barcode, and then to decrypt that data to obtain and use it. For instance, a POSA would have understood how to implement suitable known encryption/decryption schemes (e.g., asymmetric encryption using a public/private key system), and how to generate or provision appropriate keys for encrypting and decrypting the data. Such implementations would merely require the use of routine and conventional encryption techniques that were widely used and well-understood in the field. *See, e.g.*, EX1009, ¶¶9, 41, 43. Accordingly, 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).

XIII. GROUND 3A: BROWN IN VIEW OF WEISS RENDERS OBVIOUS CLAIMS 1-8 AND 11-18

202. Brown in view of Weiss renders obvious claims 1-8 and 11-18.

A. Brown

203. Brown teaches techniques for “performing Bluetooth pairing between a first device and a second device.” EX1006, Abstract. 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.

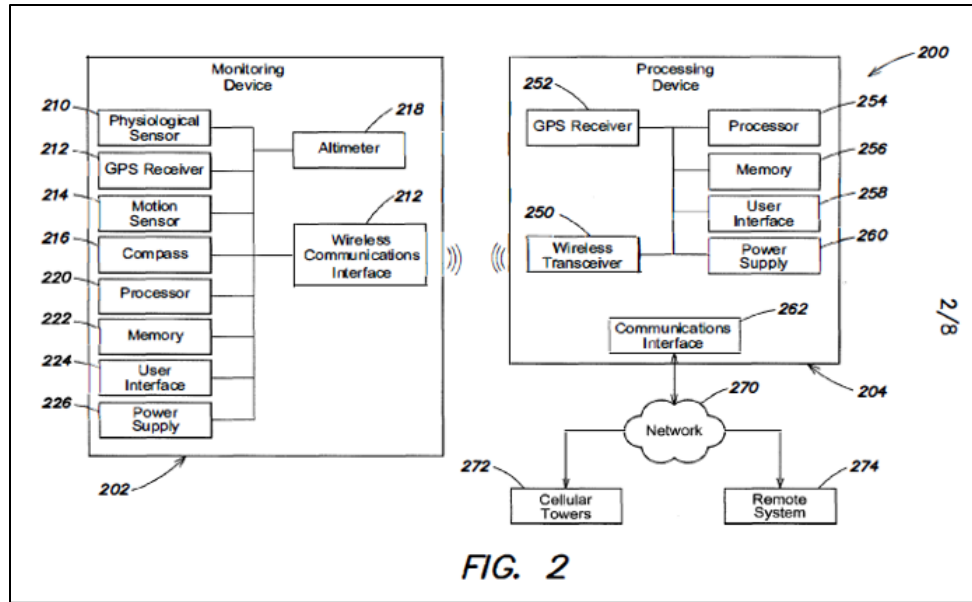
204. For instance, as shown in Figure 4 above, to initiate the pairing process, the device 401 generates or obtains from memory a “personal identification number (PIN) code.” EX1006, ¶¶71-72. The device 401 generates a barcode that “encodes Bluetooth pairing data,” which includes the PIN code and “the network address of the first device (e.g., MAC address).” EX1006, ¶75. The barcode can be a “color barcode” that “employ[s] different color combinations.” EX1006, ¶¶2, 76. The device 401 then displays an image of the barcode so that it can be captured by the device 100a. EX1006, ¶¶79, 83. The device 100a “decodes

the barcode to obtain the Bluetooth pairing data,” and “transmits Bluetooth pairing data... to first device 401, and carries out Bluetooth pairing in known manner.”

EX1006, ¶¶84-85.

B. Weiss

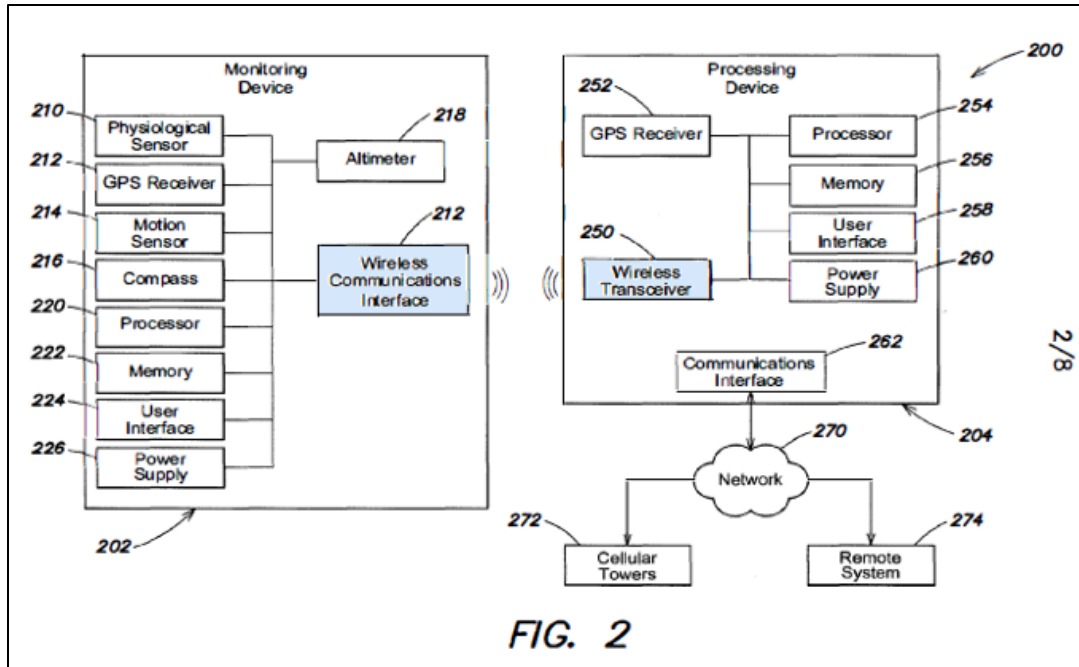
205. Weiss discloses a system for “monitoring one or more physiological conditions” that includes a “personal monitoring device” that is “designed to be easily wearable and include[s]... a plurality of sensors for detecting one or more physiological attributes” of a user. EX1007, 1:23-28, 2:11-15. The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

206. A POSA would have found it obvious to combine Brown and Weiss to arrive at the claims of the '394 patent. 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).

207. A POSA would have sought to minimize the difficulties in establishing a Bluetooth connection between Weiss’s devices. As I explained in Section VI.A, conventional pairing processes required users to “manually select a desired second [] device to pair with from a menu or list of available [] devices in range of the first [] device.” EX1021, 2:25-29, *see also* 2:66-3:1 (“[M]anual intervention may be required to pair Bluetooth devices or connect to an AP, particularly when connecting for the first time”); *see also* EX1006, ¶42 (“[T]here may be many discoverable devices within range, requiring a user to select the desired device from a long list.”); EX1023, ¶8 (“This type of manual input of data is inefficient and is prone to human error.”). In such implementations, users may select and thereby attempt to pair with the wrong device. EX1021, 3:1-11. A

POSA would have recognized this and would have sought to implement an intuitive and user-friendly pairing process for Weiss's devices.

208. This would have led a POSA to Brown, which teaches techniques for “performing Bluetooth pairing between a first device and a second device.”

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.

209. A POSA would have found it obvious to adapt Weiss's monitoring and processing devices to implement Brown's Bluetooth pairing process. Brown motivates this combination by 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 “reliev[es] the user of... the need to select the desired first device from a list of available devices that are in range.” EX1006, ¶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.

210. This is consistent with my explanation above. It was known that

wireless pairing of devices could be unintuitive and inefficient in part due to the need for manual intervention by the user and lack of easily implementable security. A POSA would have recognized the utility of Brown's process and would have thus been motivated to implement Brown's technique in Weiss. Indeed, a POSA would have recognized that Brown's process simplifies the pairing process and provides a straight-forward, intuitive manner of selecting devices with which to pair.

211. 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. Weiss's monitoring device also communicates health information related to "medical condition[s]" to "physicians and "health care providers." EX1007, 1:18-20, 3:9-12, 24:12-14. A POSA would have thus 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 that enabled the user more control over the pairing process. *See* EX1006, ¶¶38, 44-47.

212. The combination of Brown and Weiss thus teaches a wearable monitoring device that generates and communicates biometric and activity-related data to a mobile device over a wireless communications link established by a

pairing process initiated by encoding pairing information in a barcode. *See, e.g.*, EX1006, ¶¶49, 58; EX1007, 7:10-8:10. In particular, Brown teaches a wireless pairing process that establishes a wireless communications link between various types of mobile devices. EX1006, ¶¶79-80. Once this communications link is established, the devices can communicate data to each other over the link. EX1006, ¶40. Weiss teaches a usage scenario for Brown's wireless pairing process. For instance, Weiss teaches a wearable monitoring device that senses and generates data related to "physiological attributes" and communicates this data over a wireless communications link (e.g., Bluetooth) to a processing device for display by the processing device. EX1007, 7:10-8:10, 17:28-18:4.

213. The combined Brown-Weiss system would include a monitoring device and mobile device, as taught by the combination of Brown and Weiss, which would each be adapted to implement Brown's Bluetooth pairing process. For instance, the monitoring device would assume the role of Brown's device 401 (*see* EX1006, FIG. 4) in the pairing process and would initiate the process by generating and displaying a barcode encoding Bluetooth pairing information. The mobile device would assume the role of Brown's device 100a and would be configured to capture the displayed image and to generate and send Bluetooth pairing data to the monitor device to facilitate the pairing. The devices would then each be configured to establish the wireless communication link based on the

combined teachings of Brown and Weiss.

214. To this end, the monitoring device would be adapted as necessary to implement hardware and software to generate and display barcodes encoding Bluetooth pairing data for establishing a Bluetooth link, as taught by the combination of Brown and Weiss. Similarly, the mobile device would be adapted as necessary to implement hardware and software to capture and decode the Bluetooth pairing data, and to establish the Bluetooth link, as also taught by the combination of Brown and Weiss. For instance, a POSA would have found it obvious to adapt Weiss's devices to implement componentry taught by Brown, such as a "short-range communications subsystem," "computer-readable storage media," "memory," "display," "camera," and "processor" to the extent necessary to implement Brown's pairing process. EX1006, ¶¶15, 72, 75, 106. Such implementations would merely amount to a simple substitution of known elements into Weiss's devices in a known manner to achieve predictable results. That is, the resulting devices would be configured to implement Brown's pairing processes to establish a wireless communications link, and to share biometric and activity-related data over that link.

215. A POSA would have had a reasonable expectation of success in combining the references in this manner. 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." 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, 7:23-28, 12:14-18.

A POSA would have thus had no problem implementing Brown's techniques in Weiss's devices because Brown teaches similar devices and explains that the barcode pairing process can be implemented by low-resource devices EX1006, ¶46.

216. For instance, a POSA would have had no trouble adapting the monitoring device to implement a display that displays graphically encoded data, as taught by Brown. EX1006, ¶¶23, 79. Nor would a POSA have had trouble adapting the monitoring device to encode the Bluetooth pairing data in a barcode as taught by Brown. Indeed, it was well known for electronic devices, including watches, to generate and display barcodes that encoded information. For instance, Narayanaswami discloses a "Portable Shopping Device (PSD)" is implemented as a "wrist watch" with a "high definition display" configured to "convey a large amount of information on a screen using a 2D barcode." EX1010, ¶¶38, 49.

217. Moreover, as I explained above, a POSA would have also readily been able to make any other adaptations in Weiss's devices necessary to

implement Bishop's pairing process. For instance, Brown teaches conventional hardware and software components, such as such as a short-range communications subsystem, computer-readable storage media, memory, display, camera, and processor for implementing Brown's pairing process. EX1006, ¶¶15, 72, 75, 106. These components are conventional hardware and software elements that are compatible with Weiss's devices. It was within a POSA's skill to implement such components as necessary to achieve the predictable result of implementing Brown's pairing process.

