

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner

v.

SECURE COMMUNICATION TECHNOLOGIES, LLC,
Patent Owner

Case IPR2026-00445
U.S. Patent No. 11,334,918

**PETITION FOR *INTER PARTES* REVIEW
OF U.S. PATENT NO. 11,334,918**

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

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	THE '918 PATENT	2
	A. Summary	2
	B. Prosecution History	4
	C. Person of Ordinary Skill in Art (POSITA)	5
III.	CLAIM CONSTRUCTION	5
IV.	FOUNDATIONS	5
V.	GROUND 1: RIBAUDO-WATANABE RENDERS OBVIOUS CLAIMS 1, 4-6, 9, 14, 16-22, AND 24-30	7
	A. Ribaudó.....	7
	B. Watanabe	9
	C. Motivation to Combine	11
	D. Independent Claim 1	15
	1. 1[pre]	15
	2. 1[a]	16
	3. 1[b]	17
	4. 1[c]	18
	5. 1[d]	18
	6. 1[e]	20
	7. 1[f][1]	23
	8. 1[f][2]	27
	9. 1[g]	33
	10. 1[h]	36
	E. Independent Claim 9	39
	F. Dependent Claims 4-6, 14, 16-22, and 24-30	40
	1. Claim 4	40
	2. Claim 5	42
	3. Claim 6	43

4.	Claims 14/19	45
5.	Claims 16/24	46
6.	Claim 17	47
7.	Claims 18/28	48
8.	Claim 20	48
9.	Claim 21	49
10.	Claim 22	50
11.	Claim 25	52
12.	Claim 26	52
	a. 26[pre]	52
	b. 26[a]	52
	c. 26[b]	53
	d. 26[c]	54
	e. 26[d]	54
	f. 26[e]	55
13.	Claim 27	56
14.	Claim 29	56
15.	Claim 30	57
	a. 30[pre]	57
	b. 30[a]	57
	c. 30[b]	58
	d. 30[c]	59
VI.	GROUND 2: RIBAUDO-WATANABE-BEHRENS RENDERS OBVIOUS CLAIMS 3, 7-8, 10, 12-13, 15, AND 31	60
	A. Behrens	60
	B. Motivation to Combine	61
	C. Dependent Claims 3, 7-8, 10, 12-13, 15, and 31	65
	1. Claim 3	65
	a. 3[pre]	65

b.	3[a].....	65
c.	3[b].....	66
d.	3[c].....	69
2.	Claim 7.....	71
3.	Claim 8.....	71
4.	Claim 10.....	71
a.	10[pre].....	71
b.	10[a].....	71
c.	10[b].....	71
d.	10[c].....	72
5.	Claim 12.....	72
a.	12[pre].....	72
b.	12[a].....	72
c.	12[b].....	72
d.	12[c].....	73
6.	Claims 13/15	73
7.	Claim 31	76
VII.	GROUND 3: RIBAUDO-WATANABE-BEHRENS-NORDMAN RENDERS OBVIOUS CLAIMS 2 AND 11	76
VIII.	GROUND 4: RIBAUDO-WATANABE-MGRDECHIAN RENDERS OBVIOUS CLAIM 23.....	79
IX.	CERTIFICATION UNDER RULE 42.104(A)	80
X.	MANDATORY NOTICES (37 C.F.R. § 42.8(A)(1)).....	80
A.	Real Party-in-Interest (37 C.F.R. § 42.8(b)(1)):	80
B.	Related Matters (37 C.F.R. § 42.8(b)(2)).....	81
C.	Lead and Back-up Counsel (37 C.F.R. § 42.8(b)(3)).....	82
D.	Service Information (37 C.F.R. § 42.8(b)(4))	83
XI.	CONCLUSION.....	83

PETITIONER'S EXHIBIT LIST

Exhibit No.	Description
1001	U.S. Patent No. 11,334,918 (“the ’918 patent”)
1002	Declaration of Dr. Sundeep Rangan
1003	Curriculum Vitae of Dr. Sundeep Rangan
1004	Prosecution History of U.S. Patent No. 11,334,918
1005	Japanese Patent Application Publication No. 2005/12973 to Watanabe
1006	Certified English-language translation of Japanese Patent Application Publication No. 2005/12973 to Watanabe (“Watanabe”)
1007	U.S. Patent Application Publication No. 2007/0030824 to Ribaudó (“Ribaudó”)
1008	International Patent Application Publication No. WO2008/132241 to Behrens (“Behrens”)
1009	International Patent Application Publication No. WO2008/076827 to Krikorian (“Krikorian”)
1010	U.S. Patent Application Publication No. 2005/00174975 to Mgrdechian (“Mgrdechian”)
1011	Declaration of James A. Proctor, Jr., filed April 20, 2020 in U.S. Patent Application No. 15/271,410
1012	U.S. Patent Application Publication No. 2002/0116494 to Kocol (“Kocol”)
1013-1020	<i>Intentionally Left Blank</i>
1021	Bluetooth Specification v.2.0 + EDR (Nov. 2004)
1022	Telecom Dictionary (2007) (“beacon channel,” “beaconing”)

Exhibit No.	Description
1023	Webster's New World Telecom Dictionary (2008) ("beaconing")
1024	"Radio beacon," Wikipedia, accessible at https://en.wikipedia.org/wiki/Radio_beacon
1025	IEEE 802.11 Specification IEEE Standard 802.11, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications (June 2007) ("Wi-Fi Specification")
1026	IEEE Standard 802.15.1, Part 15.1: Wireless medium access control and physical layer (PHY) specifications for wireless personal area networks (WPANs) ("Bluetooth Specification")
1027	U.S. Patent No. 7,000,001 to Lazaridis et al. ("Lazaridis")
1028	U.S. Patent Application Publication No. 2009/0239467 to Gulin et al. ("Gulin")
1029	U.S. Patent Application Publication No. 2004/0248569 to Kondou et al. ("Kondou")
1030	U.S. Patent Application Publication No. 2006/0287813 to Quigley et al. ("Quigley")
1031	U.S. Patent Application Publication No. 2005/0130634 to Godfrey ("Godfrey")
1032	Jansen et al., "Proximity Beacons and Mobile Device Authentication," <i>National Institute of Standards and Technology</i> (June 2005) ("Jansen")
1033	U.S. Patent Application Publication No. 2003/0220114 to Langensteiner et al. ("Langensteiner")
1034	U.S. Patent Application Publication No. 2008/0261526 to Suresh ("Suresh")
1035	U.S. Patent Application Publication No. 2009/0059878 to Tamura ("Tamura")

Exhibit No.	Description
1036	U.S. Patent No. 8,411,662 to Saund et al. (“Saund”)
1037	U.S. Patent Application Publication No. 2008/0045181 to Suzuki (“Suzuki”)
1038	International Patent Application Publication No. WO2006/028640 to Briancon et al. (“Briancon”)
1039	Sorte et al., “Service publishing to support an efficient network selection in an 802.11 multi-access environment,” January 2006 (“Sorte”)
1040	U.S. Patent No. 6,928,263 to Blake et al. (“Blake”)
1041	Yeong et al., “802.11a MAC Layer: Firmware/Hardware Co-Design,” Fourth International Conference on Information, Communications, and Signal Processing, December 2003 (“Yeong”)
1042	Huang, L. et al., “Enhancing Wireless Location Privacy Using Silent Period,” <i>IEEE Wireless Communications and Networking Conference</i> , Vol. 2, pp. 1187-1192, March 2005 (“Huang”)
1043-1045	<i>Intentionally Left Blank</i>
1046	U.S. Patent Application Publication No. 2002/0174364 to Nordman et al. (“Nordman”)

CLAIM LISTING

1[pre]	A mobile wireless device comprising:
1[a]	a first radio;
1[b]	a second radio;
1[c]	one or more processors;
1[d]	one or more memory devices coupled to the one or more processors, the one or more memory devices storing a set of instructions that when executed by the one or more processors cause the one or more processors to perform operations including:
1[e]	receiving, using the first radio, identifier related information associated with a proximity beacon service, from one or more servers;
1[f]	[1] receiving, using the second radio, a plurality of short range transmissions, including a plurality of proximity beacon transmissions when the device is located within a detection range of one or more beacon transmitter devices associated with the proximity beacon service, [2] each of the proximity beacon transmissions including a respective MAC address, a respective unique identifier, and a Proximity Beacon Service Identifier (PBSI);
1[g]	determining if a particular short range transmission of the plurality of short range transmissions a) includes a MAC address, and b) includes the proximity beacon service identifier (PBSI) and if c) the PBSI indicates the particular short range transmission is a proximity beacon transmission associated with the proximity beacon service; then:

1[h]	determining if an entity or object associated with the proximity beacon service is in proximity to the mobile wireless device by utilizing the identifier related information and the unique identifier.
2	The mobile wireless device of claim 1, wherein the MAC address is a randomly generated 48 bit number matching a format of a Bluetooth BD_ADDR.
3[pre]	The mobile device of claim 1 wherein the one or more processors further execute the instructions to perform operations including:
3[a]	receiving, by the second radio, a first proximity beacon transmission including a first MAC address and a first unique identifier at a first time; and
3[b]	receiving, by the second radio, a second proximity beacon transmission including a second MAC address and a second unique identifier at a second time, the second MAC address being different from the first MAC address and the second unique identifier being different from the first unique identifier; and
3[c]	associating the first and second unique identifier with a single beacon transmitter device.
4	The mobile wireless device of claim 1, wherein the one or more processors further execute the instructions to perform operations including: further determining that at least one beacon transmitter device associated with the proximity beacon service is in proximity to the mobile wireless device, by utilizing an action function including one or more previously downloaded unique identifiers.

5	The mobile wireless device of claim 1, wherein the one or more processors further execute the instructions to perform operations including determining, based upon at least a portion of the identifier related information, that at least one beacon transmitter is a broadcast device having a predetermined location.
6	The mobile wireless device of claim 1, wherein the identifier related information comprises application software for execution upon the mobile wireless device, and the one or more processors further execute the instructions to perform operations including: sending of the unique identifier by the mobile wireless device to at least one server of the one or more servers; and in response to the sending of the unique identifier, downloading the application software.
7[pre]	The mobile wireless device of claim 3, wherein
7[a]	the identifier related information comprises a list of contact information, and the one or more processors further execute the instructions to perform operations including:
7[b]	further determining that at least one beacon transmitter device associated with the proximity beacon service is further matched with an entity included within the list of contact information based upon comparing a contact identifier information with at least a portion of the unique identifier, and
7[c]	the mobile wireless device, upon determining there is a match, allowing further communications with the detected beacon transmitter device associated with the entity included within the list of contact information, wherein the further communications utilize the first radio.

8[pre]	The mobile wireless device of claim 1 wherein the one or more processors further execute the instructions to perform operations including:
8[a]	receiving, via a second radio, the plurality of proximity beacon transmissions further includes receiving a first unique identifier at a first time that is different from a second unique identifier received at a second time; and
8[b]	associating the first and second unique identifier with a single beacon transmitter device.
9[pre]	A method for facilitating use of proximity beacons, the method executing within a mobile device, and the method comprising:
9[a]	communicating between the mobile device and one or more servers and receiving, at the mobile device, identifier related information, using a first radio;
9[b]	receiving, at the mobile device using a second radio, a plurality of short range transmissions, including a plurality of proximity beacon transmissions from one or more beacon transmitter devices associated with a proximity beacon service, each of the proximity beacon transmissions including a respective MAC address, a respective unique identifier (UID), and a Proximity Beacon Service Identifier (PBSI);
9[c]	a) determining that a particular short range transmission of the plurality of short range transmissions includes a MAC address, b) determining that the Proximity Beacon Service Identifier (PBSI) is present, and

	c) determining that the PBSI indicates the particular short range transmission is a proximity beacon transmission associated with the proximity beacon service; and
9[d]	when the three determining steps a) b) and c) are each true, then d) determining that an entity or object associated with the proximity beacon service is within proximity to the mobile device, by utilizing the identifier related information and the unique identifier.
10[pre]	The method of claim 9,
10[a]	wherein a first one of the plurality of proximity beacon transmissions received at a first time includes a first unique identifier, and
10[b]	wherein a second one of the plurality of proximity beacon transmissions received at a second time includes a second unique identifier the second unique identifier being different from the first unique identifier; and
10[c]	associating both the first unique identifier and the second unique identifier with a particular entity or object in proximity to the mobile device.
11	The mobile wireless device of claim 9 wherein the MAC address is selected from a group consisting of (a) a randomly generated 48 bit number matching a format of a MAC address and (b) a Bluetooth BD_ADDR.
12[pre]	The method of claim 9

12[a]	wherein a first one of the plurality of proximity beacon transmissions is received at a first time and includes a first unique identifier and first MAC address, and the Proximity Beacon Service (PBSI); and
12[b]	where a second one of the plurality of proximity beacon transmissions received at a second time includes a second unique identifier different from the first unique identifier and a second MAC address different from the first MAC address, and the Proximity Beacon Service Identifier; and
12[c]	associating both the first unique identifier and the second unique identifier with the same entity or object in proximity to the mobile device.
13	The method of claim 9, further comprising preventing the sending of the unique identifier, using the first radio, to the one or more servers, based upon previous detections of the respective unique identifier associated with the proximity beacon transmission.
14	The mobile wireless device of claim 1, wherein the instructions further comprise: sending the unique identifier, using the first radio, to at least one server of the one or more servers, and receiving further information relating to an object or entity associated with being within proximity to the mobile device.
15	The mobile wireless device of claim 1, wherein the instructions further comprise:

	preventing the sending of the unique identifier, using the first radio, to the one or more servers, based upon previous detections of the respective unique identifier associated with the proximity beacon transmission.
16	The mobile wireless device of claim 1, wherein the instructions further comprise: controlling further communications between the mobile device and at least one device or server associated with an entity or object in proximity to the mobile device.
17	The method of claim 9, further comprising: receiving, using the first radio, access code information by the mobile device from at least one of the servers; and utilizing the access code information to gain access to the entity or object determined to be in proximity to the mobile device.
18	The method of claim 9, wherein receiving the identifier related information, using the first radio, is performed in response to sending at least the unique identifier to at least one of the one or more servers using the first radio.
19	The method of claim 9, additionally comprising: sending the unique identifier, using the first radio, to at least one server of the one or more servers, and receiving further information relating to an object or entity associated with being within proximity to the mobile device.

20	The method of claim 19, wherein the further information relates to one or more of the following: a loyalty program; a payment service; or a coupon relating to an entity in proximity to the mobile device; or advertising content.
21	The method of claim 19, wherein the further information relates to a service for providing a menu for use by a user of the mobile device for use in purchasing items, and further comprising: allowing for the user take delivery at or near the location of a fixed proximity beacon device.
22	The method of claim 19, wherein the further information relates to a nearby user of an application on another device, in common with an application on the mobile device.
23	The method of claim 22, wherein the application is a multiuser game.
24	The method of claim 9, additionally comprising: controlling further communications between the mobile device and at least one device or server associated with an entity or object in proximity to the mobile device.
25	The method of claim 9, wherein the step of determining that an entity or object is within proximity further comprises: comparing the identifier related information with the unique identifier or information derived from the unique identifier.
26[pre]	The method of claim 9, additionally comprising:

26[a]	sending the unique identifier, using the first radio, to at least one server of the one or more servers, and wherein the one or more servers perform the following steps:
26[b]	associating an object or entity as being within proximity to the mobile device;
26[c]	storing a user's purchasing practices or requests from the one or more servers, related to the associated object or entity information as stored proximity user behavior;
26[d]	retrieving a stored user email address associated with an account associated with the mobile device; and
26[e]	sending an email, addressed to the user email address containing customized content based upon the stored proximity user behavior.
27	The mobile wireless device of claim 1, wherein the one or more processors further execute the instructions to perform the operations for determining that an entity or object is within proximity by further: comparing the identifier related information with the unique identifier or information derived from the unique identifier.
28	The mobile wireless device of claim 1, wherein the receiving of the identifier related information, using the first radio, is performed in response to the one or more processors executing instructions for: sending at least the unique identifier to at least one of the one or more servers using the first radio.
29	The method of claim 9, wherein the proximity beacon transmissions are received, at the mobile device, without requiring the mobile device

	to first perform a step of transmitting to the one or more beacon transmitter devices from which the plurality of proximity beacon transmissions are received.
30[pre]	The mobile wireless device of claim 1 wherein:
30[a]	the identifier related information comprises a list of contact information, and the one or more processors further execute the instructions to perform operations including:
30[b]	further determining that at least one beacon transmitter device associated with the proximity beacon service is further matched with an entity included within the list of contact information based upon comparing a contact identifier information with at least a portion of the unique identifier, and;
30[c]	the mobile wireless device, upon determining there is a match, allowing further communications with the detected beacon transmitter device associated with the entity included within the list of contact information, wherein the further communications utilize the first radio.
31[pre]	The mobile wireless device of claim 3 wherein the one or more processors further execute the instructions to perform operations including:
31[a]	receiving, via a second radio, the plurality of proximity beacon transmissions further includes receiving a first unique identifier at a first time that is different from a second unique identifier received at a second time; and

31[b]	associating the first and second unique identifier with a single beacon transmitter device.
-------	---

I. INTRODUCTION

Apple Inc. petitions for *inter partes* review of claims 1-31 of U.S. Patent No. 11,334,918 (“the ’918 patent”).

The ’918 patent claims a mobile device that detects “beacon transmissions” that include three parameters: a MAC address, a unique identifier, and a proximity beacon service identifier (“PBSI”). When the mobile device detects such a beacon transmission, the mobile device determines that the transmitting device employs a particular beacon service that facilitates short-range communications between devices (e.g., via Bluetooth or Wi-Fi) and long-range communications between the mobile device and a server (e.g., via a cellular network). This may include a mobile device detecting a beacon transmission from a museum exhibit (short-range) and subsequently retrieving content related to that exhibit from a server (long-range).