218. A POSA would have recognized that these adaptations would have been straightforward and would have been implemented without undue burden. 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 (Brown and Weiss's mobile devices) in the same way (to efficiently and securely Bluetooth communications).

D. Independent Claims

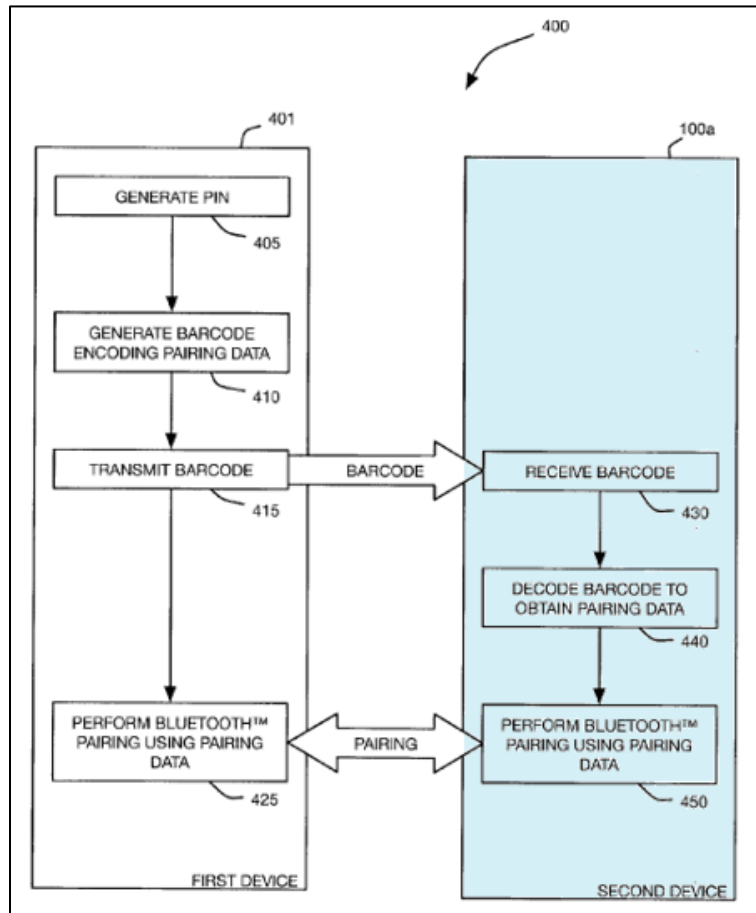
1. Claim 1

- a. [1.P] A mobile device, wherein the mobile device is comprised of:**

219. Brown discloses a mobile device 100a, which can be, for instance, "a

data messaging device, a two-way pager, a cellular telephone with data messaging capabilities, a wireless Internet appliance, or a data communication device.”

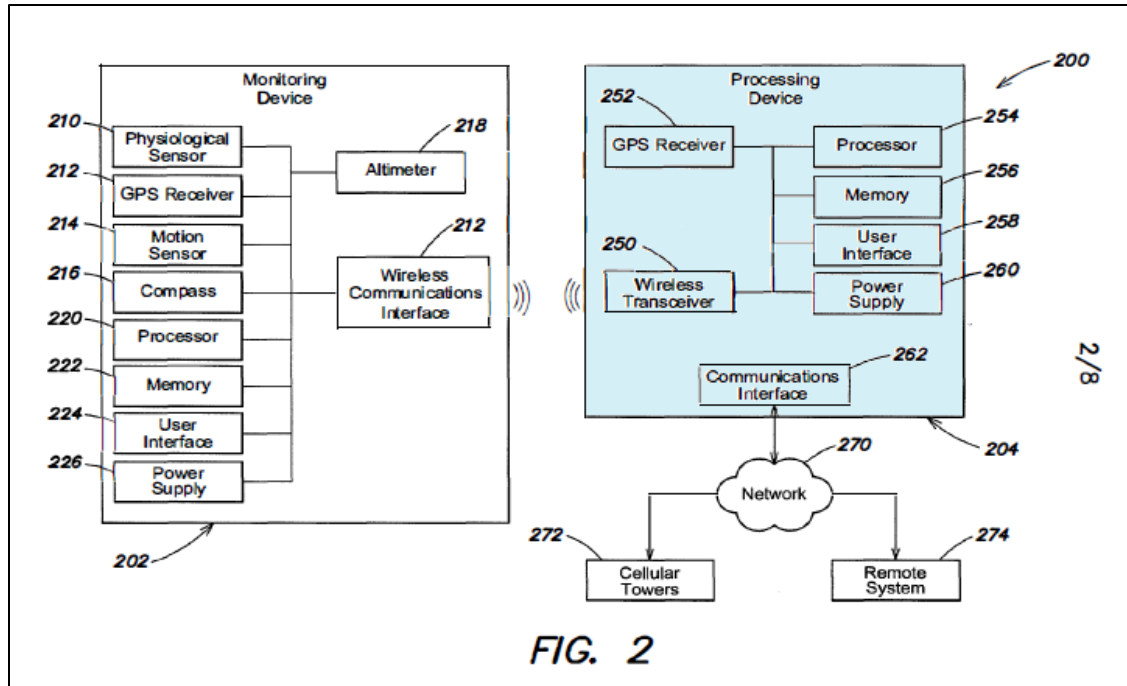
EX1006, ¶¶11, 13, 79 (the mobile device 100a may be “mobile device 100 of FIG. 1”).



EX1006, FIG. 4 (annotated).

220. Weiss also teaches a *mobile device* in the form of its “processing device,” which can be “smartphone,” such as an “iPhone” or “Blackberry.”

EX1007, 12:14-18.



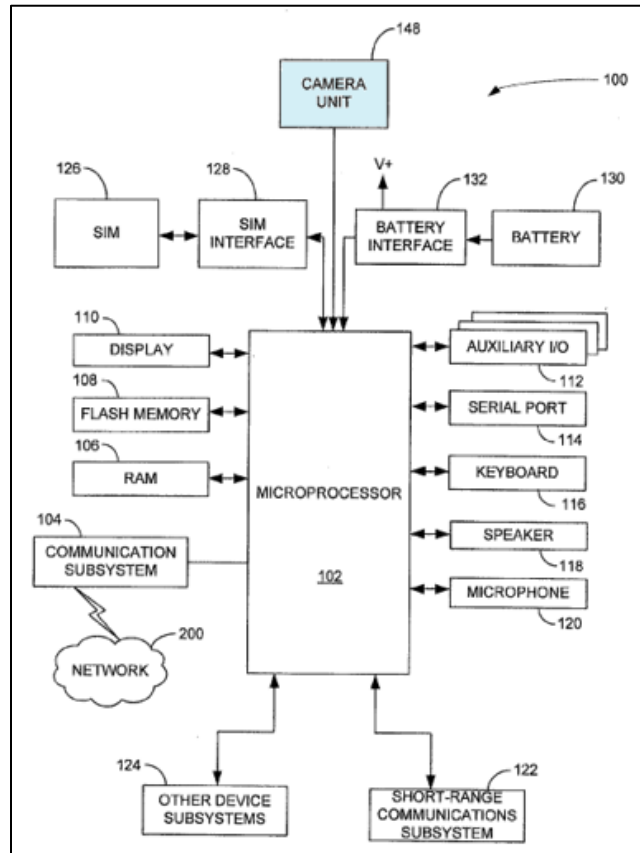
EX1007, FIG. 2 (annotated).

221. As explained in Section XIII.C, the combined Brown-Weiss system includes a mobile device taught by the combination of Brown (e.g., mobile device 100a) and Weiss (e.g., processing device 204) that communicates wirelessly with a monitoring device. As explained below, the combined mobile device teaches the componentry and functionality of the claimed *mobile device*. For instance, the combined mobile device is adapted to implement Brown’s barcode pairing process to establish a wireless communication link, and also to receive and display biometric and activity related information, as taught by Weiss.

b. [1.1] at least one camera sensor, included within the mobile device;

222. Brown-Weiss’s mobile device includes a “camera unit 148” that is “configured to capture an image comprising [a] barcode.” EX1006, ¶¶15, 59. “The

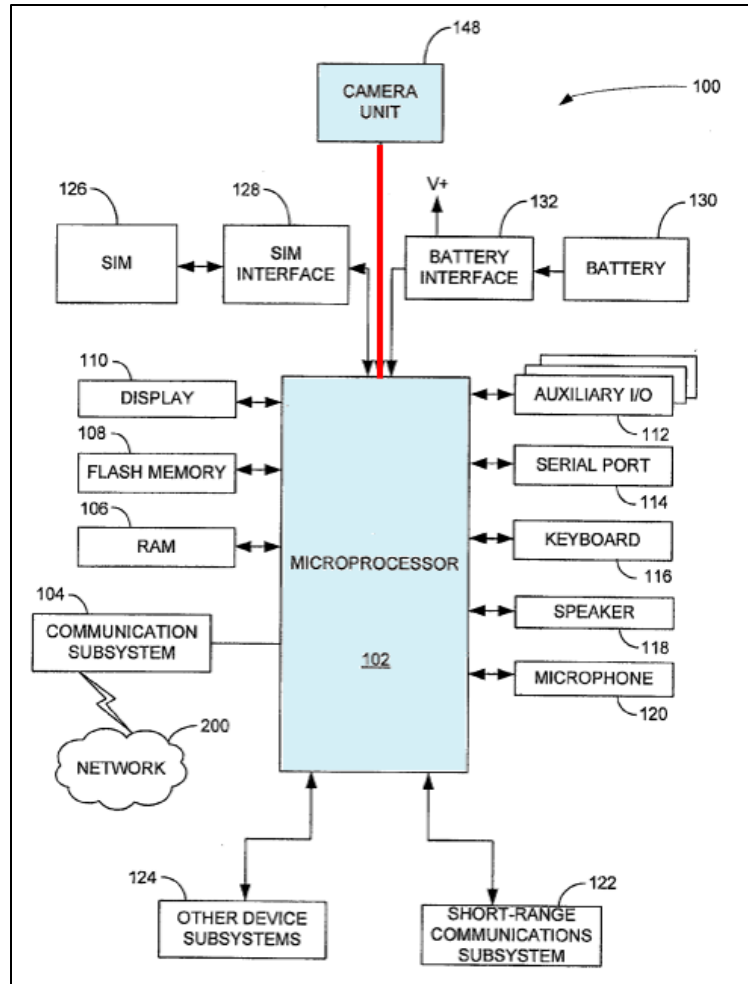
camera... may be built into the [] device itself.” EX1006, ¶83. Thus, the combination of Brown and Weiss teaches this element.



EX1006, FIG. 1 (annotated).

c. [1.2] at least one processor in signal communication with the at least one camera sensor;

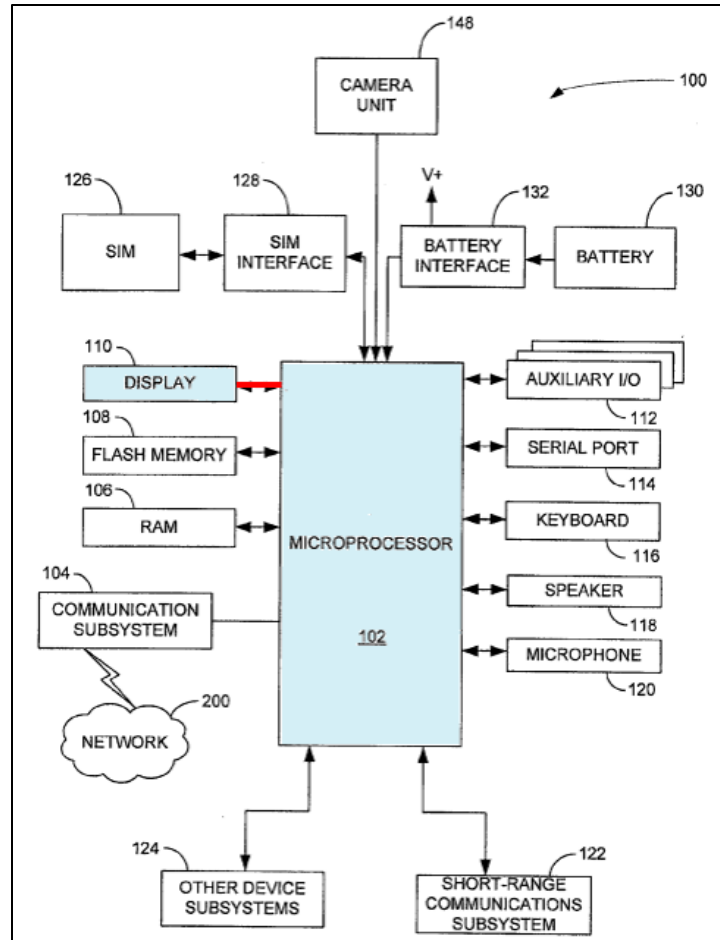
223. Brown-Weiss’s mobile device includes a “[m]icroprocessor 102 [that] controls the overall operation of mobile device.” EX1006, ¶13. The microprocessor “interact[s] with additional subsystems such as... camera unit 148” (is *in signal communication with the at least one camera sensor*). EX1006, ¶15. Thus, the combination of Brown and Weiss teaches this element.