But before the ’918 patent, using an identifier to signal short- and long-range communication capabilities was already well known. For example, both Ribaud and Watanabe separately disclose the claimed “proximity beacon service identifier” (“PBSI”). The combination also discloses the claimed MAC address and unique identifier and determining whether beacon transmissions include these three parameters. In view of Ribaud’s and Watanabe’s teachings, the independent claims are unpatentable. The dependent claims are similarly unpatentable in view

of Ribaud and Watanabe and in further view of Behrens, Nordman, and Mgrdechian. Thus, Petitioner respectfully requests that the Board institute trial and determine that claims 1-31 of the '918 patent are unpatentable.

II. THE '918 PATENT

A. Summary

The '918 patent describes mobile wireless devices (e.g., cellular phones) exchanging information “utilizing both a short range and a long range wireless capability.” EX1001, 2:66-3:3; EX1002, ¶¶64-70. The '918 patent concedes that conventional cellular phones “support at least two wireless standards”—namely, conventional cell phones already had access to both “wide area” cellular connection between the device and a central server, and short-range “Bluetooth” “peer to peer” capability. EX1001, 2:25-48. The '918 patent proposes using both wireless capabilities and identifiers for proximity detection, while also using a server to broker the exchange of information between two wireless devices. EX1001, 2:58-3:14.

As shown in Figure 1 below,¹ “a central server 100 [(red)] is connected to devices 106 and 108” (blue) through “wide area wireless links 104 and 103

¹ Throughout, emphasis and annotations are added unless otherwise specified.

respectively” (green), via a combination of the Internet and a cellular network.

EX1001, 5:62-6:6, FIG. 1. The devices are able to communicate directly with each other via “a short range wireless link 107” (yellow). EX1001, 6:55-66.

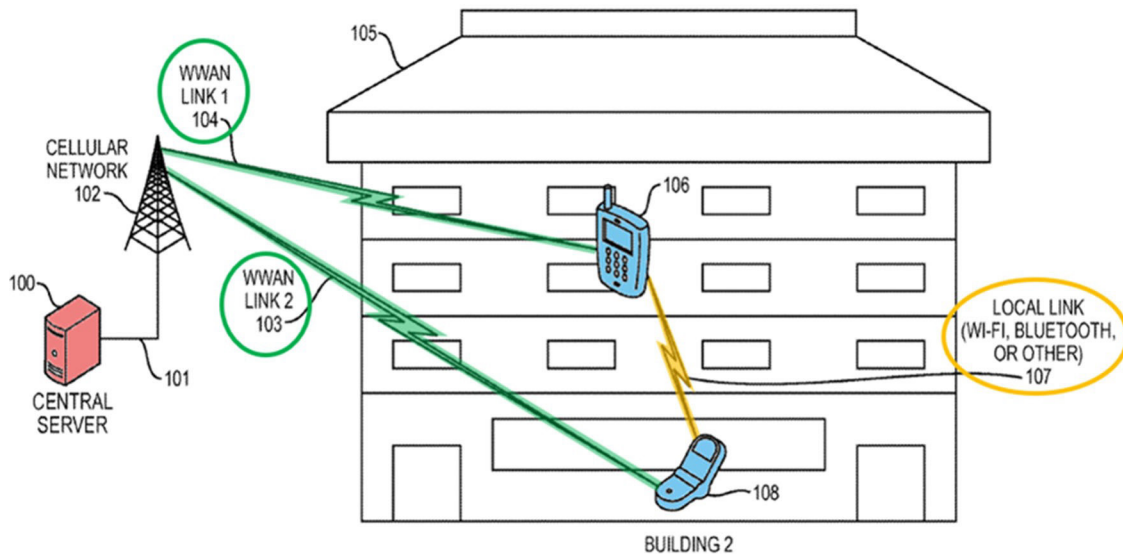


Figure 1

EX1001, FIG. 1 (annotated).

One example of the short-range wireless capability, shown in Figure 6, is an “independent basic service set or IBSS,” involving an “ad-hoc network” of wireless devices that “transmit identifiers called *beacons*.” EX1001, 10:31-44. Beacon transmissions include a MAC address (i.e., a hardware address/identifier) and a basic service set identifier (BSSID) or ad-hoc network name (SSID), where “one or both of the BSSID and the SSID” may identify a service. EX1001, 10:44-57, FIG. 6; EX1002, ¶66. While Figure 6 provides an example of multiple identifiers, the ’918 patent does not explicitly define the claim terms *PBSI* or *unique identifier*.

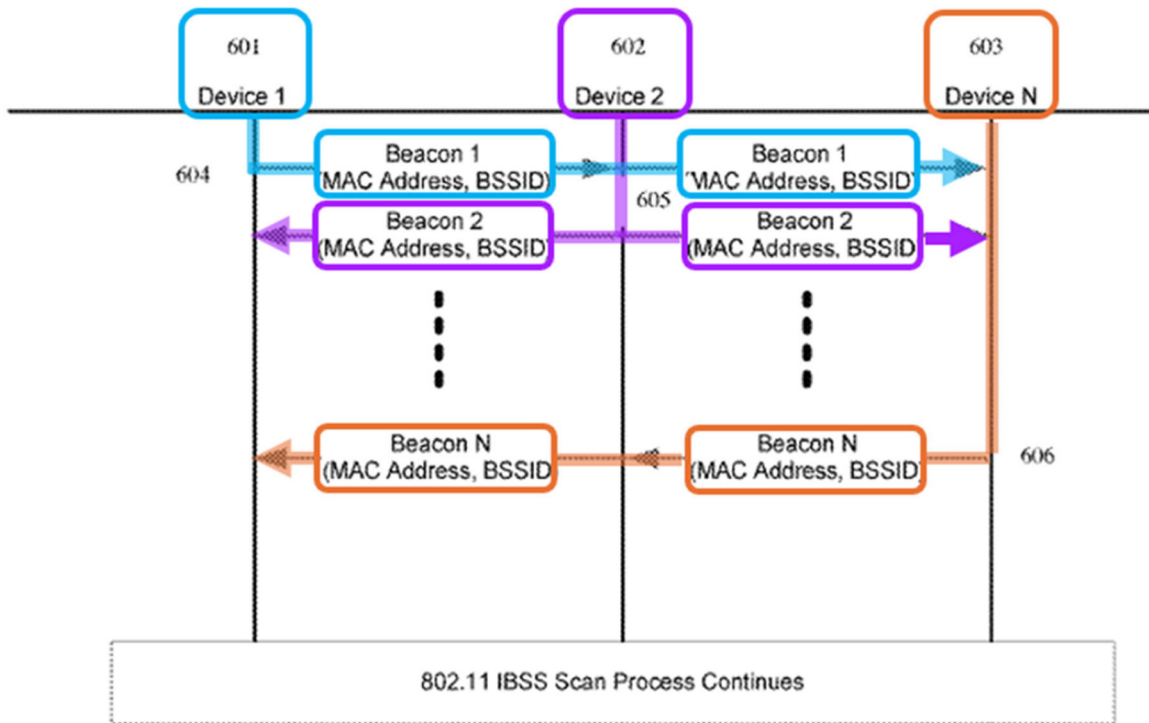


Figure 6 - 802.11 IBSS Beacon Process

EX1001, FIG. 6 (annotated).

B. Prosecution History

The '918 patent was filed on September 21, 2016, as a continuation of a series of patents, the earliest of which was filed on February 3, 2009. It also claims priority to provisional application Nos. 61/095,359 and 61/095,001, filed on September 8, 2008, and September 9, 2008, respectively.

To overcome written description rejections, the inventor submitted a declaration asserting that the claimed requirement that “beacon transmissions” comprise a “PBSI,” “MAC address,” and “unique identifier” is supported by the

specification’s discussion of the “IBSS beacon process” (EX1001, 10:31-11:6, FIG. 6)—where, in one embodiment, “‘PBSI’ is the BSSID field of the beacon,” and in another embodiment, “‘PBSI’ is the SSID.” EX1004, 1533-1534 (Proctor Decl., ¶¶120-124), 1565-1566; EX1011.

C. Person of Ordinary Skill in Art (POSITA)

A POSITA at the relevant time would have had a bachelor’s degree in electrical engineering, computer science, computer engineering, or a related field, and two to three years of experience in the research, design, development, or testing of wireless data communication systems, with additional education substituting for experience and vice versa. EX1002, ¶¶25-27.

III. CLAIM CONSTRUCTION

Claims are construed according to *Phillips*. 37 C.F.R. §42.100(b). Apple does not believe that any term requires express construction at this time. CTPG, 44; EX1002, ¶71.

IV. GROUNDS

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

Ground	Claims	References
1	1, 4-6, 9, 14, 16-22, 24-30	Ribaud-Watanabe
2	3, 7-8, 10, 12-13, 15, 31	Ribaud-Watanabe-Behrens

3	2, 11	Ribaudo-Watanabe-Behrens-Nordman
4	23	Ribaudo-Watanabe-Mgrdechian

Each reference is prior art:

- U.S. Patent Publication No. 2007/0030824 (“Ribaudo”) was published on February 8, 2007, and is prior art under §102(b).
- JP Patent Publication No. 2005/12973 (“Watanabe”) was published January 13, 2005, and is prior art under 35 U.S.C. §102(b). Watanabe citations herein are to the certified English translation of EX1005, attached as EX1006.
- PCT Patent Publication No. WO2008/132241 (“Behrens”) was filed in English as International Application PCT/EP2008/055394 on April 30, 2008, and designated the United States. Behrens published in English on November 6, 2008, and is prior art under §102(e). *See* MPEP § 2136 (Example 4).
- U.S. Patent Publication No. 2002/0174364 (“Nordman”) was published on November 21, 2002, and is prior art under §102(b).
- U.S. Patent Publication No. 2005/0174975 (“Mgrdechian”) was published on August 11, 2005, and is prior art under §102(b).

Each reference is analogous art: it is in the same field (e.g., facilitating the

exchange of information between devices via short- and long-range wireless communications) as the '918 patent, is reasonably pertinent to the problems (e.g., detecting wireless devices in close proximity to exchange information) of the '918 patent, or both. EX1002, ¶¶28, 72.

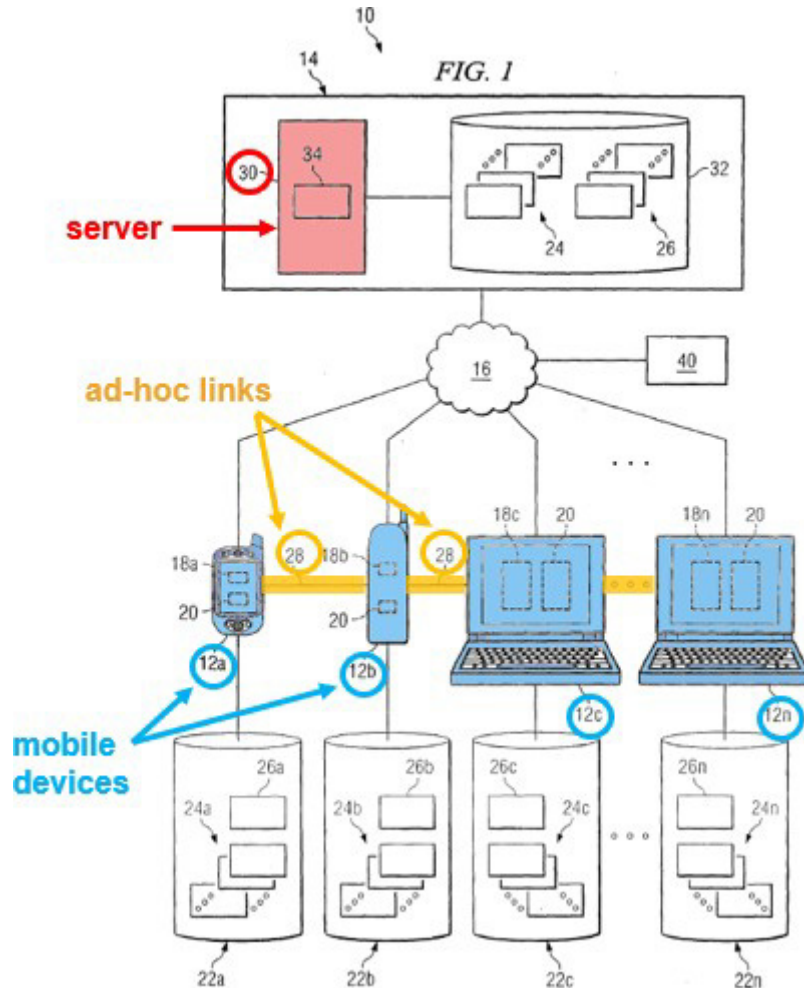
V. GROUND 1: RIBAUDO-WATANABE RENDERS OBVIOUS CLAIMS 1, 4-6, 9, 14, 16-22, AND 24-30

A. Ribaudó

Ribaudó discloses mobile devices that (i) detect other mobile devices in proximity using identifiers beacons using a short-range wireless protocol and (ii) communicate with a server via a long-range wireless protocol. EX1007, Abstract, ¶¶24-25, 57, 66-67, 79, FIG. 1; EX1002, ¶¶73-76. Ribaudó teaches “providing communication services to mobile device users incorporating proximity determination” to facilitate activities, such as social networking. EX1007, ¶¶2, 8, 29. For example, “when the user is in proximity to another user, the user’s mobile device detects the presence of the other user’s mobile device, receives an identifier associated with the detected other user, and compares the received identifier with the pre-processed match data stored on the user’s mobile device to determine whether the other user is one of the user’s predetermined matches.” EX1007, ¶¶6, 223 (“the present invention may connect users based on any desire, relation, affiliation, or other reason.”).

Ribaudó’s system, illustrated in Figure 1, “includes one or more mobile

devices 12” (blue) with “links 28” (yellow) indicating “ad-hoc connections between [the] devices,” “a data center 14” that “includes a server system 30” (red), “and a network 16” that connects the mobile devices to the server. EX1007, ¶¶15, 34, 66, FIG. 1.



EX1007, FIG. 1 (annotated).

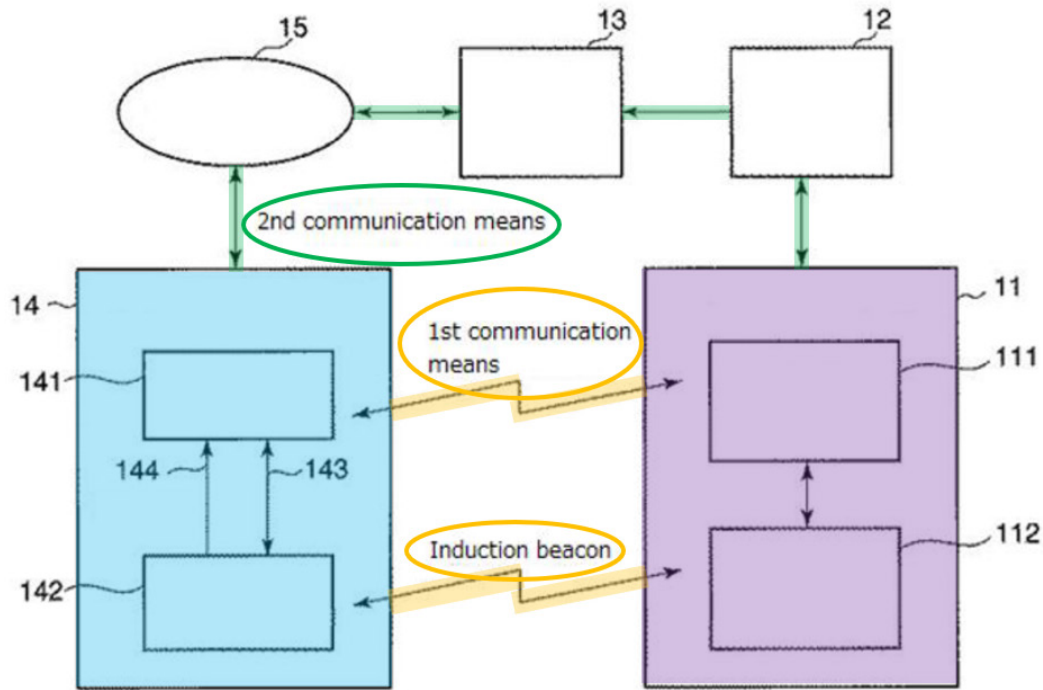
As Ribaudo explains, “a user (e.g., of mobile device 12a) may be associated with one or more client IDs, which may identify the user publicly,” which “may be the unique MAC address[es] of the Wi-Fi NIC of the user’s mobile device[s] 12.”

EX1007, ¶68. The mobile device “may beacon data such as the client ID of the user associated with [the] mobile device” (EX1007, ¶57) and “an SSID” of a proprietor of system 10. EX1007, ¶123. Moreover, “[t]he unique MAC address of mobile device 12a may be beacons when the BLUETOOTH interface of mobile device 12a is active.” EX1007, ¶157.

B. Watanabe

Watanabe discloses using a short-range wireless protocol to detect beacons identifiers from other devices in proximity and a long-range wireless protocol to communicate with a server. EX1006, ¶¶12, 26-27, FIG. 1; EX1002, ¶¶77-81. Watanabe teaches a system that “reduce[s] power consumption when a mobile terminal is not communicating data with an access point.” EX1006, ¶7, Abstract. As shown in Figure 1, “client terminal 14” (blue) “communicates with an electronic information device (for example, a server) connected to the network via the access points 11” (purple). EX1006, ¶¶12, 53, FIG. 1. “Each access point 11 has an AP main unit ... 111 as a first communication means” (yellow) “for [short or medium-distance] wireless communication (data communication) with client terminals 14” (i.e., mobile device). EX1006, ¶¶14, 27. Client terminal 14 also has a “second communication means” (green) “for communicating ... via the internet 15.” EX1006, ¶26.