EX1006, FIG. 1 (annotated).

d. [1.3] a display in signal communication with the at least one processor;

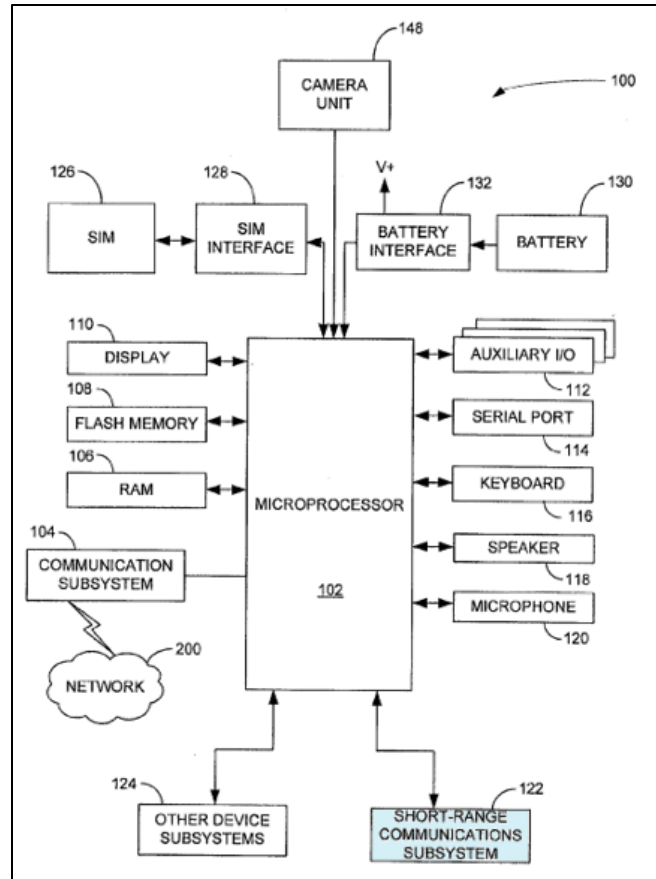
224. Brown-Weiss’s mobile device includes a display 110 that “interact[s] with” (is *in signal communication with*) the microprocessor 102. EX1006, ¶15. For instance, “[m]icroprocessor... processes [] received signal for output to display 110.” EX1006, ¶23. Thus, the combination of Brown and Weiss teaches this element.



EX1006, FIG. 1 (annotated).

- e. **[1.4] communication circuitry configured for wireless communication with an external wearable activity tracking device;**

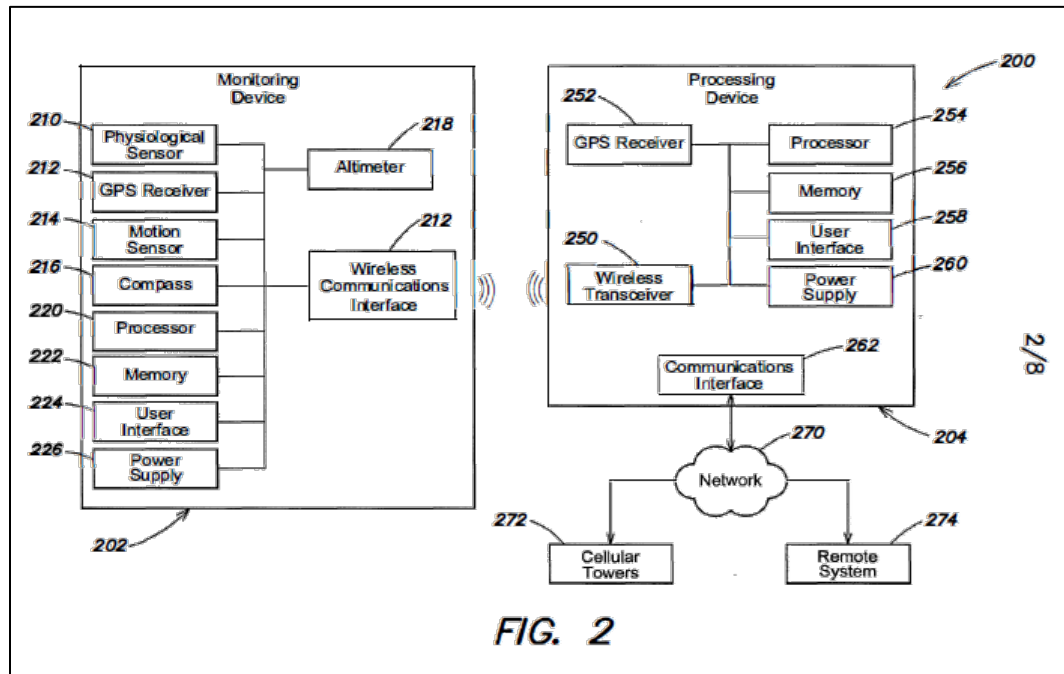
225. Brown-Weiss's mobile device includes a "short-range communications subsystem 122" that "provide[s] for communication between mobile device 100 and different systems or devices." EX1006, ¶¶20, 22. "For example, subsystem 122 may include... circuits and components for short-range communication," including Bluetooth communication (*communication circuitry for wireless communication*). EX1006, ¶22.



EX1006, FIG. 1 (annotated).

226. As explained in Section XIII.C, in the Brown-Weiss system, the mobile device communicates with Weiss's monitoring device. *See* EX1007, 2:8-11. The monitoring device is an *external wearable activity tracking device* as claimed because it is external to the processing device (*mobile device*), and “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. For instance, the monitoring device can be

“integrated into... a wristwatch.” EX1007, 7:26-29.



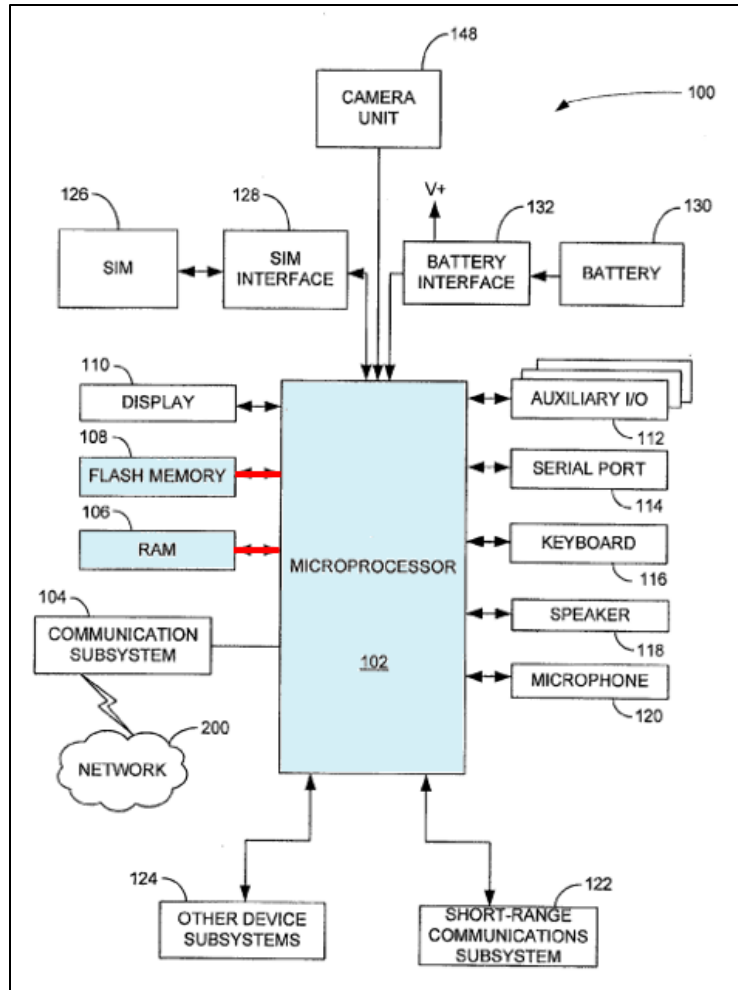
EX1007, FIG. 2.

227. In the Brown-Weiss system, the mobile device would be adapted to communicate with Weiss’s monitoring device over a Bluetooth link using the mobile device’s short-range communication subsystem 122. *See, e.g.*, EX1006, ¶22; EX1007, 12:10-13. Thus, the combination of Brown and Weiss teaches this element.

- f. [1.5] memory, included within the mobile device, associated with one or more processors and configured to store software instructions, which, when executed by the one or more processors, cause the one or more processors to perform operations comprising;

228. Brown-Weiss’s mobile device includes “Random Access Memory (RAM) 106” and “flash memory 108” (*memory*), which “interact with” microprocessor 102. EX1006, ¶15. Flash memory 108 stores, for instance,

“[o]perating system software used by microprocessor 108.” EX1006, ¶16. In the mobile device 100a, “the operating system, specific device applications, or parts thereof, may be temporarily loaded into a volatile store such as RAM 106” to “enable[] execution of software applications on mobile device 100.” EX1006, ¶¶16, 19. For instance, the device “has a Bluetooth pairing application stored in its memory,” that when executed by the microprocessor 102, causes the device to establish a wireless communication link as claimed. EX1006, ¶82, *see also* ¶81 (Pairing functionality “performed by a processor executing an application (e.g., comprising one or more application modules) residing on a second device 100a.”).



EX1006, FIG. 4 (annotated).