[FIG. 1]

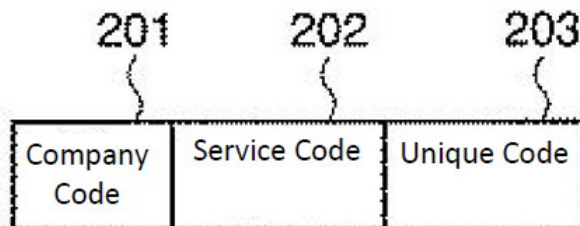


EX1006, FIG. 1 (annotated).

“[E]ach access point 11 ... generates an induction *beacon* ... via the first communication means” and reports “transmitter identification information.”

EX1006, ¶¶14, 49. Transmitter identification information includes: a “company code 201 indicating the service provider,” a “service code 202 indicating the type of service that can be provided via the access point 11,” and “a unique code 203 specific to the electrical power induction transmitter 112.” EX1006, ¶15, FIG. 2.

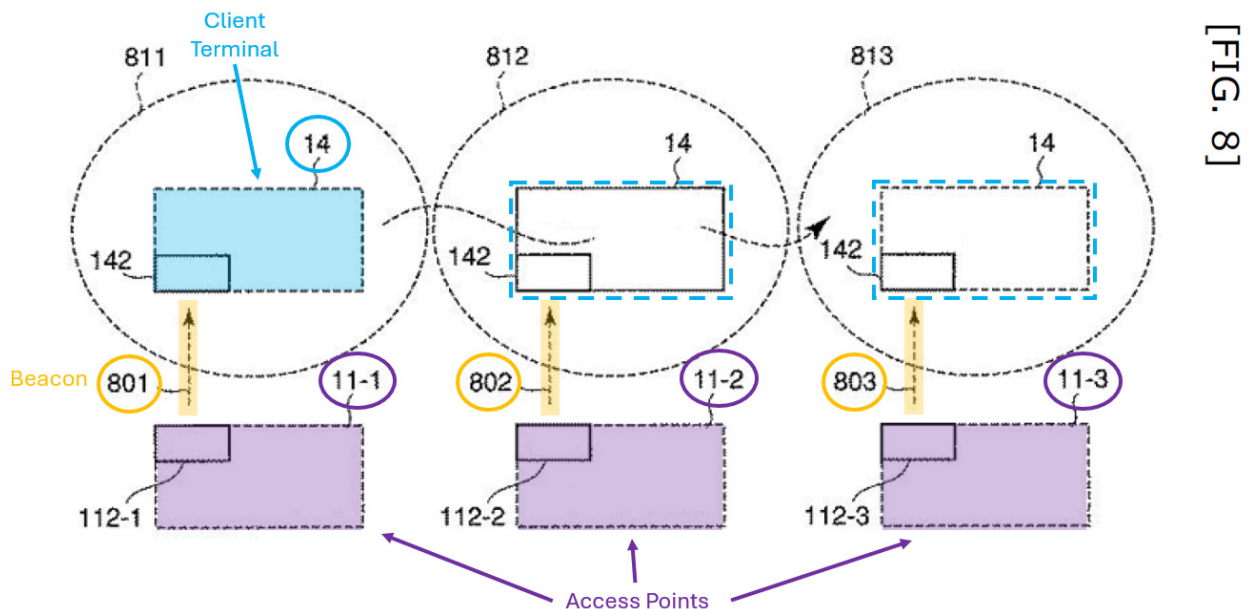
[FIG. 2]



EX1006, FIG. 2.

When “client terminal 14 receives a beacon, it extracts the transmitter identification information in the beacon and compares this information with the pre-set filtering identification information,” and, “[i]f the comparison results match, the client main unit 141 is activated.” EX1006, ¶47.

Watanabe’s wireless system is illustrated in Figure 8, where a trio of access points (purple) “transmit induction beacons 801, 802, and 803” (yellow) “to supply power to client terminal[] 14” (blue) “within [the] range” of the access point. EX1006, ¶49, FIG. 8.



EX1006, FIG. 8 (annotated).

C. Motivation to Combine

A POSITA would have been motivated to combine the teachings of Ribaudó and Watanabe to enhance Ribaudó’s beacon transmission processing and filtering

capabilities. EX1002, ¶¶90-93. A POSITA would have also had a reasonable expectation of success in combining Ribaudó and Watanabe because each relates to detecting nearby wireless devices via beacon transmissions and establishing communications using both ad-hoc (e.g., WiFi or Bluetooth) and cellular networks. EX1006, Abstract, ¶27; EX1007, Abstract, ¶18; EX1002, ¶¶94-97.

As further discussed for Element 1[g], Ribaudó describes a beacon service identifier in the form of an SSID. In Ribaudó, a mobile device “may beacon an ***SSID of ‘proprietor_name.net’*** (e.g., where ‘proprietor_name’ corresponds to the name of a proprietor of system 10).” EX1007, ¶123. The “proprietor_name.net” may be associated with a particular service—for example, where the proprietor is a user matching or online dating platform, the SSID may identify a service provided by such a proprietor (e.g., providing dating matches). EX1007, ¶¶97-104, 138 (discussing “dating” related services). Ribaudó further describes filtering mechanisms, filtering based on “SSIDs,” and only notifying a user if a matching SSID is detected. EX1007, ¶61; *see also* ¶¶29, 55, 97-104, 123, 162, 223, 226. “Once a desirable SSID is detected... the two mobile devices 12a and 12b may establish a connection on the same network.” EX1007, ¶71. Ribaudó therefore describes filtering beacon transmissions based on a particular beacon service identifier or PBSI.

Thus, Ribaudó teaches using an identifier for a particular service and

filtering based on such an identifier. To enhance these capabilities and more efficiently process and filter beacon transmissions, a POSITA would have been motivated to implement Watanabe's beacon transmission structure, "service code," and service code "filtering" techniques. EX1002, ¶92. For example, Watanabe describes a beacon transmission that includes multiple identifiers, including a "company code," "unique code," and "service code." EX1006, FIG. 2, ¶¶14-15, 33, 49, 63. Watanabe describes filtering such beacon transmissions using the service code when determining whether a user has entered into a contract to receive corresponding services. EX1006, ¶¶41, 48-49, 51-52, 57, FIG. 8. Watanabe therefore teaches processing and filtering beacon transmissions based on "service codes" corresponding to a particular service. EX1006, ¶¶41, 48-49.

In Ribaud-Watanabe, Watanabe's "service code" would be beacons together with a MAC address, client ID, and/or SSID in Ribaud's system to enhance Ribaud's processing of beacon transmissions and filtering capabilities. EX1002, ¶93; EX1007, ¶76 (Ribaud "contemplates use of any other suitable identifiers ... according to particular needs"). For example, a POSITA would have found it beneficial to include a service code corresponding to the type of match data beacons over Bluetooth between Ribaud's mobile devices. EX1007, ¶90 (describing "nine categories" of matching including "dating" and "employment"). Including such a service code would allow the device receiving the Bluetooth beacon to distinguish between different types of matching services

or match data, and in turn, identify the desired service type. For example, the service code, as applied to Ribaudó, would identify beacon transmissions corresponding to a “dating” service, allowing receiving mobile devices to more efficiently filter beacon transmissions based on desired services as described in Watanabe and Ribaudó. EX1002, ¶93. Thus, a POSITA would have been motivated to combine Ribaudó and Watanabe to enhance Ribaudó’s processing of beacon transmissions.

A POSITA would have had a reasonable expectation of success in combining the teachings of Watanabe and Ribaudó. EX1002, ¶¶94-96. Both describe mobile devices that receive beacon transmissions comprising identification information associated with a transmitting device, receive information relating to an entity associated with the identification information from a server using the Internet, compare the beacons identification information to preset identification information stored at the mobile device to identify it matches, and take further action relating to the stored information if it matches. EX1006, ¶¶46-55; EX1007, ¶¶6-7. Further, Ribaudó explains “although MAC addresses and SSIDs are primarily described, [the] invention contemplates use of any other suitable identifiers ... according to particular needs.” EX1007, ¶76. Watanabe also explains that its “field configuration for this transmitter identification information is commonly used when using internet services.” EX1006, ¶¶15-16. A POSITA would thus have understood that these references disclose interrelated teachings

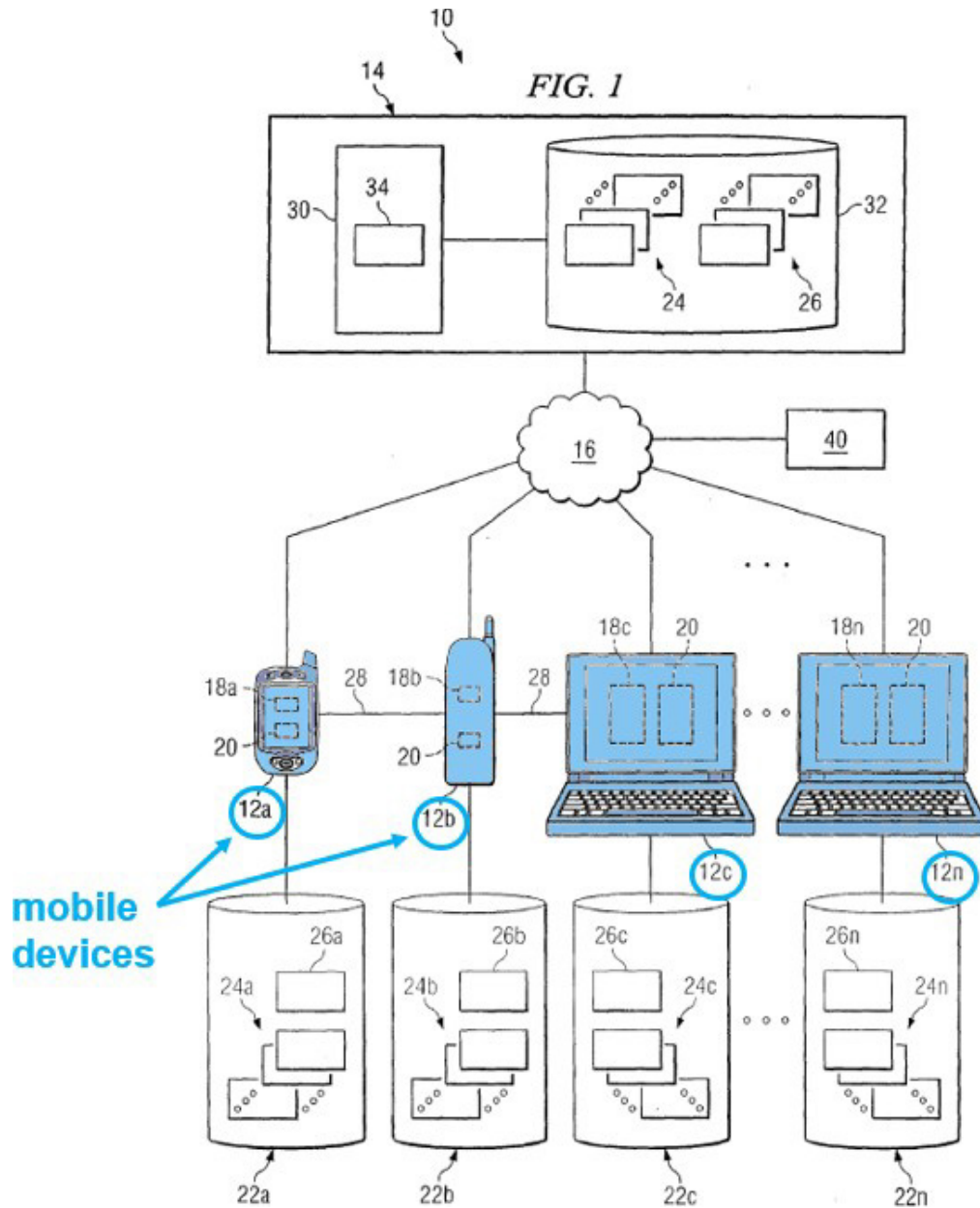
based on well-understood technologies that would have been amenable to various well-understood and predictable combinations. EX1002, ¶¶95-97. Implementing Watanabe's service code and filtering techniques based on the service code would have amounted to combining prior art elements according to known methods to yield predictable results. *Id.* Ribauda teaches the system and functionality for sending and receiving beacon transmissions that include identifiers, and Watanabe describes a specific identifier that would have been obvious and within the skill of a POSITA to include in Ribauda's beacon transmissions. *Id.*

D. Independent Claim 1

1. 1[pre]

Ribauda teaches² the preamble. EX1002, ¶¶98-99. Figure 1 of Ribauda includes “[m]obile devices 12” (blue), where each device (*e.g.*, 12a) “may include one or more suitable devices for wireless communication.” EX1007, ¶18; *see also* EX1007, ¶15, FIG. 1.

² The term “teaches” includes both express teachings and those fairly suggested to a person of ordinary skill in the art. *In re Baird*, 16 F.3d 380, 383 (Fed. Cir. 1994); *In re Keller*, 642 F.2d 413, 425 (CCPA 1981).



EX1007, FIG. 1 (annotated).

2. 1[a]

Ribaudo teaches 1[a]. Ribaudo's "[m]obile devices 12 may each include any suitable combination of hardware, software, and firmware to provide the functionality described herein," and "[e]ach mobile device 12 may include one or

more suitable devices for wireless communication,” including an “adaptor 18” that “may facilitate communication ... between mobile device 12 and data center 14.” EX1007, ¶¶18-19, 21-22 (discussing NIC), FIG. 1. Further, “mobile devices 12 may each be coupled to data center 14 via network 16”—including “*wide area networks (WANs)*, [or] all or a portion of a global computer network such as the Internet”—and through a “*wireless link.*” EX1007, ¶¶24-25. Ribaudó’s system may “employ[] a *cellular* connection ... to download from data center 14.” EX1007, ¶204. Mobile device 12a satisfies the recited wireless mobile device, and adaptor 18a’s cellular/WAN radio satisfies the recited first radio. EX1002, ¶¶100-101; EX1011 (Proctor Decl.), ¶¶73-89 (explaining how the ’918 specification discloses “first” and “second radio[s]”).

3. 1[b]

Ribaudó teaches 1[b]. “Each mobile device 12 may include one or more suitable devices for wireless communication, such as one or more wireless fidelity (*Wi-Fi*) devices [or] one or more *BLUETOOTH* devices,” for example an “adaptor 18” that “may facilitate communication with other mobile devices 12 (e.g., mobile devices 12b through 12n).” EX1007, ¶¶18-19, 21-22, 73, 205, FIG. 1.

Adaptor 18a’s Wi-Fi (or Bluetooth) radio satisfies the “second radio.” EX1002, ¶¶102-104; EX1011 (Proctor Decl.), ¶¶73-89.

4. 1[c]

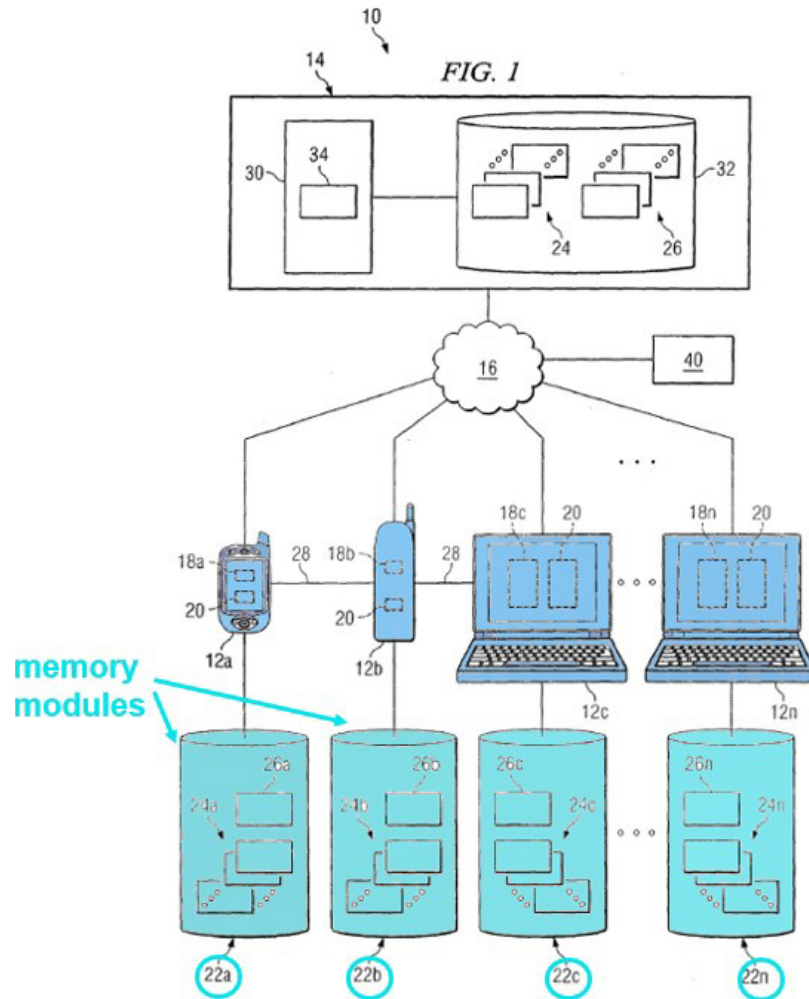
Ribaudo teaches 1[c]. Ribaudo's mobile devices 12 "each include any suitable *combination of hardware, software, and firmware* to provide the functionality described" including "one or more applications 20" to "facilitate communication with other mobile devices 12 (*e.g.*, devices 12b through 12n) and between mobile device 12 and data center 14." EX1007, ¶19. "[T]he user of mobile device 12a launches [an] application 20," so that "mobile device 12a may be operable to detect other mobile devices 12" based on match data, and "may beacon data such as the client ID of the user ... within any suitable range." EX1007, ¶84, FIG. 2.