229. Thus, the combination of Brown and Weiss teaches this element.

- g. [1.6] Generate, via the mobile device processor, an optical scanning user interface on the mobile device display;**

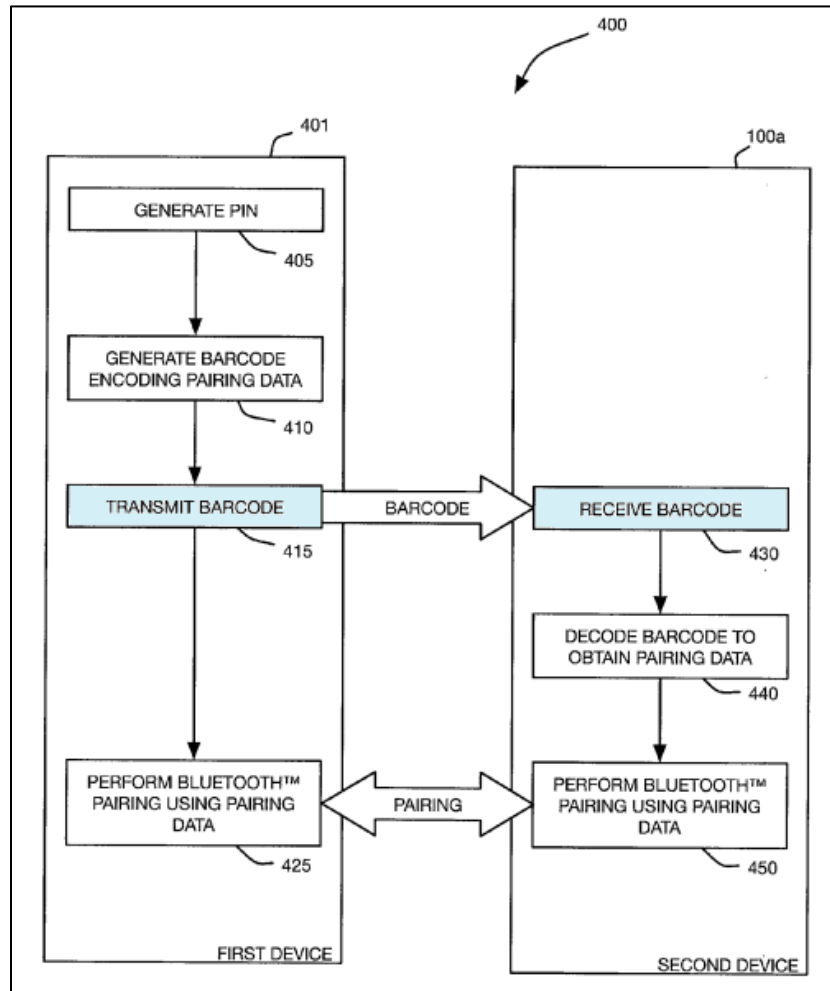
230. Brown-Weiss's mobile device implements a "Bluetooth pairing application" that includes "a user interface" (*optical scanning user interface*) "for the user to scan (e.g., using a camera associated with the device) a barcode that encodes pairing data specifically for initiating Bluetooth pairing." EX1006, ¶82, *see also* ¶91 ("A user may launch the application, which may provide an option, in

a user interface of the second device, for the user to scan (e.g., using a camera associated with the device) a barcode.”). The mobile device generates this user interface, for instance, when the user “launch[es] the application.” EX1006, ¶82. This functionality is performed via the mobile device’s processor. EX1006, ¶81 (Pairing functionality of mobile device “performed by a processor executing an application (e.g., comprising one or more application modules) residing on a second device 100a.”). Thus, the combination of Brown and Weiss teaches this element.

h. [1.7] Detect, via the at least one mobile device camera sensor and the optical scanning user interface, a color coded digital scannable media from a display included within the external wearable activity tracking device,

231. Brown-Weiss’s mobile device scans and captures an image of a “color barcode” (*color coded digital scannable media*) presented on a *display included within a* second device 401. EX1006, ¶¶77, 79, 83, 96. Device 401 “display[s] the image on a display” that is “integrated with” the device. EX1006, ¶79. The device 100a captures this displayed image using the camera and above-described user interface, “detect[s] [that it] comprises a barcode,” and “automatically identif[ies] that [] the barcode comprises Bluetooth pairing data.” EX1006, ¶¶94, 96. This functionality is performed *via the at least one mobile device camera sensor and the optical scanning user interface* because the camera unit 148 (*camera sensor*) captures the image based on the user’s interactions with the “user interface” that

enables the “user to scan [] a barcode.” EX1006, ¶¶82-83, 91 (“A user may launch the application, which may provide an option, in a user interface of the second device, for the user to scan (e.g., using a camera associated with the device) a barcode that encodes pairing data specifically for initiating Bluetooth pairing.”).



EX1006, FIG. 4 (annotated).

232. As explained in Section XIII.C, in the Brown-Weiss system, the mobile device establishes communication with Weiss’s (adapted) monitoring device (*external wearable activity tracking device*) using Brown’s pairing process. In this system, the monitoring device, which corresponds to the device 401 in

Brown's Bluetooth pairing process, generates and displays the color barcode image that is captured by the mobile device in order to "establish wireless connections" between the devices. EX1006, ¶105.

233. 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. For instance, Brown's barcode can be a 2D matrix code, such as a quick response (QR) code, Datamatrix, etc. EX1006, ¶¶36, 75-76 (referring to barcode 710 in Figure 7, which is a QR code). As I explained above, in these barcodes, data is encoded in 2D "cells" depending on the color of the cell, for instance, with dark (black) cells representing 1's and light (white) cells representing 0's. EX1015, 147-48; EX1016, ¶21; *see also* Section VI.A *supra*. A POSA would have understood that, in Brown's color barcode, a first color (e.g., blue) would represent a first value (e.g., "1") and a second color (e.g., grey) would represent a second value (e.g., "0"). Thus, a POSA would have understood that such color barcode is a *color coded digital scannable media*, as claimed because the colors represent different binary data values, and information is thus encoded through the colors.

234. Moreover, a POSA would have recognized that Brown's color barcodes contemplate using more than two colors to encode information because

“different color combinations” could be used. EX1006, ¶76. Indeed, as I explained above, such multi-colored barcodes were well known before the priority date of the ’394 patent. *See* Section VI.A *supra*. As I explained, Microsoft introduced its High Capacity Color Barcode (HCCB) in 2007 and commercialized it in its “Microsoft Tag” product. EX1017, 1; EX1018, 806. An HCCB has rows of strings of symbols (triangles) that can be one of four colors, such as black, red, green, and yellow, each of which encodes different data. EX1017, 1; EX1018, 806. Other examples of color-coded barcodes included the Color Bar Code System from Imageid Ltd. and ColorCode from Colorzip Media. EX1018, 808; EX1019, 710. Similar color-coded barcode solutions were also described in academic literature. *See generally, e.g.*, EX1017; EX1018; EX1019.

235. Based on such known color barcodes, and Brown’s disclosure of a “color barcode” that “employ[s] different color combinations,” EX1006, ¶¶2, 76, it is my opinion that a POSA would have understood Brown to contemplate using color barcodes that use two or more colors to encode data. At the very least, a POSA would have found it obvious to implement such color-coded barcode based on Brown’s disclosure of a “color barcode.” 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.” As I explained, 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. 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 (e.g., HCCB) 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). Indeed, such implementation would merely include changing the type of barcode used in Brown's system. This would be a routine implementation, as evidenced by Brown's disclosure that numerous different barcode types could be used. *See* EX1006, ¶¶36, 75-76.

i. [1.8] wherein the color coded digital scannable media contains wireless pairing information associated with the external wearable activity tracking device;

236. Brown's barcode (*color coded digital scannable media*) "encodes Bluetooth pairing data" comprising "the network address of the [the device 401] (e.g., MAC address)" (*wireless pairing information*) and a "personal identification number (PIN) code." EX1006, ¶¶71, 75. The MAC address is *wireless pairing information because it is used* "for initiating Bluetooth pairing," and "usable to complete a Bluetooth pairing" between devices. EX1006, ¶¶56, 82. The pairing process is used "to establish communications [between devices] for the first time." EX1006, ¶41, *see also* ¶43 ("the devices establish a communication link, in order

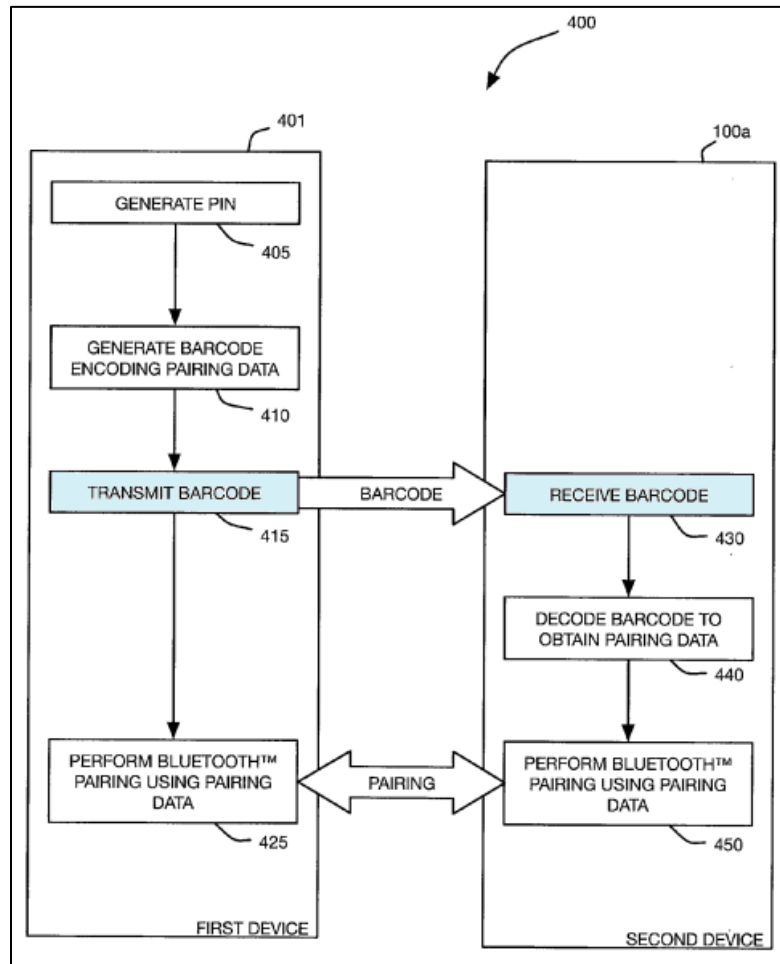
to complete the Bluetooth pairing”). Thus, Brown’s MAC address included in the Bluetooth pairing data comprises *wireless pairing information* because it is used to wirelessly pair devices so that a communication link can be established between the devices.

237. As explained in Section XIII.C, in the combined Brown-Weiss system, the pairing data is encoded and displayed by Weiss’s monitoring device (*external wearable activity tracking device*) to pair the monitoring device with the mobile device. In this system, the pairing data is generated by the monitoring device and includes a network address and PIN code associated with the monitoring device. EX1006, ¶¶71-75.

j. [1.9] Optically obtain, via the at least one mobile device camera sensor, the wireless pairing information from the color coded digital scannable media;

238. Brown-Weiss’s mobile device “receives” and “captures” (*optically obtains*) the “image comprising the barcode” that is displayed by the first device. EX1006, ¶83. The “image is captured” via “camera unit 148” (*camera sensor*) of the device. EX1006, ¶83. This process comprises *optically obtaining the wireless pairing information from the color coded digital scannable media* because the device uses the camera unit (*camera sensor*) to capture (*optically obtain*) the pairing data, including the MAC address (*wireless pairing information*), that is stored in the barcode (e.g., Brown’s color barcode) (*color coded digital scannable*

media).



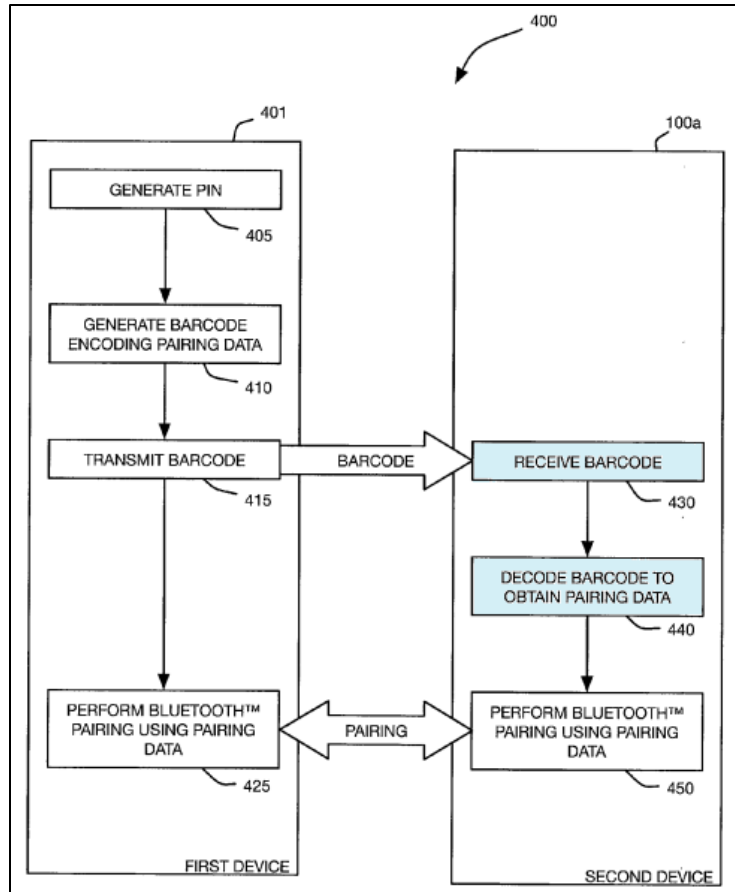
EX1006, FIG. 4 (annotated).