Accordingly, a POSITA would have recognized or found obvious that the mobile device 12a includes at least one processor (*e.g.*, a microprocessor or microcontroller, programmed with software or firmware) to provide the described functionality of application 20. EX1002, ¶¶105-107; EX1008, 20:31-21:15 (confirming it was well known in the art for mobile devices to include "at least one microprocessor for managing the wireless radio transmissions as well as for processing and storing data").

5. 1[d]

Ribaudo teaches 1[d]. Ribaudo's "[m]obile devices 12 may each have an associated memory module 22"—or "any suitable number of memory modules 22

according to particular needs”—that may be “operable to store data as one or more compressed binary files.” EX1007, ¶32, FIG. 1; *see also* EX1007, ¶¶18-19 (“[m]obile devices 12 may each include any suitable combination of hardware, software, and firmware to provide the functionality described herein.”).



EX1007, FIG. 1 (annotated).

Specifically, “[m]emory module 22 may store various data associated with the user of mobile device 12,” including “one or more user profiles 24 for the user of mobile device 12[,] ... match data 26 downloaded from data center 14 and

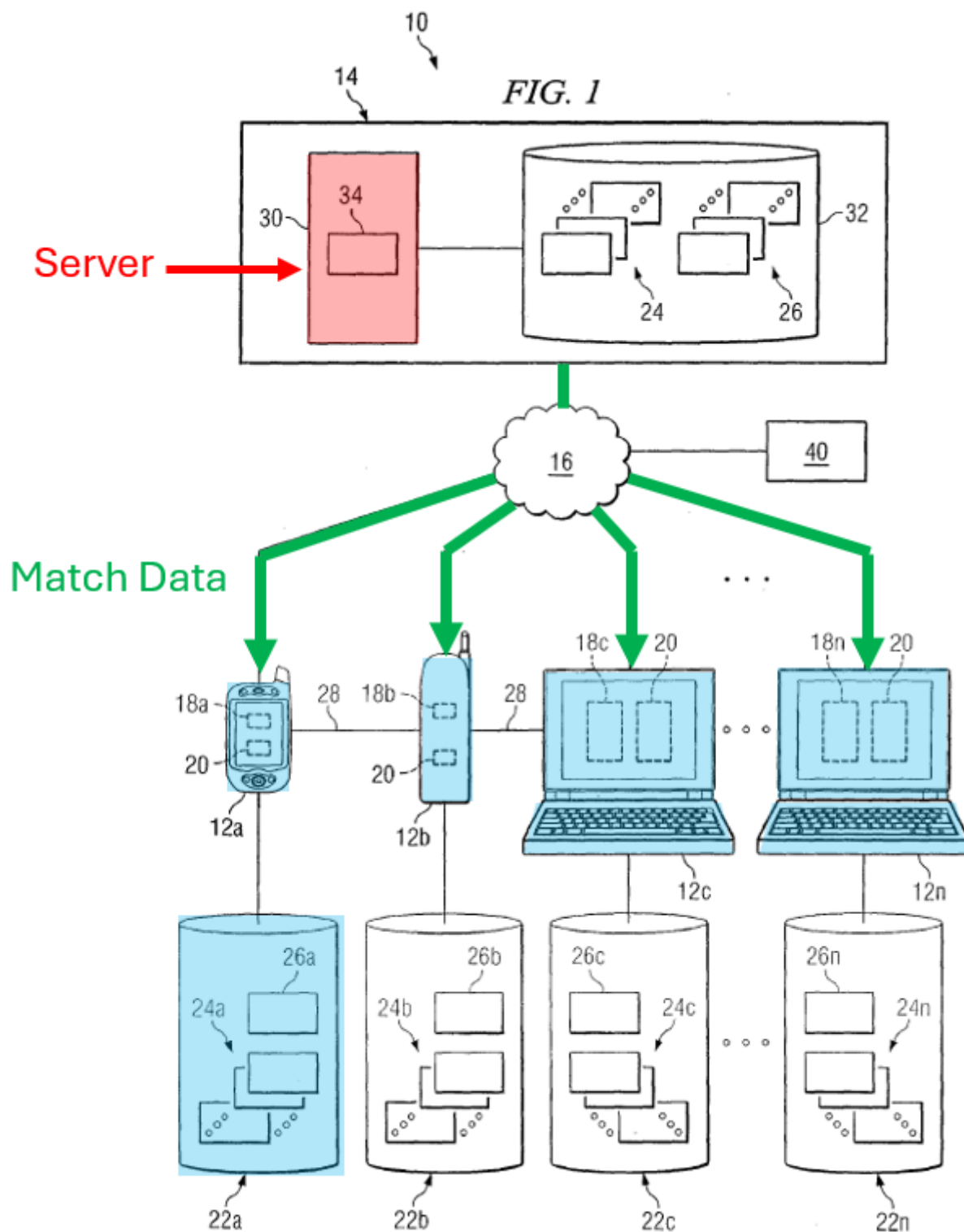
identifying one or more predetermined matches for the user[, and] ... any other suitable information, according to particular needs.” EX1007, ¶¶33, ¶¶84 (describing the operations performed by mobile device 12 in the Figure 2 communication services method, including detecting devices and beaconing data).

Memory module 22 also stores software instructions for performing the functions described below. EX1007, Claim 31 (directed to “[s]oftware for proximity determination, the software being embodied in a computer-readable medium and when executed, operable to” perform the claimed functions).

Accordingly, a POSITA would have recognized or found obvious that the mobile device 12a includes a memory module 22 that is coupled to one or more processors, and that stores a set of software instructions that when executed by the processors, cause the processors to perform the communication services operations described further below. EX1002, ¶¶108-112.

6. 1[e]

Ribaudo teaches 1[e]. Ribaudo’s “[d]ata center 14 includes a server system 30” (red) as shown in Figure 1. EX1007, ¶¶34, FIG. 1.



EX1007, FIG. 1 (annotated).

Ribaudo's data center "*transmit[s] to each user match data containing match identifiers and other information* for the other users determined to be matches for the user. This *pre-processed match data* for the user is stored locally on the user's mobile device 12." EX1007, ¶16; *see* EX1007, ¶¶31, 33 ("memory module 22 may store match data 26 downloaded from data center 14 and identifying one or more predetermined matches for the user"), 45-52 (describing match data and an example match ID including a "client ID"), 53-54. Ribaudo teaches the user's mobile device receives the transmitted match data via the first radio (via WAN or cellular). EX1007, ¶¶24, 53-54.

Ribaudo's match data is "*identifier related information*." Ribaudo explains, "using match data 26 (e.g., the match IDs) downloaded from data center 14, mobile devices 12 are operable to *detect in proximity other mobile devices 12 that may be associated* with a user who is a potential match" based on matching beacons client IDs. EX1007, ¶57; *see* EX1007, ¶¶123, 157, 173.³

Finally, this pre-processed match data is "associated with" a proximity beacon service because the mobile device uses the match data "to detect *in proximity* other

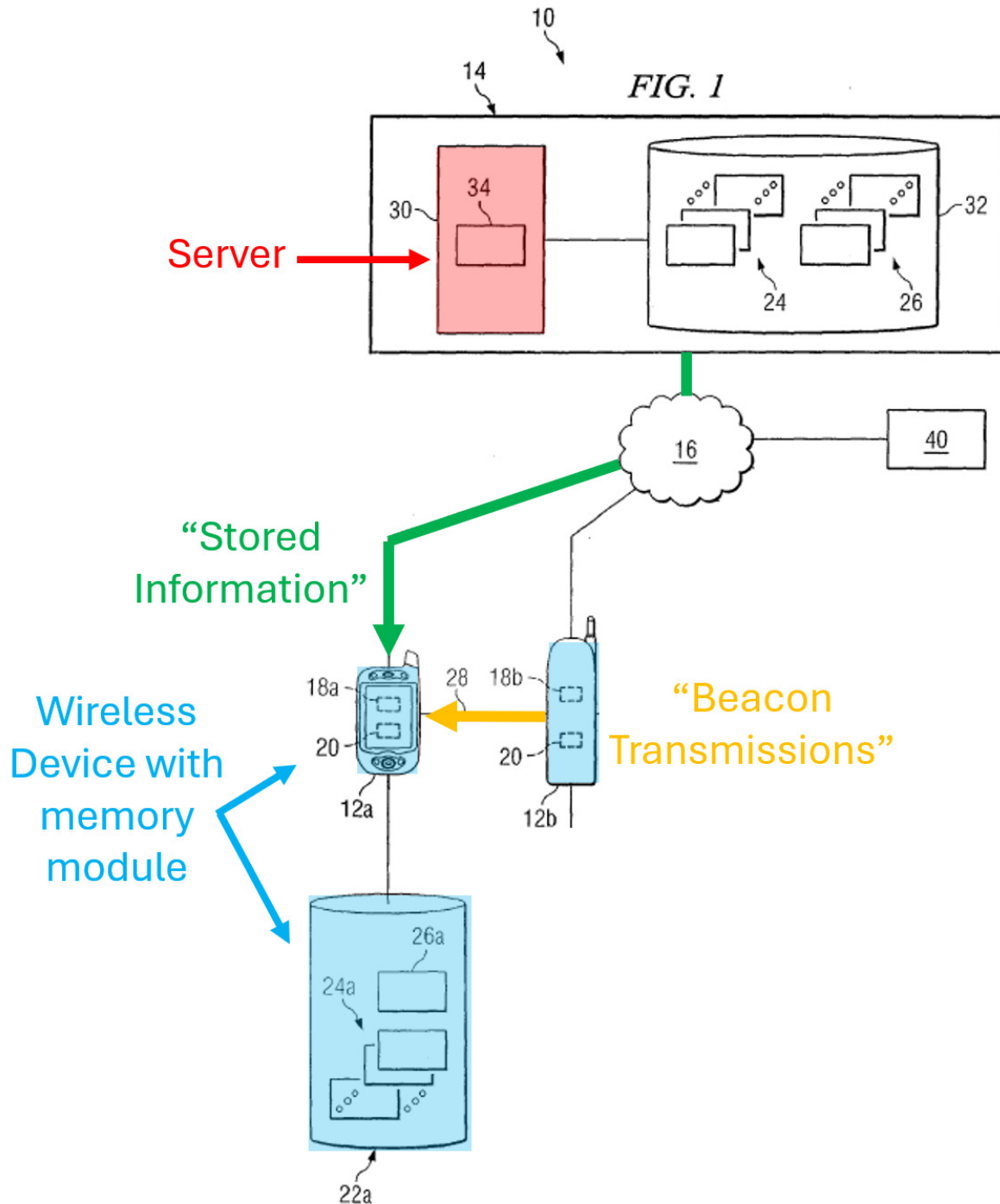
³ Ribaudo also discloses performing proximity detection before using the first radio (e.g., cellular) to download match data from the server. EX1007, ¶¶204-205.

mobile devices 12 that may be associated with a user who is a potential match” by “*beacon[ing] data* ... within any suitable range,” EX1007, ¶57, and because the match data relates to “commonalities or other reasons for interacting” between two users of a given internet service (e.g., matching service or online dating). EX1007, ¶¶29, 97-105; EX1002, ¶¶113-117. *See also* EX1007, ¶¶158-171 (describing various services, including “Closed Group Matching,” “Implied Proximity” matching, “External Web Service,” and “Use of Match Data in Cooperation with Third Parties”), 221-223.

7. 1[f][1]

Ribaudo-Watanabe teaches 1[f][1]. Ribaudo’s mobile devices receive proximity beacon transmissions from other mobile devices that are located within a detection range. Ribaudo explains that “mobile devices 12 are operable to *detect in proximity other mobile devices 12 that may be associated* with a user who is a potential match. ... Mobile device 12 may *beacon data* such as the client ID of the user associated with mobile device 12 (and possibly the user’s availability level and other identification information, such as trust score and status).” EX1007, ¶57. As depicted below, mobile device 12b may be an “other mobile device[]” in the detection range. The Wi-Fi or Bluetooth radio (i.e., second radio) of mobile device 12a receives short range transmissions from mobile device 12b, and such beaconing is performed using short-range transmissions. “In Fig. 1, links 28”

(yellow) “illustrate example ad-hoc connections between mobile devices 12,” in which “*Wi-Fi technology* may be used to implement the detection process. ... Additionally or alternatively, ... mobile devices 12 may use *BLUETOOTH technology* to detect matches in proximity.” EX1007, ¶66, FIG. 1.



EX1007, FIG. 1 (annotated).

“This *beaconed data may be broadcast within any suitable range*, depending on the technology being employed.” EX1007, ¶57; *see* EX1007, ¶76 (“[A]lthough

a 300-foot range is described as an example, a smaller or larger range is also contemplated for detecting other users in proximity.”). The proximity beacon transmissions, based on Wi-Fi or Bluetooth, are “short range,” when compared to cellular/WAN transmissions. EX1002, ¶¶118-121.

Finally, there are a plurality of such short-range, proximity beacon transmissions. A POSITA would have understood Ribaudó’s explanation that “[m]obile devices 12 may *beacon* data that can be used to identify them,” EX1007, ¶191, along with Ribaudó’s disclosure that Wi-Fi and Bluetooth are the standards used for proximity detection, EX1007, ¶66, as teaching that each mobile device transmits *a plurality of* short-range, proximity beacon transmissions, EX1002, ¶¶122-125. This is because Wi-Fi and Bluetooth beacons are well known to POSITAs as periodic signals (sent a plurality of times). *Id.* (citing EX1025, 420 (“Beacon interval”); EX1026, 131-132 (“beacon train”)). Watanabe similarly teaches that a plurality of beacons can be transmitted “continuously” or “periodically.” EX1006, ¶¶14, 46, 49.

Ribaudó also teaches receiving a plurality of beacons from more than one other mobile device. For example, Ribaudó explains that “John’s mobile device 12 detects Steve’s mobile device 12 at a first time” and subsequently “detects Mary’s mobile device 12 at a second time.” EX1007, ¶148; EX1002, ¶126.

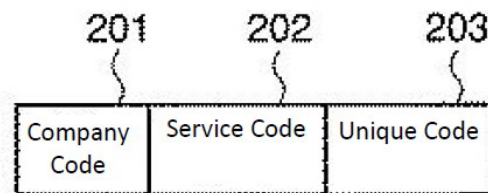
8. 1[f][2]

The Ribaudo-Watanabe combination teaches or renders obvious 1[f][2]. The mapping below is an example of how Ribaudo-Watanabe teaches 1[f][2]:

Claim Element	Ribaudo-Watanabe
“respective MAC address”	Ribaudo’s MAC address of transmitting device
“respective unique identifier”	Ribaudo’s client ID and potentially other suitable information for uniquely identifying a user ⁴ or entity (e.g., Watanabe’s company code)
“PBSI”	Ribaudo’s SSID of the proprietor of the system (10) as sent from transmitting device (e.g., 12b); or Watanabe’s service code

Additionally, the Ribaudo-Watanabe combination teaches each proximity beacon transmission including these three elements. EX1002, ¶¶127-141. For example, Watanabe teaches a beacon transmission including multiple identifiers. EX1006, FIG. 2, ¶¶14-15, 33, 49, 63.

[FIG. 2]



EX1006, FIG. 2.

⁴ As discussed below, Ribaudo contemplates that, in addition to “client ID,” other suitable information can be used to uniquely identify a mobile device user.

As depicted in Figure 2, Watanabe describes a beacon transmission that includes a “unique code 203 specific to the ... transmitter,” which identifies a device transmitting the beacon. EX1006, ¶15. Watanabe’s “unique code” is similar to Ribaudó’s MAC address and the claimed respective MAC address, which also identifies the transmitting device. EX1007, ¶¶68-69, 157. Watanabe’s “company code 201 indicat[es] the service provider company.” EX1006, ¶15. Watanabe’s “company code”—which identifies a particular entity (a company rather than a device)—is similar to Ribaudó’s client ID and the claimed “respective unique identifier,” which identifies a particular entity, such as a user. EX1007, ¶¶46, 84-85, 155-156. Watanabe’s “service code 202”—which “indicat[es] the type of service that can be provided”—teaches the claimed “PBSI.” EX1006, ¶15; EX1002, ¶129. Thus, Ribaudó in view of Watanabe renders obvious a beacon transmission including each of the claimed identifiers. *Id.*

As explained in Section V.C, Ribaudó teaches beaconing MAC addresses, client IDs, and SSIDs. In view of Ribaudó’s beaconing, a POSITA would have found it obvious to beacon such identifiers together as taught in Watanabe to enable efficient processing and filtering of received beacon transmissions. Section V.C.

MAC address: As Ribaudó explains, “[t]he adaptor 18 of a mobile device 12 ... may use the 802.11 frame or media access control (MAC) layer for detecting

other mobile devices 12 in proximity.” EX1007, ¶21; *see also* ¶25 (“Mobile devices 12 may be identified on network 16 by a network address or combination of network addresses, such as a *MAC address*.”), ¶¶27, 68-69. Ribaudo further discloses that “[t]he *unique MAC address* of mobile device 12a *may be beacons* when the BLUETOOTH interface of mobile device 12a is active.” EX1007, ¶157. Although specifically referencing device 12a, a POSITA would have understood Ribaudo teaches that each of the other mobile devices (12b, 12c, etc.) may likewise beacon its unique MAC address. EX1002, ¶131.