239. Thus, the combination of Brown and Weiss teaches this element.

k. [1.10] Process, via the at least one mobile device processor, the wireless pairing information;

240. Brown-Weiss's mobile device "process[es] the Bluetooth pairing data," including the MAC address (*wireless pairing information*). EX1006, ¶95. For instance, the device may "automatically identify that []the barcode comprises Bluetooth pairing data, and [] automatically process the Bluetooth pairing data accordingly, treating the scan of the barcode as a Bluetooth pairing request."

EX1006, ¶96, *see also* ¶¶60, 99-100. As another example, the device 100a *processes* the pairing data by “extract[ing] the barcode” from the captured image. EX1006, ¶83 (The camera “provide[s] captured data to the processor, for example, in order to extract the barcode and decode the data represented in the barcode. Extraction of the barcode may require processing the captured image to isolate the barcode...”). Yet another example, the device 100a *processes* the pairing data by “decod[ing] the barcode to obtain the Bluetooth pairing data.” EX1006, ¶84. This functionality is performed via the mobile device’s processor. EX1006, ¶¶81 (Mobile device functionality is “performed by a processor executing an application (e.g., comprising one or more application modules) residing on a second device 100a.”), 83 (processor extracts and decodes barcode data).



EX1006, FIG. 4 (annotated).

241. Thus, the combination of Brown and Weiss teaches this element.

- I. [1.11] Establish, via the at least one mobile device processor, a wireless communications link with the external wearable activity tracking device responsive to the processing of the wireless pairing information;

242. Brown-Weiss's mobile device, via its processor, "establish[es] a communication link" with the second device (*establishes a wireless communications link*) using the Bluetooth pairing data. EX1006, ¶43. The communication link is a Bluetooth (wireless) link. EX1006, ¶¶40-41. To establish the link, the mobile device decodes the Bluetooth pairing data from the barcode,

and “transmits Bluetooth pairing data, which depends in part on the PIN code...

decoded from the barcode... to first device 401, and carries out Bluetooth pairing

in known manner.” EX1006, ¶85. The pairing process “establish[es]

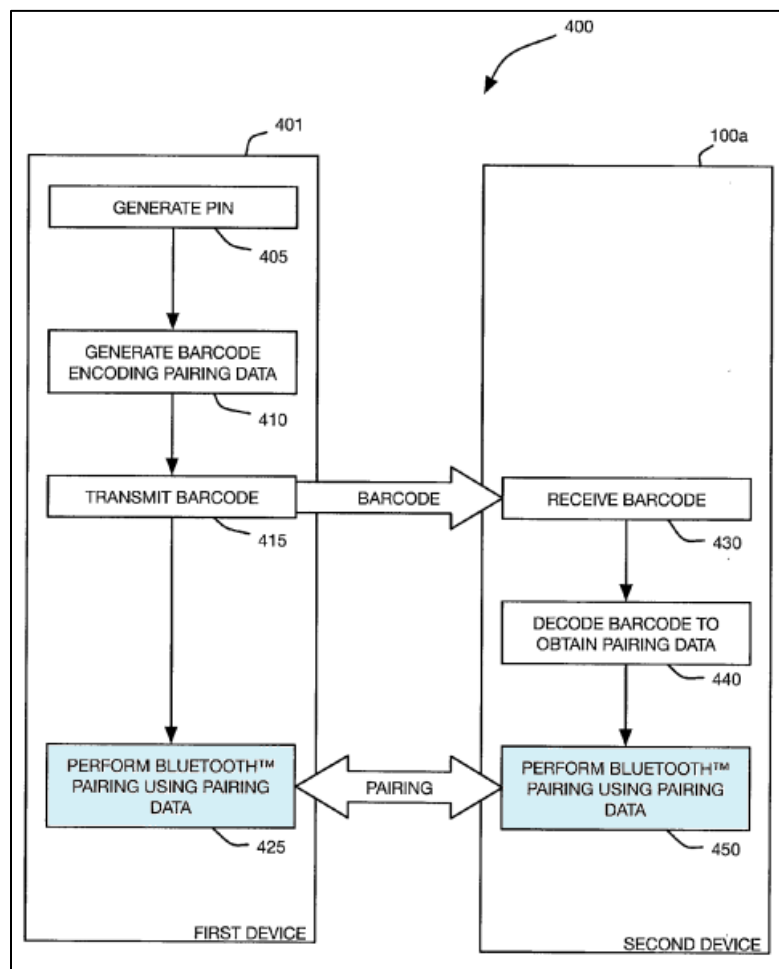
communications [between the devices] for the first time.” EX1006, ¶41, *see also*

¶¶43 (“[T]he devices establish a communication link, in order to complete the

Bluetooth pairing.”), 105 (Pairing used to “establish wireless connections between

devices”). This functionality is performed via the mobile device’s processor.

EX1006, ¶81.

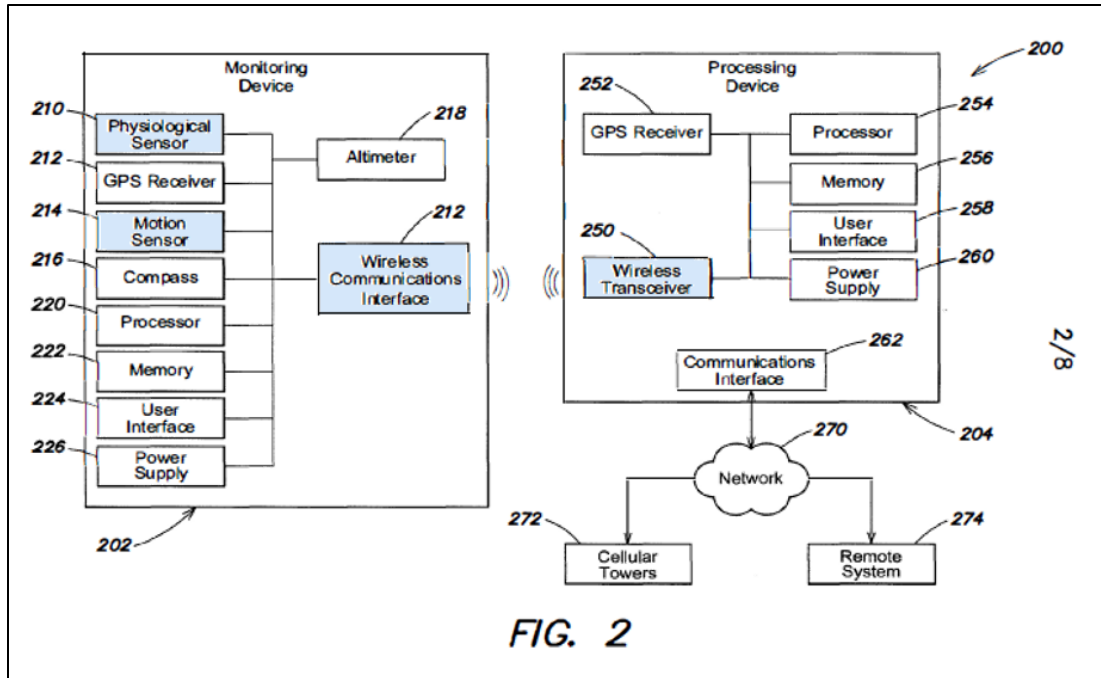


EX1006, FIG. 4 (annotated).

243. As explained in Section XIII.C, in the combined Brown-Weiss system, the mobile device would be paired with Weiss's monitoring device (*external wearable activity tracking device*). As described, these devices would use Brown's device pairing process to "establish a communication link" between them. Thus, the combination of Brown and Weiss teaches this element.

- m. **[1.12] Receive, via the wireless communications link, at least one of activity related information and bio-metric information generated by the external wearable activity monitoring device;**

244. The combination of Brown and Weiss teach this element. Weiss's "monitoring device" (*external wearable activity monitoring device*) communicates with the "processing device" (*mobile device*) through a "wireless communications interface." EX1007, 12:10-11. "The processing device [] includes a wireless transceiver [] that is adapted to receive communications transmitted by [the] monitoring device," for instance, over a Bluetooth link (*wireless communications link*). EX1007, 7:30-8:10, 12:11-13.



EX1007, FIG. 2 (annotated).

245. The processing device “receives data transmitted wireless by [the] monitoring 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 (“[T]he monitoring device [] communicates one or more of the following to the processing device []: sensor data (e.g., physiological data), location data, motion data... etc.”).

246. The processing device thus receives *bio-metric 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.”

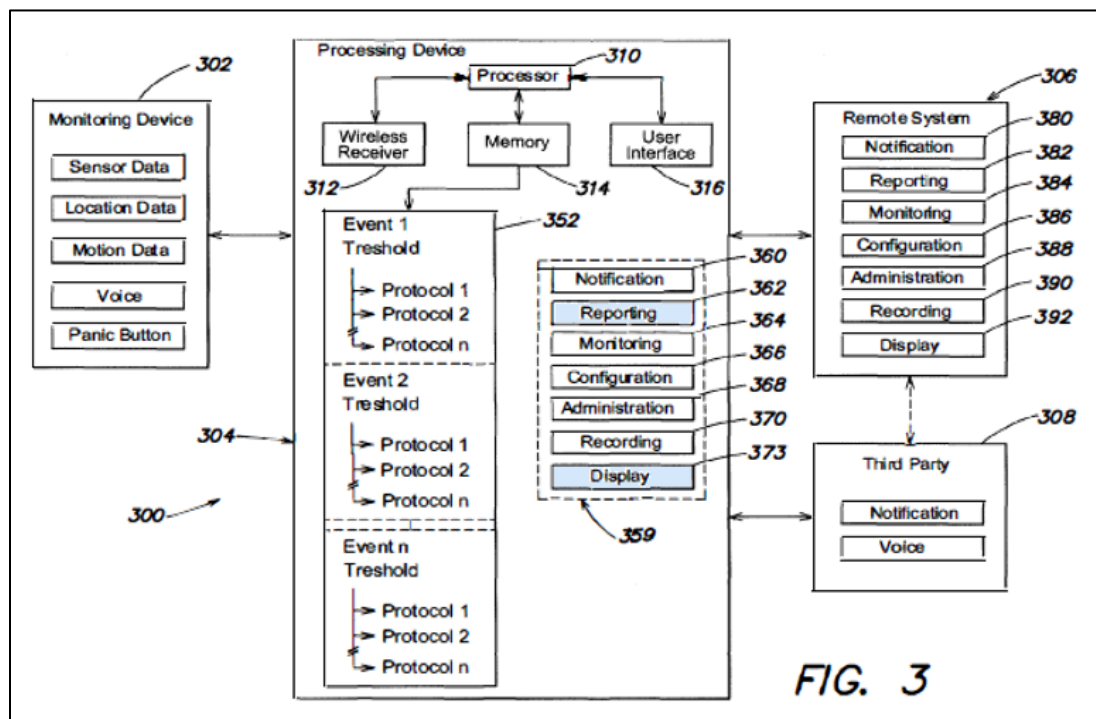
EX1007, 2:11-15, *see also* 21:30-22:5. This information also comprises *activity related information* because it relates to physiological activity of the user (e.g., heart rate). The processing device receives other *activity related information* in the form of, for instance, “motion data” and data relating to “activities of an individual,” etc. EX1007, 13:1-5 (“[P]rocessing device 204 receives data transmitted wirelessly by a monitoring device 202” such as “data or information provided by any of the sensors 210, the GPS receiver 212, the motion sensor 214, the compass 216 and/or other data associated with the physiological attributes, the location and/or activities of an individual using the monitoring device 202.”), *see also* 12:3-9 (“[M]onitoring device 202 may include a motion sensor, such as an accelerometer, and/or a compass for determining rate and/or direction of movement of the user.”), 14:2-5.

247. As explained in Section XIII.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. Thus, the combination of Brown and Weiss teaches this element.

n. [1.13] Display, via the mobile device display, at least one of the activity related information and the biometric information.

248. As explained for element [1.12], Weiss’s monitoring device sends

biometric and activity related information for a user to the processing device (*mobile device*). EX1007, 12:10-13. The processing device then *displays* this information in a user interface. For instance, the processing device includes a “reporting module” that “generat[es] and/or display[s] reports such as charts, tables, figures, data plots versus time or other parameters, summaries, or other compilations of data” relating to “data communicated by the monitoring device.” EX1007, 17:28-31. The processing device “textually” or “graphically” displays data, such as “physiological parameters, location data, motion data, or other data associated with the monitoring device.” EX1007, 19:29-20:4. The processing device also displays “data received from the monitoring device [] in substantially real-time.” EX1007, 20:3-4.



EX1007, FIG. 3 (annotated).

249. Thus, with respect to elements [1.12] and [1.13], Weiss’s monitoring device “communicates... sensor data (e.g., physiological data), location data, [and] motion data” to the processing device. EX1007, 14:2-5. The processing device then displays data “compiled from” this received data, such as in the form of “a list of historical sensor data, such as the heart-rate of a user over a period of time.” EX1007, 17:28-18:4, *see also* 19:29-20:4 (Data including “physiological parameters, location data, motion data, or other data associated with the monitoring device” is displayed in “substantially real-time.”).

250. Thus, the combination of Brown and Weiss teaches this element.

2. Claim 11

- a. **[11.P] A system for establishing a wireless communications link between a wearable activity tracking device and a mobile device, the system comprised of:**

251. The combination of Brown and Weiss teaches this element. As I explained in Section XIII.C, and for claim 1, Brown teaches a *system for establishing a wireless communications link between two mobile devices*. EX1006, Abstract. Weiss teaches a system in which a monitoring device (*wearable activity tracking 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.

b. [11.A.1] The wearable activity tracking device, wherein the wearable activity tracking device is comprised of;

252. The combination of Brown and Weiss teaches this element for the reasons provided for element [1.4].

c. [11.A.2] A display device;

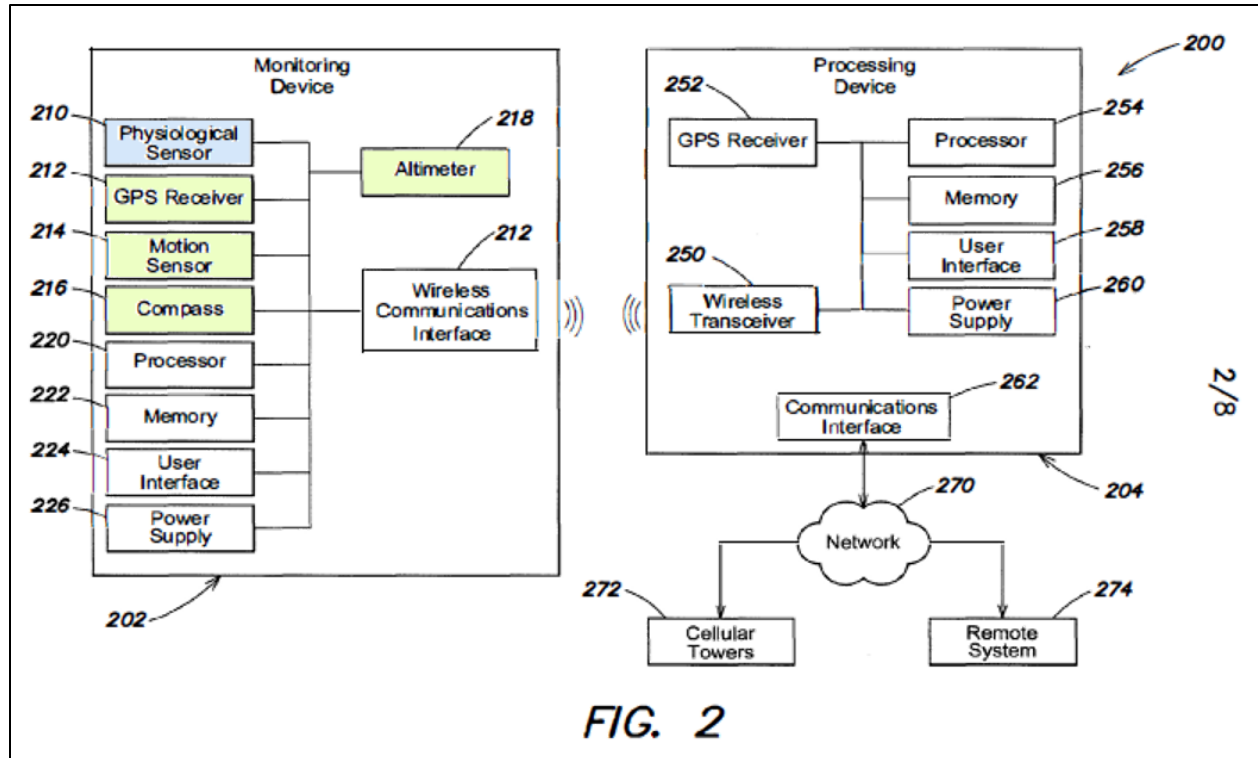
253. The combination of Brown and Weiss teaches this element. Weiss's monitoring device includes a "user interface 224." EX1007, 11:14-16. Brown's device 401 includes a display, on which it displays the barcode image. EX1006, ¶¶37, 75, 79, *see also* ¶16. In the combined system, to the extent Weiss's monitoring device's user interface does not include a display device, it would be adapted to implement a display device for displaying barcode images as explained in Section XIII.C. Thus, the combined Brown-Weiss monitoring device includes a *display device*.

d. [11.A.3] At least one of an activity tracking capability and an embedded bio-metric monitoring sensor associated with the wearable activity tracking device;

254. As explained for elements [1.4] and [1.12], Weiss's monitoring device (*wearable activity tracking device*) includes "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” (*bio-metric sensors*). EX1007, 2:11-15, *see also* 7:21-23 (“Each sensor 112 can detect and measure, for example, one or a plurality of physiological attributes such as pulse, blood oxygen level, temperature, respiration, or other vital signs.”), 11:26-29. The ability to detect such physiological attributes also constitutes an *activity tracking capability* because the monitoring device tracks physiological activity of the user (e.g., heart rate, pulse).

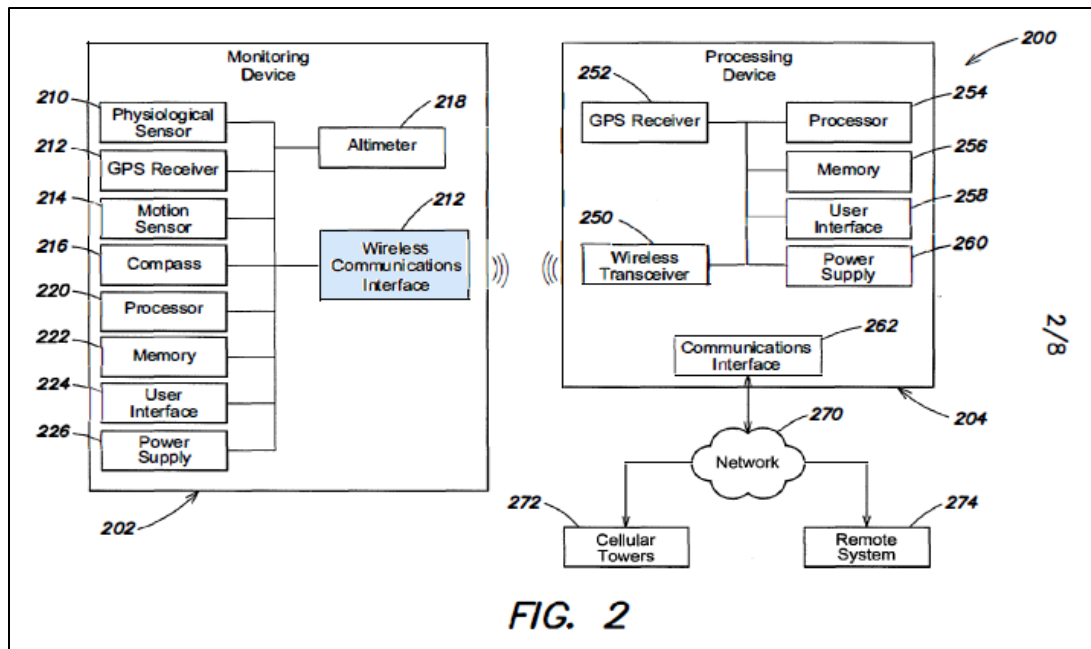
255. The monitoring device includes additional *activity tracking capabilities* because it includes “a GPS receiver 212, a motion sensor 214 (e.g., accelerometer), a compass 216, and/or an altimeter 218 for detecting the location and motion of an individual wearing the device.” EX1007, 11:12-14, *see also* 12:3-9 (“[M]onitoring device [] is adapted to determine a location and/or a movement of the user.”).



EX1007, FIG. 2 (annotated).

- e. **[11.A.4] Wireless communication circuitry, wherein the wireless communication circuitry is configured to establish a wireless communications link with the mobile device;**

256. Weiss's monitoring device (*wearable activity tracking device*) includes a "wireless communications interface" that is a "Bluetooth™-compatible transmitter." EX1007, 11:10-12, *see also* 7:30-8:2 ([M]onitoring 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 enable wireless communication with the processing device (*mobile device*) using, for instance, the Bluetooth protocol.



EX1007, FIG. 2 (annotated).

- f. **[11.A.5] at least one processor with software, wherein the at least one 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;**

257. The combination of Brown and Weiss teaches this element. 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 monitoring device also includes "memory 222," which "may be, for example, static RAM, dynamic RAM, ROM, EPROM, EEPROM, or flash memory." EX1007, 11:14-19.

258. Moreover, as explained in Section XIII.C, the combined Brown-Weiss monitoring device is adapted to implement Brown's wireless pairing process. The combined monitoring device includes "software instructions stored on physical

computer-readable storage media 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. 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 (Pairing method “performed by a processor of the device.”), 57.

- g. [11.A.6] the memory device, wherein the memory device is configured to store wireless pairing information associated with the wireless communication circuitry;**

259. The combination of Brown and Weiss teaches this element. As explained for element [11.A.5], Weiss’s monitoring device includes “memory” 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, such as a “Bluetooth communication interface.” EX1006, ¶70, *see also* ¶¶15-16, 22. Brown’s memory is configured to store Bluetooth pairing data, including the MAC address (*wireless pairing information*), that is *associated with* the Bluetooth communication interface. 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.

260. Indeed, because the Bluetooth MAC address must be globally unique to identify a specific device, it is assigned through coordination by a registration authority and the device manufacturer to ensure that no two devices share the same address. *See, e.g.*, EX1029, ¶8 (“The uniqueness of [the Bluetooth] address is guaranteed by the IEEE (Institute of Electrical and Electronic Engineers) organization, which assigns communicating device manufacturers part of the specific address for each physical device placed in circulation.”). Upon assignment of the address, it is stored in non-volatile memory, and is accessed from this memory to communicate with other devices. EX1029, ¶¶13-14 (“[U]nique [Bluetooth] address” is written into memory of the device during “service activation” of the device.). The Bluetooth address is used by the system “to implement the core Bluetooth functionality.” EX1021, 2:16-24. For instance, the address is used “during physical connection establishment,” “device discovery,” and to “maintain link layer security.” EX1021, 2:16-24.