Unique identifier: Ribaudo teaches: “[m]obile device 12 may beacon data such as *the client ID of the user* associated with mobile device 12 (and possibly the user’s availability level and other identification information, such as trust score and status).” EX1007, ¶57; *see also* ¶84. Ribaudo describes the “client ID” as one of several “identifiers (IDs) for a user,” and explains that “[t]he client ID may include a public ID that may be broadcast from mobile device 12 and used by mobile devices 12 to detect a match in proximity[,]” or that it “may be used to shield the true identity of the user, for privacy purposes for example. Alternatively, the client ID may simply be the user ID of the user, which ... may reveal the true identity of the user.” EX1007, ¶¶45-46; *see also* ¶140 (listing identifiers of “another user” as including “an email address, telephone number, name, [etc.], or *other suitable information for identifying [a] user*”), ¶85. The client ID and potentially other

suitable information⁵ included in Ribaudó's beacons that uniquely identifies a user is thus a "*unique identifier*." EX1002, ¶¶132-133.

Proximity Beacon Service Identifier ("PBSI"): The term "PBSI" is not a term of art, but as discussed in Section II.B, during prosecution, the inventor of the '918 patent submitted a declaration explaining that the claimed "PBSI" may be satisfied by an SSID, citing the specification's description that "the SSID may be used to indicate that these particular beacons are associated with a service." EX1011 (Proctor Decl.), ¶124, Exhibit 8, n.5; EX1001, 10:52-59; EX1002, ¶134. In view of the inventor's characterization of a *PBSI*, Ribaudó's SSID teaches the claimed "*PBSI*." EX1007, ¶123.

Ribaudó discloses that "[i]n ad hoc mode, in certain embodiments, application 20" of a mobile device "may beacon an *SSID of 'proprietor_name.net'* (e.g., where 'proprietor_name' corresponds to the name of a proprietor of system 10)." EX1007, ¶135. Ribaudó teaches that the "proprietor_name.net" may be associated with a particular service—for example, where the proprietor is a user matching platform (e.g., an online dating platform), the SSID itself may be associated with, and therefore identify, one more services

⁵ An example of other suitable information may include Watanabe's company code. EX1006, ¶15; EX1002, ¶133.

provided by the proprietor (e.g., providing dating matches). EX1007, ¶¶97-104, 138 (discussing “dating” related services). Thus, Ribaudó’s “SSID of ‘proprietor_name.net’” teaches the claimed *PBSI* under the inventor’s interpretation of the claim term. EX1011 (Proctor Decl.), ¶124; EX1002, ¶136.

Additionally, the Ribaudó-Watanabe combination teaches the *PBSI*. EX1002, ¶137. Watanabe discloses the transmission of beacons containing multiple fields, including a “*service code 202* indicating the type of service that can be provided” via that device. EX1006, ¶15. Such a service code 202 also teaches the claimed “*PBSI*” because it identifies a type of service available via the beacon transmitter device. EX1002, ¶137; EX1006, ¶¶14-15, FIG. 2.

In the Ribaudó-Watanabe combination, a POSITA would have found it obvious and would have been motivated to use a “service code” to convey service information—e.g., providing a user matching platform and/or providing dating matches to users within a given area—as described in Ribaudó. EX1007, ¶¶97-104, 123; EX1006, ¶15; EX1002, ¶138. For example, such a service code would indicate that a particular beacon transmission corresponds to a “dating” service. Conveying Ribaudó’s service information using such a parameter would identify beacon transmissions received from other devices as relevant to the particular service (e.g., a user matching service or dating platform). EX1002, ¶138.

A POSITA would have been motivated to beacon a service code together

with Ribaudó's MAC addresses and client IDs to filter out beacon transmissions based on service codes (i.e., services the user is interested in). EX1002, ¶139. For example, as further described with reference to claim element 1[g], including a service code would allow mobile devices receiving beacon transmissions to efficiently filter beacon transmissions as described in both Watanabe and Ribaudó. *Id.*; Sections V.C, V.D.9.

Thus, a POSITA would have been motivated to include a service code, as taught by Watanabe, along with Ribaudó's other identifiers (MAC addresses, SSIDs, and client IDs) to convey service information, such as an indication that a particular beacon transmission corresponds to a matching or dating service. EX1002, ¶140.

A POSITA would have had a reasonable expectation of success in applying Watanabe's teachings to Ribaudó. EX1002, ¶141; Section V.C. Both describe receiving beacon transmissions comprising identification information from a nearby device, via Bluetooth, receiving preset identification information relating to an entity from a server using the Internet, assessing the contents of the beacon transmissions, and determining whether the transmitting device is in proximity by utilizing the transmitted identification information and the preset identification information. EX1006, ¶¶46-55; EX1007, ¶¶6-7. A POSITA would thus have understood that these references disclose interrelated teachings based on well-

understood technologies that would have been amenable to various combinations with predictable results. EX1002, ¶141.

9. 1[g]

Ribaudo-Watanabe teaches or renders obvious 1[g].

Ribaudo discloses that “[m]obile devices 12 are operable to detect matches in proximity in any suitable manner,” EX1007, ¶65, including by determining whether a particular short-range transmission includes well-known network identifiers, such as a MAC address and an SSID, EX1007, ¶¶20-21, 66-77, 123-124. Ribaudo discloses that “a first user’s mobile device detects the presence of a second user’s mobile device in proximity based on *network identifiers* communicated from the mobile devices of the first and second users,” and that this detection is achieved by “*processing* the network identifiers.” EX1007, ¶7; *see also* ¶6, cl. 1. Ribaudo teaches that MAC addresses and SSIDs are examples of network identifiers. EX1007, ¶¶20, 25, 117, 213. Again, an SSID is an example of the claimed PBSI. EX1011, ¶124.

As discussed for 1[f][1]-[2] above, Ribaudo teaches that network identifiers are received via a short-range transmission, such as a Wi-Fi or Bluetooth beacon. EX1007, ¶¶66, 142, 157, FIG. 1. Ribaudo’s mobile device “*compares*” the identifiers received via beacon transmission “with the pre-processed match data stored on the user’s mobile device” to determine matches. EX1007, ¶6; *see also*

¶¶48-51, cl. 9 (“comparing the *one or more network identifiers* received from the first mobile device to the plurality of network identifiers received from the plurality of other mobile devices.”). Ribaudó’s teaching of “processing” and “comparing” network identifiers entails ***determining that such identifiers (MAC and PBSI) are present*** in the beacon transmission. EX1002, ¶¶142-146.

Additionally, Ribaudó-Watanabe teaches 1[g]. In view of Watanabe’s teaching of multiple identifiers being included in a beacon transmission and determining whether two identifiers match, the combination also teaches determining whether two particular identifiers are present in a transmission. EX1006, FIG. 2, ¶¶14-15, 33, 41, 48-49, 51-52, 57, 63. Specifically, Watanabe teaches determining whether beacon transmissions include a beacon service identifier, such as a “service code.” Watanabe describes filtering beacon transmissions based on “service codes” corresponding to a particular service. EX1006 ¶¶41, 48-49. For example, Watanabe describes identifying particular beacon transmissions that include particular service codes when determining whether a user has entered into a contract to receive services corresponding to the service code. EX1006, ¶¶41, 51-52, 57, FIG. 8; EX1002, ¶¶147-148. A mobile device receiving a service code “S2” included in a transmitted beacon may check the service code for filtering purposes and to determine whether the beacon is associated with a particular service. EX1006, ¶52; *see also* ¶15 (referring to a service code as part of a “filter” code). Thus, Watanabe teaches determining whether a beacon transmission includes a service code corresponding to a particular

service type. EX1002, ¶¶147-148. Given Ribaudó's teaching of determining that a MAC address is present in a beacon transmission, a POSITA would have found it obvious to identify both a MAC address and a PBSI in a beacon transmission based on Watanabe's teaching of using two identifiers (e.g., a company code and a service code) to filter beacon transmissions. EX1006, ¶52.

Finally, Ribaudó-Watanabe teaches a PBSI that indicates that *the particular short range transmission is a proximity beacon transmission associated with the proximity beacon service*. Ribaudó teaches that a mobile device “**may beacon an SSID** of ‘proprietor_name.net’ (e.g., where ‘proprietor_name’ corresponds to the name of a proprietor of system 10).” EX1007, ¶123. As discussed for Element 1[f][2], the SSID itself may be associated with, and therefore identify, one or more services provided by a proprietor. EX1007, ¶¶29, 55, 71, 97-104, 162, 223, 226; EX1002, ¶149. Additionally, when using Watanabe's service code, such a service code would indicate that a particular transmission is associated with a proximity beacon service because the “**service code 202** indicat[es] the type of service that can be provided” via that device. EX1006, ¶15. In the Ribaudó-Watanabe combination, a particular beacon transmission would include a service code to identify the transmission as being related to a particular matching service provided by Ribaudó (e.g., a dating service). Section V.C; EX1002, ¶149.

10. 1[h]

Ribaudo teaches that a mobile device determines if an entity or object associated with the proximity beacon service is in proximity to the mobile wireless device by utilizing the “identifier related information” and the “unique identifier,” as follows:

Claim Element	Ribaudo
“identifier related information”	pre-processed match data from server
“unique identifier”	client ID and potentially other suitable information for uniquely identifying a user

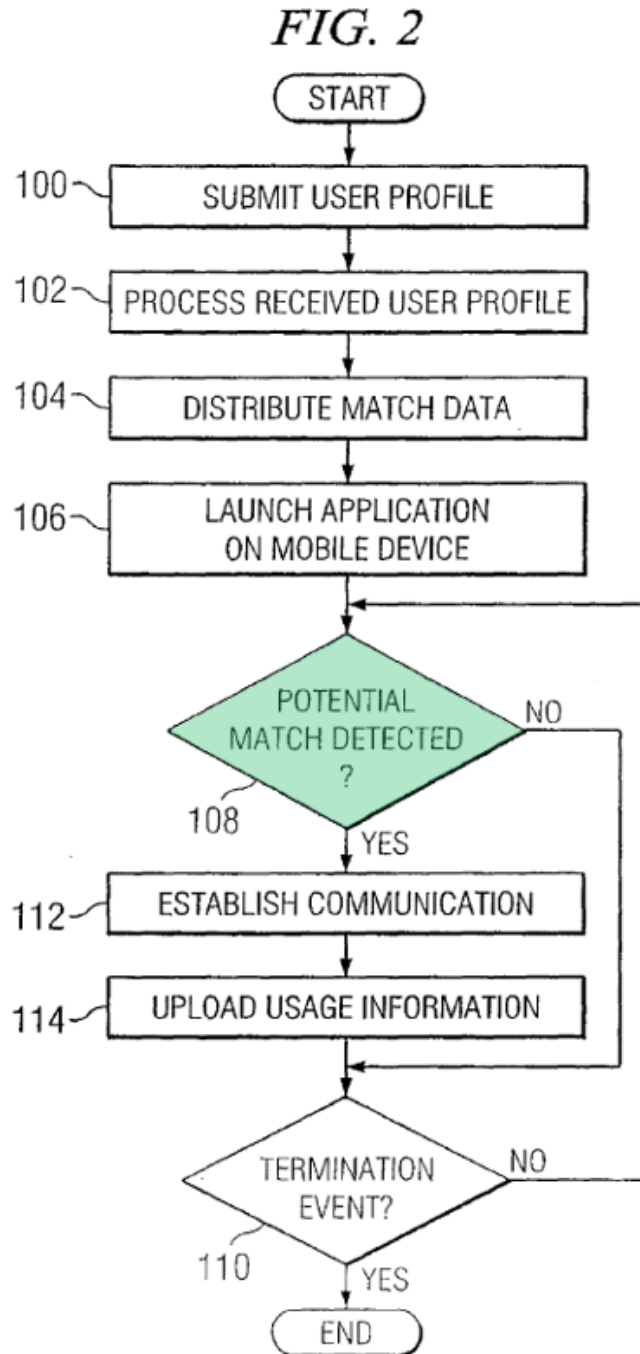
Ribaudo explains that “when the user is in proximity to another user, the user’s mobile device detects the presence of the other user’s mobile device, *receives an identifier associated with the detected other user, and compares* the received identifier *with the pre-processed match data* stored on the user’s mobile device to determine whether the other user is one of the user’s predetermined matches. ... [T]his detection of another user in proximity and determination of whether another detected user is a match is performed locally on the user’s mobile device.” EX1007, ¶6; *see also* ¶16 (same).

In Ribaudo’s Figure 2, “a user of mobile device 12a submits a user profile 24a to data center 14,” which then “pre-processes the information ... to generate match data 26 for the user,” and then “distributes the generated match data to one or more appropriate mobile devices 12.” EX1007, ¶¶80-83, FIG. 2. As shown below, “[a]t

step 106, the user of mobile device 12a launches application 20[,]" which:

may attempt to detect other mobile devices 12 in proximity to mobile device 12a. Using match data 26a (e.g., the match IDs) downloaded from data center 14, mobile device 12a may be operable to detect other mobile devices 12 that may be associated with a user who is a potential match. *Mobile device 12a may beacon* data such as *the client ID of the user* associated with mobile device 12a (and possibly his availability level and other identification information, such as trust score and status). ... [and] may also listen for data being beaconsed by other mobile devices 12.

EX1007, ¶84.



EX1007, FIG. 2 (annotated).

Finally:

At step 108, *mobile device 12a determines whether a match is detected in proximity*. ... The detection process may be used, for example, so

that a user's mobile device 12 becomes aware that another client ID is on the same or a different network subnet and/or within wireless proximity... [W]hen mobile device 12a *detects another client ID* (or other suitable identifier indicating a potential user of system 10), mobile device 12a may *consult match data 26a to determine* whether the user associated with the detected client ID is identified in the match data 26a for mobile device 12a.

EX1007, ¶85; *see also* ¶148 (explaining how to determine whether Steve and Mary are in proximity).

Accordingly, Ribaudó's mobile device determines whether an entity (e.g., user of another mobile device) associated with a proximity beacon service is in proximity, based on pre-processed match data received from the data center ("identifier related information"), and the user's client ID (the "unique identifier"). EX1002, ¶¶150-156.

E. Independent Claim 9

The limitations of claim 9 closely map to the limitations of claim 1, as indicated below. EX1002, ¶¶157-161.

9[pre]	Elements 1[pre] and 1[c]-[e]. Sections V.D.1, V.D.4-6.
9[a]	Elements 1[a] (first radio) and 1[e]. Sections V.D.2, V.D.6.

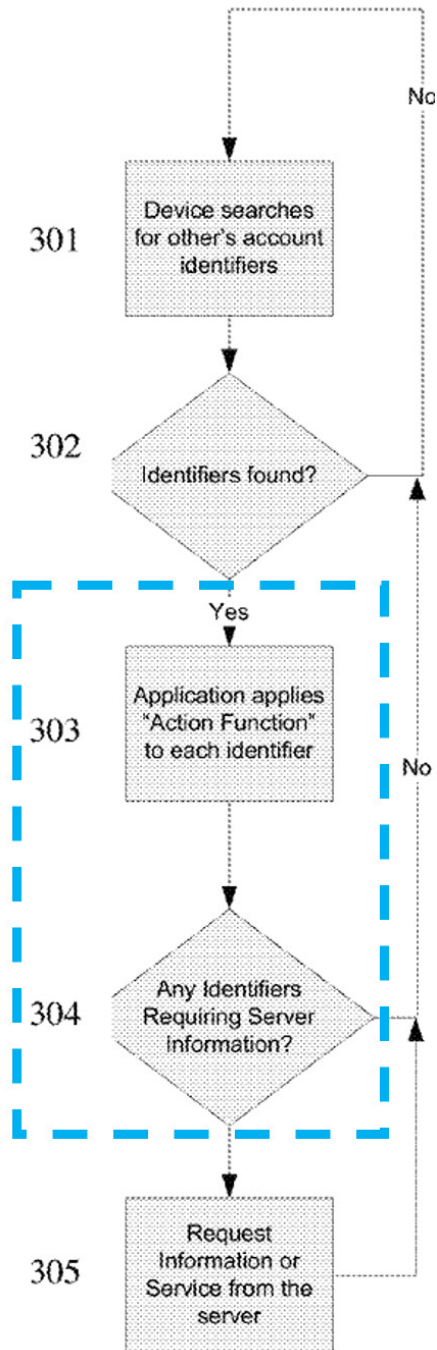
9[b]	Elements 1[b] (second radio) and 1[f][1]-[2]. Sections V.D.3, V.D.7-8.
9[c]	Element 1[g]. Section V.D.9.
9[d]	Element 1[g]-[h]. Sections V.D.9- V.D.10.

F. Dependent Claims 4-6, 14, 16-22, and 24-30

1. Claim 4

The term “action function” is not a term of art. EX1002, ¶¶162-163. The ’918 patent refers to an “action function” as acting “as a filter that determines which of the detected identifiers should be passed to the server.” EX1001, 8:15-25, 22:65-23:3. Steps 303 and 304 of Figure 3 depict using an “action function” to determine whether additional information from a server is needed. EX1001, 8:9-47; EX1011 (Proctor Decl.), ¶134. The ’918 patent provides an example where if identifiers corresponding to a user’s “friends list” are already stored on the detecting mobile device, “re-requests to the server” are not needed. EX1001, 8:34-47.

Figure 3



EX1001, FIG. 3 (annotated).

Ribaudo teaches this functionality when determining that a detected

identifier matches a client ID that was previously downloaded to a detecting mobile device. EX1002, ¶¶164-165. As discussed for Elements 1[f][1]-[2] and 1[h], Ribaudo teaches a beacon transmitter device that broadcasts a client ID and other suitable information to uniquely identify a user (a “*unique identifier*”), which is then used by another mobile device “to detect a match in proximity.” EX1007, ¶¶46, 57; Sections V.D.7-8, V.D.10. Ribaudo’s mobile device compares detected identifiers received via beacon transmission “with the *pre-processed match data* stored on the user’s mobile device” to determine whether a match is in proximity. EX1007, ¶¶6-7 (describing match determination “*without consulting the data center*”); *see also* Abstract, ¶¶16, 48-51, cl. 9. The match data is downloaded from the data center 14 and includes unique identifiers in the form of match IDs and client IDs. EX1007, ¶¶48-51, 53. Because no additional information is needed from the server to detect a match in proximity, Ribaudo teaches the claimed use of *an action function*. EX1002, ¶¶164-165.