- h. [11.A.7] wherein the at least one processor software is configured to; obtain, from the memory device, the wireless pairing information associated with the wireless communication circuitry;**

261. The combination of Brown and Weiss teaches this element for the reasons I provided for element [11.A.6]. In particular, to generate a barcode encoding Bluetooth pairing data, including the PIN code and MAC address,

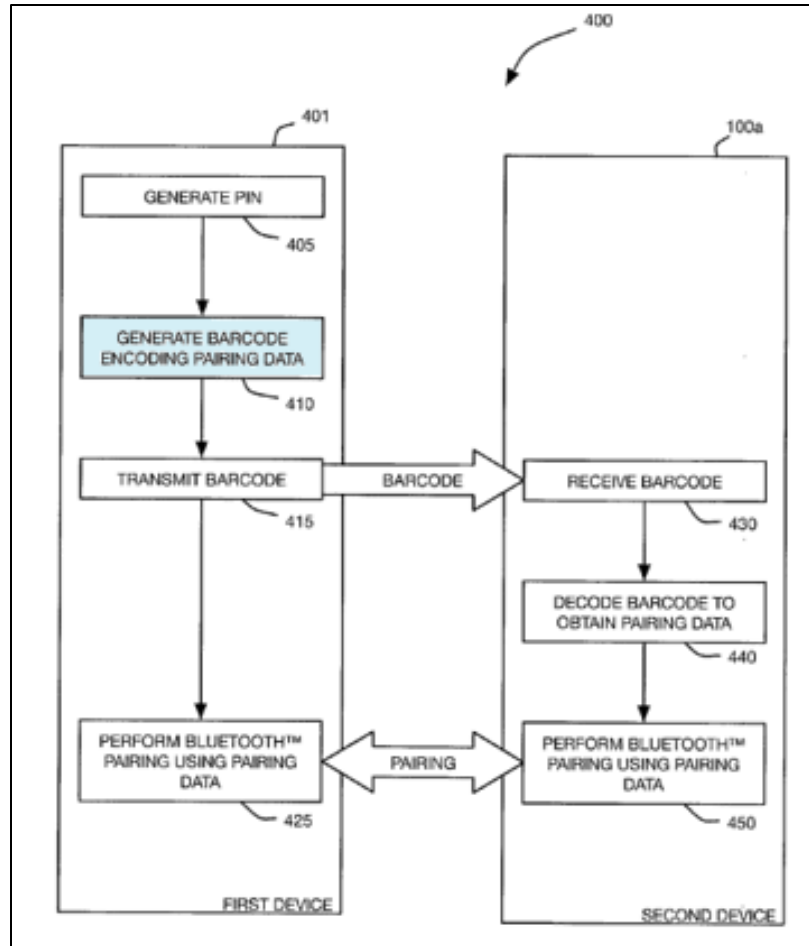
Brown's device 401, via its processor software, "select[s]" (*obtains*) the PIN code that is "stored in memory." EX1006, ¶72, *see also* ¶75. A POSA would have also understood that the device also *obtains* the MAC address from memory because as explained above, it is a "unique network address that [was] assigned to [the] device (i.e., when it [was] manufactured)," and is thus stored in memory. EX1006, ¶40.

The device accesses this address from memory to encode it in the barcode.

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.

i. [11.A.8] generate a color coded digital scannable media image responsive to the wireless pairing information;

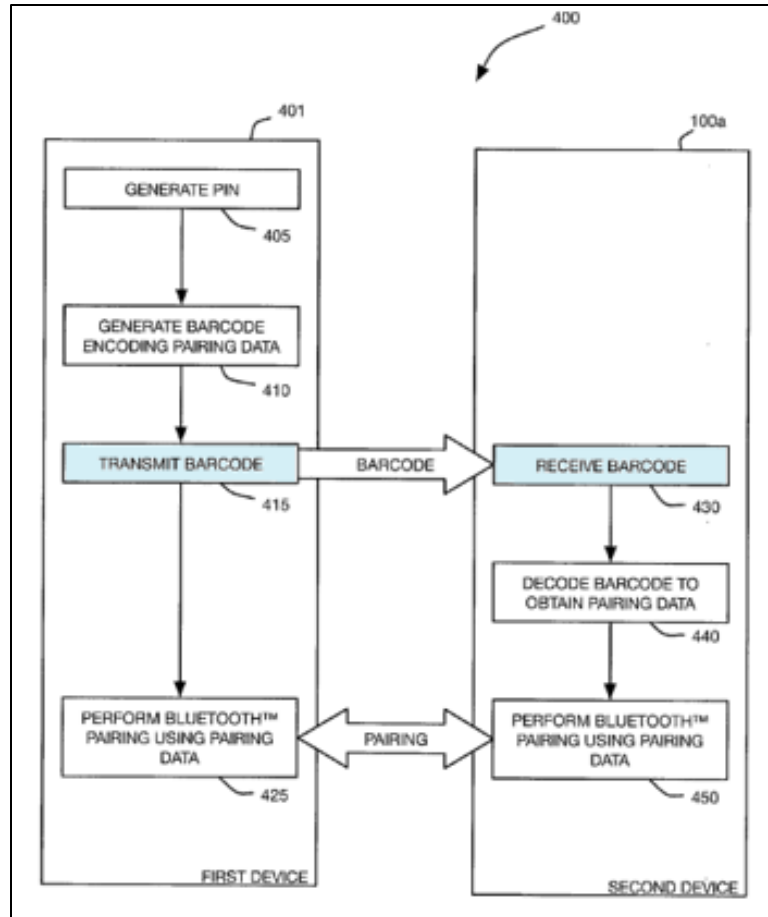
262. As explained for element [1.7], Brown's device 401 "encodes Bluetooth pairing data" to generate a "color barcode." EX1006, ¶¶2, 75-76. As also explained, Brown's "color barcode" teaches or renders obvious the *color coded digital scanning media*.



EX1006, FIG. 4 (annotated).

- j. [11.A.9] control the display device, wherein the display device is configured to display the color coded digital scannable media image;

263. Upon generating the image of the color barcode (*color coded digital scannable media image*) encoding the Bluetooth pairing data, Brown's device 401 controls the display device by "display[ing] the image on a display." EX1006, ¶79, *see also* ¶37 ("[A] barcode is generated by a first device, and displayed as an image on a display associated with the first device, to be subsequently read using a camera or other similar hardware component of a second device.").



EX1006, FIG. 4 (annotated).

- k. [11.A.10] 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;

264. The combination of Brown and Weiss teaches this element for the reasons provided for element [1.11]. Specifically, Brown’s pairing process “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”).

l. [11.A.11] Generate at least one of activity tracking information and bio-metric information;

265. The combination of Brown and Weiss teaches this element for the reasons provided for element [1.12]. Specifically, Weiss's monitoring device includes "a plurality of sensors for detecting one or more physiological attributes." (*bio-metric 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. As explained, the monitoring device generates this information via the sensors and transmits it to the processing device. EX1007, 13:1-12. The Brown-Weiss monitoring device generates 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"). It does so using the *processor software* taught by the combination of Brown and Weiss. *See, e.g.*, EX1006, ¶¶57, 106.

m. [11.A.12] Communicate, via the wireless communications link, at least one of the activity tracking information and the bio-metric information to the mobile device; and

266. The combination of Brown and Weiss teaches this element for the reasons provided for element [1.12].

- n. **[11.B.1] The mobile device, wherein the mobile device is comprised of; at least one camera sensor, included within the mobile device;**

267. The combination of Brown and Weiss teaches this element for the reasons provided for elements [1.P] and [1.1].

- o. **[11.B.2] at least one processor in signal communication with the at least one camera sensor;**

268. The combination of Brown and Weiss teaches this element for the reasons provided for element [1.2].

- p. **[11.B.3] a display in signal communication with the at least one processor;**

269. The combination of Brown and Weiss teaches this element for the reasons provided for element [1.3].

- q. **[11.B.4] communication circuitry configured for wireless communication with the wearable activity tracking device;**

270. The combination of Brown and Weiss teaches this element for the reasons provided for element [1.4].

- r. **[11.B.5] memory, included within the mobile device, associated with one or more processors and configured to store software instructions, which, when executed by the one or more processors, cause the one or more processors to perform operations comprising;**

271. The combination of Brown and Weiss teaches this element for the reasons provided for element [1.5].

- s. **[11.B.6] Generate, via the mobile device processor, an optical scanning user interface on the mobile device display;**

272. The combination of Brown and Weiss teaches this element for the reasons provided for element [1.6].

- t. **[11.B.7] Detect, via the at least one mobile device camera sensor and the optical scanning user interface, a color coded digital scannable media from the display included within the wearable activity tracking device, wherein the color coded digital scannable media contains wireless pairing information associated with the wearable activity tracking device;**

273. The combination of Brown and Weiss teaches this element for the reasons provided for elements [1.7] and [1.8].

- u. **[11.B.8] Optically obtain, via the at least one mobile device camera sensor, the wireless pairing information from the color coded digital scannable media;**

274. The combination of Brown and Weiss teaches this element for the reasons provided for element [1.9].

- v. **[11.B.9] Process, via the at least one mobile device processor, the wireless pairing information;**

275. The combination of Brown and Weiss teaches this element for the reasons provided for element [1.10].

- w. **[11.B.10] Establish, via the at least one mobile device processor, a wireless communications link with the wearable activity tracking device responsive to the processing of the wireless pairing information;**

276. The combination of Brown and Weiss teaches this element for the

reasons provided for element [1.11].

- x. **[11.B.11] Receive, via the wireless communications link, at least one of activity related information and bio-metric information generated by the wearable activity tracking device;**

277. The combination of Brown and Weiss teaches this element for the reasons provided for element [1.12].

- y. **[11.B.12] Display, via the mobile device display, at least one of the activity related information and the bio-metric information.**

278. The combination of Brown and Weiss teaches this element for the reasons provided for element [1.13].

E. Dependent Claims

1. Claims 2 and 13

279. Claims 2 and 13 recite “wherein the mobile device is at least one of a smartphone device and a tablet device.”

280. Brown-Weiss’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).”).

281. 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.

2. Claim 3

282. Claim 3 recites “wherein the wireless communications link is a two-way wireless communications link.”

283. Brown-Weiss’s *wireless communications link* is implemented using the Bluetooth protocol, which is “a voice and data wireless communication protocol commonly used for short-range communications between electronic devices.” EX1006, ¶40. A POSA would have understood that Bluetooth communication links are *two-way wireless communications links*. See EX1021, 1:11-64 (discussing Bluetooth communication techniques including “packet exchange” and devices that transmit and receive packets); EX1023, ¶¶4-6 (Bluetooth “devices talk to one another by creating a common language between them.”).

3. Claims 4 and 15

284. Claims 4 and 15 recite “wherein the wireless pairing information includes at least one of a MAC address identifier associated with the [external] wearable activity tracking device and a unique identification number associated

with the [external] wearable activity tracking device.”

285. Brown’s Bluetooth pairing data includes a MAC address of the device 401(*wireless pairing information*). EX1006, ¶75. In the combined Brown-Weiss system, the MAC address would be associated with Weiss’s monitoring device (*wearable activity tracking device*). A POSA would have understood that this MAC address is also a *unique identification number* because the device is a “unique network address” that “identifie[s]” the device. EX1006, ¶40, *see also* ¶56; EX1021, 2:16-18 (“To facilitate pairing, each Bluetooth device is associated with a unique 48-bit address known as the Bluetooth Device Address.”).

4. Claims 5 and 17

286. Claims 5 and 11 recite “wherein the color coded digital scannable media [displayed by the wearable activity tracking device] 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, a augmented reality marker, a augmented reality image, and a augmented reality code.”

287. As explained for element [1.7], Brown teaches or renders obvious the claimed *color coded digital scannable media*. 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; Section VI.A *supra*.