2. Claim 5

Ribaudo teaches determining that a *beacon transmitter is a broadcast device* corresponding to a *predetermined location* when matches are detected at a particular location using stored match data. EX1007, ¶¶117, 160-161, 212. Ribaudo describes an “implied proximity” scenario, which involves “distribut[ing] pre-processed matches to members of a particular group *at a particular location*

and/or time”—e.g., “a conference, a cocktail party, a speed-dating event.”

EX1007, ¶160. And “match data 26 may be sent to some or all users who are members of a particular group at a particular time or location.” EX1007, ¶¶163, 166. Therefore, when a match is detected at a particular location, the mobile device determines that the device broadcasting the beacon is associated with the predetermined location. EX1002, ¶¶166-167.

Ribaudo also teaches “location” tag information that can associate detected matches with particular locations. EX1007, ¶¶117, 160-161, 166, 185-186, 202, 213, 216. Users can edit this tag information to “include more useful information about the location, such as ‘CES-ConferenceRoom4,’ ‘MainStreetCafe,’ ‘DFWAirport-Terminal3,’...” EX1007, ¶117. Using this location tag information, mobile devices can associate a detected matching mobile device with the tagged predetermined location. EX1007, ¶117. Ribaudo’s correlation of a detected mobile device and a user match with a location tag therefore also teaches claim 5. EX1002, ¶¶168-170; EX1007, ¶¶186, 202, 216 (describing detection of mobile devices at specific locations based on wireless access points at those locations).

3. Claim 6

Ribaudo teaches sending a client ID (claimed *unique identifier*) to a server to download application software, which renders claim 6 obvious. The downloaded application software can also be part of the claimed identifier related information

when downloaded with match data.

Ribaudo teaches a mobile device that sends a client ID to a server when accessing another user's "personal URL," which may include the client ID (e.g., "www.proprietor_name.net/**clientid**_82740AF3RT432"). EX1007 ¶¶126-147, FIG. 3; Section V.D.8; EX1002, ¶¶171-175. Registered users may be assigned one or more personal URLs by data center 14. EX1007, ¶126. A mobile device may use the personal URL to connect to data center 14 and retrieve match data. EX1007, ¶¶128-130. Alternatively, a user may select a summary link showing the client IDs of nearby users to connect with the data center. EX1007, ¶139. A POSITA would have understood that accessing the personal URL or summary link transmits the client ID to the data center. EX1002, ¶¶174-175 (citing EX1012, ¶¶6-7, 9-13).

Upon connecting with the data center 14 using the client ID, Ribaudo discloses that a user (who may not be registered) "may also download application 20" to engage in messaging. EX1007, ¶¶139-140; *see also* EX1007, ¶¶81, 154. Thus, Ribaudo teaches downloading application software in response to sending a client ID to a server. EX1002, ¶176.

A POSITA would have found it obvious to download Ribaudo's match data (claimed *identifier related information*) together with the application software when additional plug-ins are downloaded or when a user initially joins Ribaudo's

matching service. EX1002, ¶177. For example, a mobile device without the application can access a personal URL, join the matching service, and download the application along with match data from data center 14 either concurrently or sequentially. EX1007, ¶139-140; Section V.D.6 (1[e]). Accordingly, Ribaudo renders obvious *identifier related information* comprising *application software* when match data and software are initially downloaded onto a mobile device. EX1002, ¶177. This is consistent with the museum example discussed during prosecution. EX1011, ¶¶104-107.

4. Claims 14/19

Ribaudo teaches claims 14/19. Ribaudo's mobile device sends a unique identifier associated with another mobile device and/or user, via the first radio (e.g., cellular or WAN link) to the server, and thereafter receives *further information* (e.g., sales communications) relating to an entity (e.g., other user) associated with being within proximity to the mobile device.

For example, Ribaudo describes identifying a "client ID" as part of detecting a "personal URL" from a mobile device in proximity. EX1007, ¶¶127, 132, 141-142, 145, 154-155; Section V.D.10 (1[h]). When this personal URL is accessed, Ribaudo sends the client ID to a server of data center 14 to form a connection. EX1007, ¶¶127-128; Section V.F.3 (Claim 6). This occurs over a *first radio*. Section V.D.2 (1[a]). Upon accessing the server, Ribaudo describes receiving

additional information (claimed *further information*) related to the object or entity corresponding to the detected client ID/personal URL. EX1007, ¶¶128-132, 139 (receiving features of a user profile, commonalities from user profiles, and introduction messages); *see also* ¶¶100, 145, 150. Ribaudo describes servers providing “a user’s web log, photos, podcasts, personal advertisements, classified advertisements, advertisements, and other suitable content.” EX1007, ¶¶215, 217. For merchants/customers in a sales context, Ribaudo also provides *further information* including “Market Information” or commonalities with a salesperson’s profile. EX1007, ¶¶106, 140.

Thus, Ribaudo teaches a mobile device that sends a unique identifier to a server to receive additional information related to an object or entity within proximity to the mobile device. EX1002, ¶¶178-181.

5. Claims 16/24

Ribaudo teaches claims 16/24 by enabling communications between mobile devices, controlling advertising, and/or blocking communications. EX1002, ¶¶182-186.

When a proximity match is detected, Ribaudo’s mobile device notifies its user, “allowing the user to initiate an interaction with the detected match.” EX1007 ¶26; *see also* ¶79. Once an interaction is initiated, mobile devices may exchange messages and access user profile information. EX1007 ¶¶78-79, 81-83, 137.

Allowing communications is an example of *controlling communications* between a mobile device and another device associated with an entity in proximity. EX1002, ¶184.

Ribaudo also describes controlling the types of communications (e.g., advertisements) sent to a wireless device based on the wireless device's proximity to a location, such as a wireless access point or cell tower. EX1007, ¶¶140, 217.

Ribaudo further discloses “controlling further communications” based on user preferences (e.g., “blocking”) or based on location or time. EX1007, ¶¶44, 47, 101, 117, 160, 163; EX1002, ¶186.

6. Claim 17

Ribaudo's “original hash value” teaches the claimed *access code information*. Ribaudo discloses using hashing to authenticate a matched user and prevent unauthorized alteration of a match ID. Data center 14 generates hash values and applies them to match IDs. “Each user may receive the other user's hash value from data center 14 as a part of the match data ... downloaded to the user's mobile device.” EX1007, ¶52. When a match is detected between two mobile devices, each device may calculate a new hash value for the other user's match ID and transmit it for comparison with the “original hash value” received from the data center. This provides a “security mechanism to authenticate matched users” when providing access to communications. EX1007, ¶52.

Thus, the “original hash value” received from the data center (i.e., server) qualifies as “*access code information ... to gain access to the entity*” (i.e., a matched user of another mobile device) “*determined to be in proximity to the mobile device.*” EX1002, ¶¶187-189; Section V.F.5 (claims 16/24).

7. Claims 18/28

As discussed for claims 6 and 14/19, Ribauda describes sending a “client ID” to a server via a cellular or WAN link when accessing a detected “personal URL” from a mobile device in proximity. EX1007, ¶¶127, 132, 141-142, 145, 154-155; Sections V.D.2 (1[a]), V.D.10 (1[h]), V.F.3, V.F.4. Upon connecting with the data center 14 (using the client ID), Ribauda discloses that a user (who may not be registered), may register and join the matching service. EX1007, ¶¶135-137, 154-156. Upon registering, data center 14 generates “match data.” EX1007, ¶137. Data center 14 can then provide this match data to the newly registered user. Section V.D.6 (1[e]); EX1007, ¶¶16, 31, 33, 45-54, 57, 123, 157, 173, 204-205. Thus, Ribauda teaches a mobile device receiving *identifier related information* in response to sending a unique identifier to a server. EX1002, ¶¶190-192.

8. Claim 20

As explained for claims 14/19, Ribauda teaches “*further information*” relating to *advertising content*. EX1007, ¶¶140, 215, 217, 223; Section V.F.4; EX1002, ¶193.

9. Claim 21

Ribaudo renders obvious claim 21.

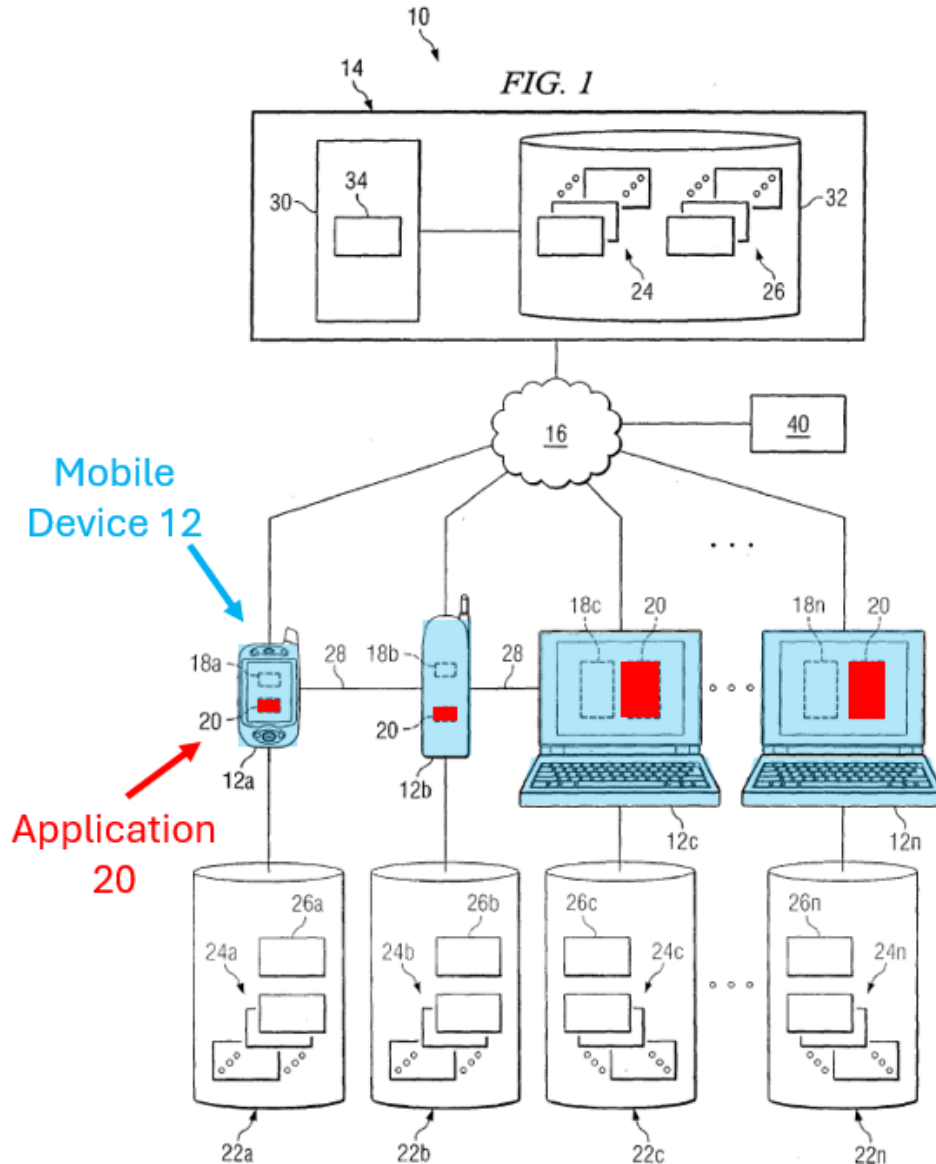
As explained for claims 14/19, Ribaudo teaches that a mobile device sends a unique identifier to the server (a client ID when accessing a personal URL) and subsequently receives *further information*. Section V.F.4. The received *further information* may include sales communications or merchant information related to a merchant nearby the mobile device. EX1007, ¶¶34, 90, 106, 140. Ribaudo additionally describes allowing users to “buy/sell items” or “free agent services.” EX1007, ¶90. Ribaudo provides “Market Information” enabling users to “browse items for sale” and view “text descriptions.” EX1007, ¶106. This browsing mechanism teaches or renders obvious the claimed *service for providing a menu for purchasing items*. EX1002, ¶¶194-195; EX1030, ¶69 (confirming that beaconing “shopping offers, specials, lists and catalogues” was known in the art).

Ribaudo also renders obvious allowing a user to make a purchase and *take delivery at or near the location of a fixed proximity beacon device*. Ribaudo connects buyers and sellers “within proximity” to facilitate “a business transaction.” (e.g., buying/selling goods). EX1007, ¶223; *see also* ¶¶34, 90, 106, 140. When a buyer is located near a seller with items in-hand, delivery naturally occurs near the seller’s beacon transmitter. *Id.*; *see also* ¶6. Thus, Ribaudo renders obvious delivery *at or near* a proximity beacon device. EX1002, ¶196.

Ribaudo-Watanabe further renders obvious such a proximity beacon device being *fixed*. EX1002, ¶197. A POSITA would have found it obvious to implement Ribaudo's transaction facilitation in physical stores, consistent with Ribaudo's "Market Information" and buying/selling disclosures. EX1007, ¶¶106, 223; EX1002, ¶197. Watanabe further teaches that fixed "access point" devices broadcasting beacon identifiers were well known. EX1006, Abstract, ¶¶2-3, 10-14, 46, 50-52, 55, 62, FIG. 8. Accordingly, a POSITA would have found it obvious to implement Ribaudo's "business transaction" functionality using fixed proximity beacons. EX1002, ¶197; EX1030, ¶¶66, 69-70 (confirming that "fixed-location" beacon transmitters in shopping centers were known in the art).

10. Claim 22

Ribaudo teaches mobile devices executing respective instances of "application 20," which provides Ribaudo's matching functionality. Sections V.D.4-5 (1[c]-1[d]); EX1007, ¶¶19, 22-23, 57-58, 78, 81, 120-125, 139-140, 184. Figure 1 from Ribaudo depicts multiple mobile devices with instances of "application 20." EX1007, ¶¶22, 57-58, 184, FIG. 1; Section V.F.3 (claim 6).



EX1007, FIG. 1 (annotated).

As explained for claims 14/19, Ribaudo discloses a mobile device receiving *further information*, which can include user profile information related to a user in proximity. Section V.F.4; EX1007, ¶¶27, 31, 47, 78, 128-132, 139, 158-159. For example, matching “University” information like “Harvard” is provided and displayed on a mobile device. EX1007, ¶47. Users can “view one or more

commonalities,” “differences between the user profiles,” or other profile information. EX1007, ¶¶78, 130. Thus, Ribaudó teaches claim 22. EX1002, ¶¶198-200.

11. Claim 25

As explained for Elements 1[h] (Section V.D.10), Ribaudó “*compares the received identifier with the pre-processed match data*” stored on the user’s mobile device to determine whether the other user is one of the user’s predetermined matches.” EX1007, ¶6. Ribaudó compares a “Client ID” with “match data” to identify matches in proximity. EX1007, ¶85, FIG. 2; *see also* EX1007, ¶¶160-167, 206-207 (describing “Implied Proximity” and “Predictive Data Caching” to derive information); EX1002, ¶¶201-202.

12. Claim 26

a. 26[pre]

Ribaudó’s description of a merchant using a detected customer client ID to send an email with a personalized advertisement to the detected customer teaches the additional features recited in claim 26. Sections V.E, V.F.4 (claims 14/19), V.F.5 (claims 16/24), V.F.8 (claim 20); EX1002, ¶203.

b. 26[a]

Ribaudó teaches a mobile device that detects a unique identifier and sends the unique identifier to a server. Section V.F.4 (claims 14/19). EX1002, ¶204. For example, a merchant’s mobile device can detect a client ID corresponding to a

customer and send the client ID to Ribaudó's data center, which includes a server.

EX1007, ¶140; *see also* ¶¶34, 90, 106, 154-155, 223 (connecting users in proximity for “facilitation of a business transaction, such as the buying or selling of goods or services”).

c. 26[b]

Ribaudó's data center (which includes a server) associates an entity (e.g., user of another mobile device) as being in proximity to the mobile device (sender of the unique identifier) by “processing the network identifiers received from the first and second mobile devices to determine whether the first mobile device and the second mobile device are in proximity to one another.” EX1007, ¶¶7, 149, 172 (“*data center 14 may be operable to determine whether two users are in proximity*”), 172-191, 221. For example, as described for claims 14/19, when data center 14 receives a client ID via a URL, data center 14 identifies a corresponding user. EX1007, ¶128. Data center 14 can also make a proximity association when providing a notification of URL access or user commonalities. EX1007, ¶¶130, 138-141. Ribaudó's data center 14 therefore identifies an object or entity (e.g., user) and associates that user as being within proximity to the mobile device. EX1007, Abstract, ¶17 (data center 14 can record “encounters between users of mobile devices 12”), ¶¶27, 56; EX1002, ¶¶205-206.

d. 26[c]

Ribaudo's server within data center 14 stores a "user's preferences" and "purchasing patterns," which teaches the claimed storage of *purchasing practices*. EX1007, ¶217; *see also* ¶17. Ribaudo explains that [d]ata center 14 may collect and store personality attributes and group attributes," and "[a]ssigning this attribute information to particular wireless access points may enable the data center 14 ... to direct users of mobile devices to specific locations." EX1007, ¶216. Additionally, Ribaudo explains that the user's purchasing practices can be used along with proximity information (e.g., proximity to a wireless access point) to serve "advertisements, personal advertisements, and classified advertisements" and to "enable advertisers to advertise on specific wireless access points (e.g., MAC addresses or cell tower IDs) that have the demographics or the usage that the advertiser is targeting for its ads or other offers." EX1007, ¶217; EX1002, ¶¶207-208.

e. 26[d]

Ribaudo teaches that data center 14 stores email addresses for user accounts to provide notifications or facilitate communications. EX1007, ¶¶94 (generating a user ID using a "user's email address"), 119, 140, 152-153, 156-157. For example, data center 14 can send notifications via an "*email*." EX1007, ¶157. When a merchant device detecting a customer's client ID sends the client ID to data center

14 as described for 26[a], data center 14 can identify the email address corresponding to the detected customer. EX1007, ¶140 (“sales people may use this capability to *facilitate sales initiated by emails*” and “*email ... may increase the chances of a response.*”).

Accordingly, Ribauda teaches a server in data center 14 retrieving an email address corresponding to a prospective client who may have previously registered an account with Ribauda’s matching platform. EX1007, ¶¶140, 156 (describing registration using email); EX1002, ¶¶209-211.

f. 26[e]

As described for 26[d], Ribauda describes a sales context where data center 14 sends an email to an identified email address corresponding to a prospective client. Section V.F.12.e; EX1007, ¶¶140, 152, 157.

Ribauda further explains that the content of the email can be *customized* based on the stored proximity user behavior. EX1007, ¶¶94, 119, 140, 157.

Ribauda explains that “if a first user sends a second user an email ... [a] plug-in may display what the first and second users share in common.” EX1007, ¶140.

This allows “sales people ... to facilitate sales initiated by emails” that “may increase the chances of a response by allowing the recipient to view what he shares in common with the sales person.” EX1007, ¶140; *see also* ¶119 (users can “customize an introduction message”), ¶157 (“the first user may receive a

notification from data center 14 via ... email.”). Ribaudó therefore teaches customized email communication. A POSITA would have further found it obvious to include “advertisements, personal advertisements, and classified advertisements” in such an email sent by the data center based on Ribaudó’s tracking of “a user’s preferences, purchasing patterns, destinations, and other personalized information” to further aid a salesperson in establishing “rapport with a prospective client [to] increase the likelihood of making a sale.” EX1007, ¶¶140, 215, 217; EX1002, ¶¶212-214.

13. Claim 27

See Claim 25 and Elements 1[h] and 9[d]. Sections V.D.10, V.E, V.F.11. EX1002, ¶215.

14. Claim 29

Ribaudó teaches mobile devices receiving beacon transmissions without requiring the mobile devices to first transmit any information to other beacon transmitter devices. EX1002, ¶¶216-217. Ribaudó explains that “a user may choose to be invisible to other users.” EX1007, ¶61; *see also* ¶¶44, 101. In this case, Ribaudó’s mobile device can detect matches while not needing to perform initial broadcasting. EX1007, ¶¶61, 84-85; EX1002, ¶217. Additionally, Ribaudó describes different “masks”—such as a “work” or “university” mask—that can control or limit broadcasting by a mobile device. EX1007, ¶61. Ribaudó describes

the ability to still detect matches “without broadcasting a work availability mask.”

EX1007, ¶61. This provides another example of not needing to perform transmissions prior to receiving proximity beacon transmissions. EX1002, ¶217.

15. Claim 30

a. 30[pre]

See Claim 1. Section V.D; EX1002, ¶218.

b. 30[a]

As discussed for 1[e], Ribauda teaches that mobile devices receive identifier related information (*e.g.*, match data) via a first radio (*e.g.*, cellular or WAN).

EX1007, ¶16; Section V.D.6. Ribauda explains that match data stored on a mobile device can include a *list of contact information*. EX1007, ¶¶94-96, 109, 111-114, 233. For example, Ribauda describes maintaining contact lists of “Friends and Acquaintances” or “Business Networking” contacts. *Id.* A user may create contact lists such as “Cornell University Friends, Dallas Friends, or High School Friends.” EX1007, ¶114. These contact lists are used to identify matches in proximity:

“When a contact is detected by a user’s mobile device 12 ... application 20 may remind the user of the relevant facts about the contact.” EX1007, ¶96. Ribauda’s system can “notify the users when their contacts are nearby and provide relevant information.” EX1007, ¶¶106, 109, 114. Thus, Ribauda’s match data—which is used when detecting matches in proximity and teaches the claimed *identifier related information*—can comprise a list of contact information. EX1002, ¶¶219-

221.

c. 30[b]

As explained for 1[e], 1[f][1]-[2], and 1[h], Ribaudó describes a mobile device detecting beacon transmissions, determining that the beacon transmissions are associated with a proximity beacon service, and comparing received identifier information with match data stored on the mobile device to identify mobile devices corresponding to matches in proximity. Sections V.D.6-8, V.D.10. For example, Ribaudó's mobile device "detects another *client ID* (or other suitable identifier indicating a potential user of system 10)" and "may *consult match data 26a to determine* whether the user associated with the detected client ID is identified in the match data." EX1007, ¶85; Section V.D.10.

In the contacts list example, Ribaudó teaches employing this same comparing and matching technique to identify matches within a list of contact information. Section V.F.15.b (30[a]). Ribaudó describes detecting a contact's mobile device in proximity and subsequently providing a notification and contact information. EX1007, ¶¶96, 109, 114, 223. Ribaudó also describes matching contacts and providing match data for those contacts to mobile devices. EX1007, ¶¶83-85, 95, 111, 141. Thus, to facilitate Ribaudó's proximity detection of contacts from a list, Ribaudó teaches comparing contact identifier information (e.g., match data with contact information) to a unique identifier (e.g., Ribaudó's client ID).

EX1002, ¶¶222-224.

d. 30[c]

Ribaudo teaches that “[m]obile device 12 may notify its user if such a match is detected in proximity, allowing the user to initiate an interaction with the detected match if desired.” EX1007, ¶26; *see also* ¶79. Once an interaction is initiated, mobile devices may exchange messages and access respective user profile information. EX1007, ¶¶78-79, 81-83, 137. Communications or “conversation resulting from the detection” may occur for users on a contact list. EX1007, ¶96; *see also* ¶87 (“If a match is detected ... communication between matched users of mobile devices 12 may be established”), ¶140. Ribaudo therefore teaches facilitating communication between matches including those from a contact list. Sections V.F.15.b-c; EX1002, ¶¶225-226.

Ribaudo further explains that such communications can utilize the first radio when the communications are routed through data center 14. For example, as described for 1[a], Ribaudo’s mobile device uses a first radio (e.g., cellular or WAN) to communicate with data center 14. Section V.D.2; EX1007, ¶79 (using a “TCP/IP” or “cellular” protocol “to create a messaging connection between mobile devices”); *see also* ¶¶76, 156 (describing data center 14 routing messages between parties); EX1002, ¶227.

Thus, Ribaudo teaches allowing further communications between matched

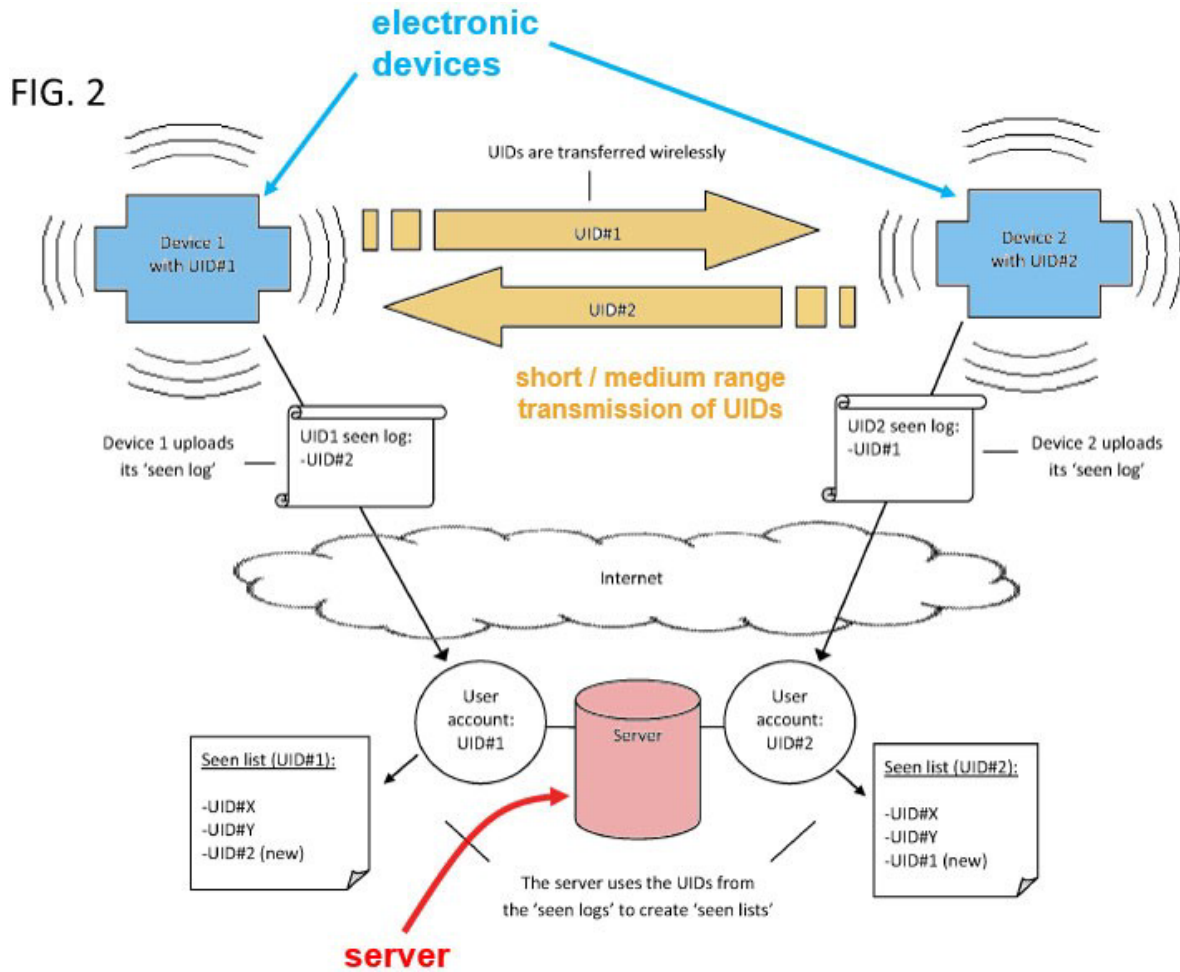
mobile devices via a contact list and using a *first radio* connection with data center 14 to facilitate the communications. EX1002, ¶228.

VI. GROUND 2: RIBAUDO-WATANABE-BEHRENS RENDERS OBVIOUS CLAIMS 3, 7-8, 10, 12-13, 15, AND 31

A. Behrens

Behrens teaches portable electronic devices (mobile phones) that “continuously/repeatedly transmit” and scan for “unique identifiers (UID) via non-directed wireless radio frequency transmission” to establish social networks. EX1008, Title, 11:1-5; EX1002, ¶¶82-84. The UID “contains information for identifying the device (and thus its user).” EX1008, 6:6-8. The UID “may consist of or include a MAC (media access control) address, Bluetooth Device Address (i.e., BD_ADDR), or other unique or quasi-unique identifier.” EX1008, 11:21-26. Behrens’s system “may even allow a user to have multiple or changing UIDs and, therefore, different online identities,” which “may also be linked to a single user account.” EX1008, 23:1-5.

Figure 2 shows electronic devices (blue) in communication with a server (red), where the “two devices send[] out UIDs” via short- and medium range transmission (yellow). EX1008, 32:21-22, FIG. 2.



EX1008, FIG. 2 (annotated).

B. Motivation to Combine

A POSITA would have been motivated to combine the teachings of Ribaud-Watanabe with Behrens to facilitate Ribaud's capability of allowing a user to selectively "shield" or "reveal" her true identity in different circumstances. EX1007, ¶¶45-46, 68; EX1002, ¶¶229-233. A POSITA would have had a reasonable expectation of success in combining Ribaud, Watanabe, and Behrens because each relates to detecting nearby wireless devices and establishing

communications. EX1007, Abstract, ¶18; EX1006, Abstract; EX1008, 1:6-9. *See* Sections V.C-V.D; EX1002, ¶234.

As explained for Ground 1 above, Ribaud and Watanabe teach a mobile device receiving a plurality of proximity beacon transmissions, each including a MAC address, unique identifier, and Proximity Beacon Service Identifier (“PBSI”). EX1002, ¶230.

Behrens teaches electronic devices that “continuously/repeatedly transmit” and scan for “unique identifiers (UID) via non-directed wireless radio frequency transmission.” EX1008, 11:1-5. In Behrens, a UID “may consist of or include a [WLAN] MAC (media access control) address, Bluetooth Device Address (i.e., BD_ADDR), or other unique or quasi-unique identifier.” EX1008, 11:21-26, 22:25-27. Behrens’s “software may instruct the device for sending out a UID via short or medium range wireless transmission” and may “obtain the device’s own UID(s)” or “assign (or allow the user to assign) a UID.” EX1008, 22:24-28. Moreover, “[e]ven in the event that the device has a UIDs, the software may allow use of a different UID.” EX1008, 22:28-29. Behrens teaches that “this may be beneficial to the user” because it “may even allow a user to have *multiple or changing UIDs* and, therefore, different online identities,” which “may also be linked to a single user account,” where the user could manage them. EX1008, 23:1-5. Behrens cites “MAC addresses” as a type of UID. EX1008, 19:8-14. A

POSITA would thus have understood that Behrens teaches that multiple unique identifiers and MAC addresses may be associated with the same user device, which is used to transmit beacons. EX1002, ¶231.

Ribaudo similarly describes that “a user (e.g., of mobile device 12a) may be associated with *one or more client IDs*, which may identify the user publicly,” EX1007, ¶68, and that “[t]he client ID may be used to shield the true identity of the user, for privacy purposes for example,” or, “[a]lternatively, the client ID may simply be the user ID of the user, which in certain embodiments may reveal the true identity of the user.” EX1007, ¶46. Ribaudo also teaches “*time-slicing* to join and bounce between several networks.” EX1007, ¶72. Ribaudo defines “time slicing” as “bouncing between being associated with an access point for a certain period of time (e.g., milliseconds) and being in an ad-hoc mode for a certain period of time (e.g., milliseconds).” EX1007, ¶72. Ribaudo thus explains that for certain periods of a time a device may have an ID associated with one identity and functionality, and during another period of time, the same device may have a different ID associated with a different functionality. *See id.*

In view of Ribaudo’s teaching of using multiple client IDs, a POSITA would have been motivated to implement Behrens’ teaching that *multiple unique identifiers* (which include MAC addresses or other unique IDs) may be associated with the same transmitting device or mobile device. EX1002, ¶233. Combining

Behrens' teachings would have provided a mechanism for Ribaudó to implement multiple client IDs and multiple MAC addresses, which are sent or received at different times. *Id.* Additionally, Behrens explains that employing multiple identifiers would provide the benefit of a user having "different online identities" so that the user may "create a new online identity for an event or party he attends or has attended." EX1008, 23:2-4. This would provide a mechanism for enabling a user or mobile device to associate multiple unique identifiers with the same entity/object (*i.e.*, the same mobile device user) to facilitate Ribaudó's teaching of using multiple client IDs. EX1007, ¶¶45-46, 61-62, 68; EX1002, ¶233. In the combination, the multiple unique identifiers would be included in beacon transmissions (e.g., via Bluetooth) from the same transmitting device, as taught by Behrens. EX1008, 4:21-24, 11:21-26, 18:21-28, 19:5-14, 25:22-25.

A POSITA would have had a reasonable expectation of success in combining Ribaudó-Watanabe with Behrens. EX1002, ¶234. All three describe similar proximity detection techniques in wireless systems that feature short-range, Bluetooth communication as well as communication to a central server over the Internet. *E.g.*, EX1006, ¶¶46-55; EX1007, ¶¶6-7; EX1008, Abstract, 6:1-30, 19:5-14. As discussed above, Ribaudó already contemplates a system that may assign multiple unique identifiers to a given user in order to "shield" or "reveal" her true identity in different circumstances. EX1007, ¶¶45-46, 68. A POSITA would thus

have understood that applying Behrens' teachings to the Ribaudo-Watanabe system would have yielded predictable results. EX1002, ¶234. Further, a POSITA would have understood that these references disclose interrelated teachings based on well-understood technologies that would have been amenable to various well-understood and predictable combinations. *Id.*

C. Dependent Claims 3, 7-8, 10, 12-13, 15, and 31

1. Claim 3

a. 3[pre]

See Ground 1 - claim 1. Section V.D, V.D.4 (1[c]); EX1002, ¶235.

b. 3[a]

See Ground 1 - Elements 1[f][1]-[2]. Sections V.D.7-8. Ribaudo-Watanabe-Behrens also teaches that a first proximity beacon transmission is received ***at a first time***. A POSITA would have understood that Ribaudo's wireless device receives beacon transmissions from different users, or even the same users, at different times, such as different times during the same day, on different days, etc. EX1007, ¶¶45-46, 58, 60-61, 64, 68, 72 (describing "time-slicing"), 78, 148, 162-164, FIG. 2; EX1002, ¶236.

Behrens describes beacon transmissions transmitted over multiple time periods based on portable electronic devices that "continuously/repeatedly transmit" and scan for "unique identifiers (UID) via non-directed wireless radio frequency transmission" in order to establish social networks. EX1008, Title, 11:1-

5; *see also* 4:21-24, 11:21-26, 18:21-28, 19:5-14, 23:2-4, 25:22-25; EX1002, ¶237.

As further described for Element 3[b], Ribaud-Watanabe-Behrens also teaches changing unique identifiers and MAC addresses at different times. Section VI.C.1.c. Relative to Element 3[b], in Ribaud-Watanabe-Behrens, the first MAC address and unique identifier would be transmitted and received at a first time and therefore the combination teaches 3[a]. EX1002, ¶238.

c. 3[b]

Ribaud-Watanabe-Behrens teach Element 3[b].