288. For instance, as I explained, Brown’s color barcode encodes data through colors. An example of such barcode is the HCCB, which is a *2D matrix code* and a *representation of non-human readable information using colored pixels*. EX1019, 2 (HCCB is an example of a “2D barcode[]” and “use[es] colors to create more symbols, resulting in larger data capacity within the same size”); EX1017, 1 (HCCB is “2D” barcode that implements “four colors: black, red, green and yellow” to encode machine-readable information.). The HCCB is a 2D matrix code because it encodes data using symbols in two dimensions. It also encodes *non-human readable information using colored pixels* for the reasons I provided in Section VI.A. Indeed, a POSA would have understood that the Brown’s image of the color barcode implements color using pixels.

5. Claims 6 and 18

289. Claims 6 and 18 recite “wherein the activity related information is generated by the [external] wearable activity tracking device from an accelerometer included within the [external] wearable activity tracking device.”

290. Brown-Weiss’s monitoring device (*wearable activity tracking device*) includes an “accelerometer... for detecting the location and motion of an individual wearing the device” (*activity-related information*). EX1007, 2:12-14, *see also* 12:6-8, 14:2-5 (monitoring device communicates “location data” and “motion data” to the processing device).

6. Claims 7 and 16

291. Claims 7 and 16 recite “wherein the bio-metric information is generated by the [external] wearable activity tracking device from at least one of a blood pressure sensor, a heart rate sensor, a blood glucose sensor, a body fat sensor, and a temperature within the [external] wearable activity tracking device.”

292. Brown-Weiss’s monitoring device generates *bio-metric information* from “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. Weiss’s sensors also detect “blood pressure” and “blood glucose.” EX1007, 23:9-15.

7. Claims 8 and 12

293. Claim 8 recites “wherein the 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 external wearable activity tracking device.”

294. Claim 12 recites “wherein the wearable activity tracking device 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.”

Brown-Weiss's *communication circuitry* is configured to implement a Bluetooth wireless connection link, which is a *personal area network communications link*. See EX1006, ¶¶22, 40, 70; see also EX1021, 1:11-24; EX1023, ¶4. Indeed, the “Bluetooth protocol is a voice and data wireless communication protocol commonly used for short-range communications between electronic devices.” EX1006, ¶40.

8. Claim 14

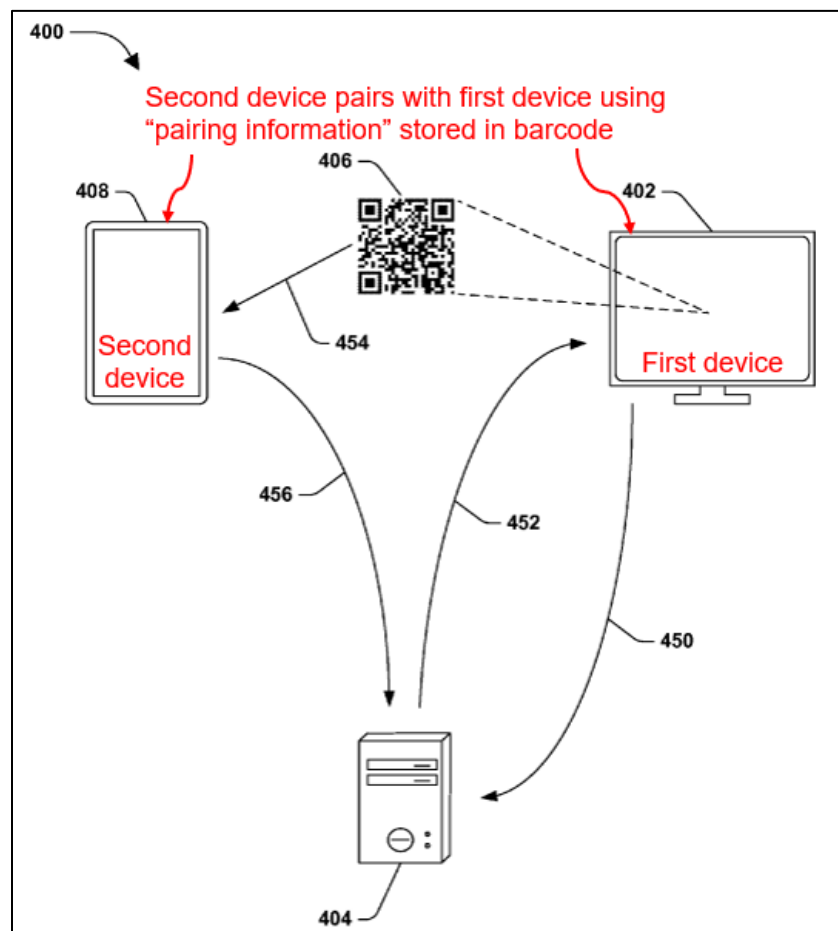
295. Claim 14 recites “wherein the wearable activity tracking device is at least one of a smartwatch device and a wearable health monitoring device.”

296. Brown-Weiss's monitoring device (*wearable activity tracking device*) is a wearable health monitoring device for the reasons provided for element [1.4]. See EX1007, 2:8-9:4. 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.

XIV. GROUND 3B: BROWN-WEISS FURTHER IN VIEW OF ORT TEACHES CLAIMS 1-8, 11-18

297. As explained in Section XIII, Brown-Weiss renders obvious all elements of claims 1-8 and 11-18. 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. 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).

298. 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. As explained, Brown at the very least *suggests* the use of color-coded barcodes through its disclosure of a "color barcode." See EX1006, ¶¶2, 76, *see also* ¶¶36, 75. As I explained in Section VI.A, Microsoft commercialized its High Capacity Color Barcode (HCCB) in 2007, well before the priority date of the '394 patent.

299. As I also explained, an HCCB has rows of strings of symbols (triangles) that can be one of four colors, such as black, red, green, and yellow, each of which encodes different data. EX1017, 1; EX1018, 806. HCCBs are advantageous over black and white barcodes because they provide a higher data density. EX1018, 807; EX1019, 710. For instance, where black-and-white barcodes encode one bit per symbol (either 0 or 1), a color barcode having four colors can represent two bits per symbol (00, 01, 10, or 11). This doubles the data density compared to black-and-white barcodes. Similarly, an 8-color barcode encodes three bits per symbol (000, 001, 010, etc.), which triples the data density compared to black-and-white barcodes. This allows the same amount of information to be represented in fewer symbols and thus allows the physical size of the barcode to be smaller. EX1020, 173 (A color barcode "convey[s] more information within the same space, allowing for a significant reduction in the

number of regions needed to convey the necessary information.”). This also makes it easier for the reading device (camera) to recognize and extract information from the barcode. EX1020, 173.

300. A POSA would have thus recognized the benefits and applicability of implementing Ort’s HCCB in Brown-Weiss. A POSA would have been motivated to implement Ort’s HCCB in Brown-Weiss to provide a barcode with greater data density, which would allow the barcode to have a smaller physical size. A POSA would have also readily been able to implement Ort’s HCCB based on Brown’s disclosure of using a barcode employing different color combinations. EX1006, ¶76. A POSA would have thus 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).

301. 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, and a POSA would not have had any trouble implementing Ort’s disclosures in Brown-Weiss. That is, the implementation of Ort’s HCCB represents a discrete modification that would not alter Brown’s pairing process, as implemented in Weiss. In the Brown-Weiss-Ort system, the devices would be adapted to encode/decode data in known manners in accordance with known

HCCB protocols. Outside of this encoding/decoding process, the Brown-Weiss pairing process would be implemented as explained in Section XIII.

302. Thus, the combination of Brown, Weiss, and Ort renders obvious the claimed *color coded digital scannable media*. 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 5 and 17 for the reasons I provided in Section XIII.E.4. Brown-Weiss-Ort renders obvious all other elements of claims 1-8 and 11-18 for the reasons provided in Section XIII.

XV. GROUNDS 4A AND 4B: BROWN-WEISS AND BROWN-WEISS-ORT FURTHER IN VIEW OF WILLIAMS RENDERS OBVIOUS CLAIMS 9, 10, 19, AND 20

1. Claims 9, 10, 19, and 20

303. Claims 9 and 19 recite “wherein the wireless pairing information is at least partially encrypted by the [external] wearable activity tracking device.” Claims 10 and 20 recite “wherein the processing [by the at least one mobile device] further includes decrypting the wireless pairing information after the mobile device optically detects the color coded digital scannable media displayed by the [external] wearable activity tracking device.”

304. As explained in Section XII, Williams teaches a Bluetooth pairing process in which a first device encrypts wireless pairing information that is encoded in a barcode image, and a second device captures the image and decrypts

pairing information to establish the Bluetooth connection. EX1009, ¶¶26-28, 29.

305. In particular, Williams teaches that its wireless pairing information is “encrypted” using various “encryption method[s].” EX1009, ¶¶26-28, 29. This results in an “encrypted image containing the” wireless pairing information. EX1009, ¶28. Although it does not expressly state that the pairing information is decrypted by the image-capturing device, a POSA would have understood that, when the pairing information encoded in the image is encrypted, the image-capturing device would need to decrypt it to use it for establishing the wireless link.

306. Indeed, for a device that receives encrypted data to understand that data, the device must first decrypt it. This holds true when the encrypted data is encoded in a barcode. For instance, Ross discloses encrypting medical data and “display[ing] the encrypted medical information in a machine readable format such as a barcode.” EX1027, ¶169. The barcode is scanned “to obtain encrypted medical information,” which is “decrypt[ed]... using the decryption key.” EX1027, ¶¶170, 173, *see also* ¶91 (describing encryption/decryption process). Accordingly, a POSA would have readily understood that Williams teaches decryption as a counterpart to its expressly disclosed encryption. The decryption method is counterpart to the chosen “encryption method.” EX1009, ¶29.

307. I also note that the ’394 patent similarly does not expressly disclose

decrypting data, even though it does disclose barcodes storing encrypted data. *See, e.g.,* EX1001, 4:39-46, 13:48-55, 22:35-53, 28:58-65. This confirms my opinion that a POSA would have readily understood that a reference, such as Williams, that teaches encryption techniques, also teaches corresponding decryption techniques.

308. 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. 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.

309. Indeed, as I explained above, encryption/decryption was a well-known technique for implementing secure communications. Furthermore, it was well known to encrypt/decrypt information encoded in barcodes. EX1027, ¶¶91, 170, 173; EX1028, ¶39 ("The cell phone device may compute encrypted validation codes" and "display a barcode having... the computed encrypted validation code.").

310. A POSA would have thus found it obvious to encrypt/decrypt 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. Indeed, encryption was commonly performed to secure data and a POSA would have

readily understood how to implement Williams's encryption techniques. A POSA would have readily understood how to encode encrypted data in a barcode, and then to decrypt that data to obtain and use it. For instance, a POSA would have understood how to implement suitable known encryption/decryption schemes (e.g., asymmetric encryption using a public/private key system), and how to generate or provision appropriate keys for encrypting and decrypting the data. Such implementations would merely require the use of routine and conventional encryption techniques that were widely used and well-understood in the field. *See, e.g.,* EX1009, ¶¶9, 41, 43. Accordingly, 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).

311. Thus, it is my opinion that the combination of Brown, Weiss, and Williams, and the combination of Brown, Weiss, Ort, and Williams renders obvious claims 9, 10, 19, and 20.

XVI. OBJECTIVE INDICIA

312. To the extent that Patent Owner presents objective indicia during this proceeding, I reserve the right to review and opine on such evidence when presented.

XVII. CONCLUSION

313. In signing this declaration, I recognize that the declaration will be filed as evidence in an *inter partes* review before the Patent Trial and Appeal Board of the United States Patent and Trademark Office. I also recognize that I may be subject to cross-examination in the case and that cross-examination will take place within the United States. If cross-examination is required, I will appear for cross-examination within the United States during the time allotted.

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

Executed on this 14th day of May 2026, in Los Angeles, CA.



Prashant Shenoy, Ph.D.