First, as discussed for Elements 1[f][1]-[2] in Ground 1, Ribaud’s teaching of “**beacon[ing]** data,” EX1007, ¶191, entails a *plurality* of short-range transmissions—e.g., regular, periodic transmissions of data (including identifiers) to facilitate device discovery. EX1002, ¶¶239-240; EX1007, ¶148. Watanabe corroborates this understanding. EX1006, ¶46 (explaining “transmitter 112 at an access point 11 appends transmitter identification information to a beacon (S501) and continuously or **periodically transmits** the beacon (S502).”).

Second, as discussed in Section VI.B, Ribaud and/or Behrens discloses that *multiple unique identifiers* can be assigned to a given transmitting device, EX1007, ¶68 (disclosing “one or more client IDs”); EX1008, 22:28-29, 23:1-5 (disclosing “**multiple or changing UIDs**”); *see also* 19:8-14 (MAC addresses are UIDs). This beneficially enhances privacy, by allowing “different online

identities,” and/or the ability to “shield” or “reveal” one’s identity depending on context. EX1007, ¶46; EX1008, 23:1-5; EX1002, ¶241.

Additionally, Behrens describes receiving UUIDs that are beacons at different time periods. EX1008, 30:23-31:13. For example, Behrens describes a portable electronic device that scans “continuously/repeatedly for UUIDs sent out by other devices” and records these UUIDs in a log. EX1008, 10:24-11:9, 28:19-20, 31:6-13. “When such a device receives another device’s UUID, it records that UUID and measures the length of time during which it continues to receive that UUID. The device stores the received UUID, along with the time, date and duration of the reception.” EX1008, 11:11-17. Behrens further describes the mobile device determining that the UUID is no longer received and subsequently detecting additional identifiers at a later time. EX1008, 30:27-31:4 (a first device detecting and logging a second device’s identifier at different times). Thus, Behrens describes the transmission of unique identifiers occurring at multiple time periods. EX1002, ¶242. In the Ribaudo-Watanabe-Behrens combination, this would include receiving a *second proximity beacon transmission including a second MAC address and a second unique identifier at a second time*.

Third, the combination also teaches *the second MAC address being different from the first MAC address and the second unique identifier being different from the first unique identifier*. Behrens teaches multiple or changing

MAC addresses. Namely, Behrens teaches that UUIDs—such as MAC addresses—can change. EX1008, 11:21-26, 19:8-14, 22:25-27, 23:1-5.

Ribaudo's client IDs teach the claimed “*unique identifiers*.” Ribaudo-Watanabe-Behrens renders obvious client IDs changing over time. EX1002, ¶243.

Ribaudo and Behrens describe assigning multiple unique identifiers to a given transmitting device. EX1007, ¶68 (disclosing “one or more client IDs”); EX1008, 22:28-29, 23:1-5 (disclosing “*multiple or changing UUIDs*”); EX1002, ¶¶244-245. This beneficially enhances privacy by allowing “different online identities” and/or the ability to “shield” or “reveal” one's identity depending on context. EX1007, ¶¶46, 61-62; EX1008, 23:1-5.

Behrens teaches electronic devices that transmit unique identifiers (UUIDs) that “may consist of or include a *MAC (media access control) address*, Bluetooth Device Address (i.e., BD_ADDR), or *other unique or quasi-unique identifier*.” EX1008, 11:21-26, 22:25-27. Behrens describes using “a combination of different types of UUIDs” which may include “Bluetooth Device Addresses, WLAN *MAC addresses and other types of UUIDs*” when providing beacon transmissions. EX1008, 25:22-25. In this manner, Behrens teaches “MAC addresses” and other unique identifiers as types of UUIDs. EX1008, 19:8-14.

Behrens further teaches that its “software may instruct the device for sending out a UID via short or medium range wireless transmission” and may “obtain the device’s own UID(s)” or “assign (or allow the user to assign) a UID.” EX1008, 22:24-28. Moreover, when a device has multiple UIDs, “the software may allow use of a different UID.” EX1008, 22:28-29. This benefits a user because it provides “*multiple or changing UIDs* and, therefore, different online identities,” which “may also be linked to a single user account,” where the user could manage them. EX1008, 23:1-5. Thus, Behrens describes multiple or changing MAC addresses used in beacon transmissions, and multiple MAC addresses and unique identifiers associated with the same user and/or mobile device that transmits beacons. EX1002, ¶246.

Based on Behren’s teachings, it would have been obvious for Ribaudó’s mobile devices to beacon different client IDs (claimed *unique identifiers*) and MAC addresses at different times for masking or privacy purposes. EX1007, ¶62 (describing using different user IDs with different masks), ¶46 (client ID may be user ID). EX1002, ¶247; Section VI.B.

d. 3[c]

As explained for 3[b], Behrens teaches a unique identifier “uniquely *identifies* a device” and Ribaudó teaches that one or more client IDs “may identify the user publicly.” EX1008, 19:8-10; EX1007, ¶68; Section VI.B. Ribaudó-

Watanabe-Behrens renders obvious a mobile device receiving different identifiers and associating them with a single transmitter device. EX1002, ¶248. For example, a user may change unique identifiers over time for, e.g., privacy reasons but still allow a recipient device to associate the different identifiers with the same user or user device. EX1007, ¶¶46, 61-63; EX1008, 23:1-5 (users may have “different online identities” or “create a new online identity for an event or party he attends or has attended”). In a business-transaction context, it was obvious for a customer to use different identifiers to make different purchases at different times while permitting the merchant to associate the purchases with the same user/device so the merchant could understand purchasing habits and reward repeat business. In a business-networking context, it was obvious for a conference attendee to use different identifiers at different conferences/events while permitting a business contact to associate the identifiers with the same attendee so the business contact could recall previous interactions. Ribaudo describes business-transaction and business-networking contexts. EX1007, ¶¶29, 55, 58, 61-63, 90, 96, 109-114, 140, 223-224, 229-231; EX1002, ¶248. These are just examples and the association may also occur in the other matching services and contexts described in Ribaudo (such as when using Ribaudo’s masking function). EX1007, ¶¶90, 223-224. Accordingly, it was obvious for the receiving device (*e.g.*, mobile device 12a) to associate first and second unique identifiers with the same beacon transmitter device (*e.g.*, 12b,

12c, etc.). EX1002, ¶248.

2. Claim 7

7[pre]	Claim 3. Section VI.C.1.
7[a]	Element 30[a]. Section V.F.15.b.
7[b]	Element 30[b]. Section V.F.15.c.
7[c]	Element 30[c]. Section V.F.15.c.

EX1002, ¶¶249-252.

3. Claim 8

8[pre]	Element 3[pre]. Section VI.C.1.a.
8[a]	Elements 3[a]-3[b]. Sections VI.C.1.b-c.
8[b]	Element 3[c]. Section VI.C.1.d.

EX1002, ¶¶253-255.

4. Claim 10

a. 10[pre]

See claim 9. Section V.E; EX1002, ¶256.

b. 10[a]

See Elements 1[f][1]-[2] and 3[a]. Sections V.D.7-8, VI.C.1.b; EX1002, ¶257.

c. 10[b]

See Element 3[a]-3[b]. Sections VI.C.1.b-c; EX1002, ¶258.

d. 10[c]

See Element 3[c]. Section VI.C.1.d. The recited “particular entity” corresponds to the same particular user of the transmitting device (*e.g.*, user of Ribaudó’s mobile device 12b, 12c, etc.) in the scenarios described in Element 3[c], and “associating” the unique identifiers with that user may occur in different contexts, such as a business transaction, work versus recreation, or business networking. Section VI.C.1.d; EX1007, ¶¶46, 55, 61-63, 90, 96, 109-114, 140, 223-224, 229-231; EX1008, 23:1-5; EX1002, ¶259.

5. Claim 12

a. 12[pre]

See Claim 9. Section V.E; EX1002, ¶260.

b. 12[a]

See Elements 1[f][1]-[2] and 3[a]. Sections V.D.7-8, VI.C.1.b; EX1002, ¶261.

c. 12[b]

See Elements 1[f][1]-[2] and Elements 3[b]-3[c]. Sections V.D.7-8, VI.C.1.c-d. Each of the plurality of transmissions from the transmitting device would include the same “PBSI”—whether Ribaudó’s proprietor SSID (EX1007, ¶123) or Watanabe’s service code (EX1006, ¶15)—to indicate a particular service associated with that device at different times. EX1011 (Proctor Decl.), ¶124; EX1002, ¶262. Taken with Behrens’s teaching of multiple changing unique

identifiers and/or MAC addresses, Ribaud-Watanabe-Behrens still teaches different proximity beacon transmissions maintaining the same PBSI (e.g., Ribaud's SSID or Watanabe's service code). EX1007, ¶¶97-104, 138; EX1008, 11:21-26, 22:25-27, 23:1-5. For example, if the particular service is Ribaud's business networking or business transaction service, the beacon transmissions in the combination would still identify this service even when unique identifiers and/or MAC addresses are changing. Sections V.C, V.D.9 (1[g]) (explaining the beacon transmission filtering provided by Ribaud-Watanabe based on service type), VI.C.d (3[c]). For example, this may occur when identifying users with changing identifiers in a business networking context while using the same "business networking" PBSI or when a merchant associates a customer's changing identifiers with the same customer while using the same "business transaction" PBSI. EX1007, ¶¶29, 58, 90, 96, 109-114, 140, 223-224, 229-231. Using the same PBSI may occur in the other matching services described in Ribaud as well. EX1007, ¶¶90, 223-224. Thus, Ribaud-Watanabe-Behrens teaches each proximity beacon transmissions including the same PBSI. EX1002, ¶262.

d. 12[c]

See Elements 3[c] and 10[c]. Sections VI.C.1.d, VI.C.4.d; EX1002, ¶263.

6. Claims 13/15

Ribaud-Watanabe-Behrens renders obvious claims 13 and 15 for the reasons

presented for claim 4 and below. Section V.F.1; EX1002, ¶¶264-267.

The '918 patent provides no description of what the claimed “preventing” entails or how it may be implemented, demonstrating this feature was obvious. *In re Epstein*, 32 F.3d 1559, 1568 (Fed. Cir. 1994) (“... that appellant did not provide the type of detail in his specification that he now argues is necessary in prior art references supports the Board’s finding that one skilled in the art would have known how to implement the features of the references”); *Paice LLC v. Ford Motor Co.*, 881 F.3d 894, 902 (Fed. Cir. 2014) (cannot hold prior art to higher standard than claimed invention).

Further, Ribaud teaches blocking actions. EX1007, ¶¶ 44, 99, 101-102. For example, “blocking a user may prevent a match from occurring with respect to the blocked user[.]” EX1007, ¶101. Additionally, Ribaud teaches filtering matches based on time or location, thus preventing certain types of matches for a certain time. EX1007, ¶¶55, 58, 61, 229. For example, “at a bar the user may be interested in being notified of business networking matches only on a particular occasion, but at a later time, the user may also be open to being notified of romantic matches.” EX1007, ¶58. Further, as discussed below, Behrens teaches the concept of blocking and blacklisting users, which involves ignoring certain user IDs. EX1008, 6:13-17, 10:20-22, 20:10-20, 26:1-8 A POSITA would have understood or found obvious that a blocked or blacklisted client ID would be ignored and prevented

from being sent to the server. EX1002, ¶265.

Ribaudo also teaches preventing the sending of a unique identifier to a server when determining whether a detected identifier matching a client ID has already been downloaded to a mobile device. EX1007, ¶¶6-7 (describing match determination “*without consulting the data center*”); *see also* Abstract, ¶¶16, 48-51, cl. 9. When no additional information is needed from the server to determine that the detected mobile device is in proximity (e.g., because the unique identifier was previously detected and information was previously retrieved), the mobile device will not request additional information. Section V.F.1. Here, it would have been obvious to prevent sending a client ID to the server to save time and transmission bandwidth, power, etc., of the mobile device. EX1002, ¶¶264-266.

Additionally, Behrens teaches that a user may “instruct the server to ignore specificUIDs,” “tell the server to block specific UUIDs, or to *have the server instruct his portable device to ignore specific UUIDs* and vice versa.” EX1008, 20:10-15. Behrens also teaches “blacklists” which can instruct a server or device to ignore certain UUIDs. EX1008, 26:1-3. In view of Ribaudo’s blocking and/or detection of matches “without consulting” a server, it would have been obvious to a POSITA to additionally instruct the wireless device not to send specific UUIDs rather than send them and have them ignored. EX1002, ¶267. Again, preventing transmission of such identifiers would beneficially reduce use of transmission

bandwidth and power. *Id.* Moreover, it would have been obvious that the specific unique identifier selected for blocking would have been one previously detected because such prior detection and interaction would have provided the reason for blocking it. *Id.*

7. Claim 31

31[pre]	Element 3[pre]. Section VI.C.1.a.
31[a]	Elements 3[a]-3[b]. Sections VI.C.1.b-c.
31[b]	Element 3[c]. Section VI.C.1.d.

EX1002, ¶¶268-270.

VII. GROUND 3: RIBAUDO-WATANABE-BEHRENS-NORDMAN RENDERS OBVIOUS CLAIMS 2 AND 11

Ribaud-Watanabe-Behrens-Nordman teaches Claims 2 and 11.

Ribaud teaches that “[t]he *unique MAC address* of mobile device 12a *may be beacons* when the BLUETOOTH interface of mobile device 12a is active.”

EX1007 ¶157. Behrens demonstrates that MAC addresses and Bluetooth device addresses (BD_ADDR) are interchangeable as identifiers: “a UID may consist of

or include a MAC (media access control) address, *Bluetooth Device Address (i.e. BD_ADDR)*, or other unique or quasi-unique identifier.” EX1008, 11:21-26,

25:22-25 (“a combination of different types of UIDs may be used” include

“Bluetooth Device Addresses, WLAN MAC addresses and other types of

UID[s]”); EX1021, 232; EX1002, ¶¶271-272. Behrens further teaches that “[i]n the

case of Bluetooth, various address parts and lengths (e.g., **48-bit BD_ADDR**, 24-bit LAP, etc.), Friendly Names, as well as a combination thereof may be used.” EX1008, 19:12-14.

Nordman teaches the use of a “pseudonym address,” which is a “randomized version” of a BD_ADDR. EX1046, Abstract, ¶6; EX1002, ¶¶85-86. “The pseudonym address is used in all the functions of the Bluetooth device that normally use the BD_ADDR.” *Id.* “The user can select introducing various parameters into the random number generator as initialization vectors to combine with the BD_ADDR ... to change the random number sequence and thus thwart an eavesdropper's discovery of that sequence.” EX1046, ¶8; *see also* ¶¶12, 57. Nordman further describes providing a “privacy options menu” to allow a user to select different ways of randomizing the BD_ADDR. EX1046, ¶¶34-42. For example, if selected, the user’s Bluetooth device “randomizes the entire 48-bits of the user’s real BD_ADDR(0) to produce the pseudonym address.” EX1046, ¶40; *see also* ¶3.

Nordman’s pseudonym address therefore teaches *a randomly generated 48-bit number matching a format of a Bluetooth BD_ADDR* and Ribaud-Watanabe-Behrens-Nordman teaches using such an address as a MAC address for Bluetooth devices. EX1002, ¶¶273-274.

A POSITA would have been motivated to implement randomly generated

Bluetooth addresses as MAC addresses to advance Ribaudó's objective of enhancing privacy for Bluetooth device users. EX1007, ¶¶46, 78, 225-227 (describing "privacy" as an important user consideration); EX1046, Abstract, ¶¶4-5, 13, 96 (protecting user privacy using pseudonym addresses). Nordman explains that pseudonym addresses protect a user's privacy "by preventing the user's identity, routes, and activities from being correlated with his/her device's address." EX1046, Abstract, ¶¶5, 13, 95-96. This confers "anonymity upon the user." *Id.*; see also ¶¶8, 12, 52. Thus, a POSITA would have been motivated to combine Nordman with Ribaudó-Watanabe-Behrens to provide additional privacy protections for device identifiers like MAC addresses. EX1002, ¶275.

A POSITA would have had a reasonable expectation of successfully implementing Nordman's pseudonym addresses because Ribaudó, Watanabe, and Behrens all describe Bluetooth communications and identifiers. EX1007, ¶¶18, 66-67, 73, 76-77, 154, 157, 181-184, 191; EX1006, ¶¶1-2, 27; EX1008, 4:21-24, 11:21-26, 18:21-28, 19:5-14, 25:22-25. Further, Behrens describes using a BD_ADDR interchangeably with a MAC address as implemented in Ribaudó. EX1008, 11:21-26, 25:22-25. Therefore, implementing Nordman's pseudonym address would have been simple because the pseudonym address functions as a BD_ADDR. EX1002, ¶276. A POSITA would thus have understood that applying Nordman's teachings would have yielded predictable results based on the

interrelated teachings of the references. *Id.*

VIII. GROUND 4: RIBAUDO-WATANABE-MGRDECHIAN RENDERS OBVIOUS CLAIM 23

Ribaudo in view of Watanabe and Mgrdechian (“Ribaudo-Watanabe-Mgrdechian”) teaches Claim 23: *application is a multiuser game*.

As explained for Claim 22, Ribaudo teaches mobile devices sending a unique identifier to the server and subsequently receiving “further information” relating to a nearby user of a common application on another device. EX1007, ¶¶120, 140.

Ribaudo aims to allow mobile device users with commonalities to interact and detect each other when in proximity (EX1007, ¶6), and mentions that “[m]obile devices 12 may include ... *game consoles*.” EX1007, ¶18. It would have been obvious that the nearby user’s “application,” for which the mobile device receives “further information,” is a multiuser game as Mgrdechian demonstrates.

Like Ribaudo and Watanabe, Mgrdechian discloses a “wireless communication system ... that provides an exchange of information between wireless devices” whose users are “previously unknown” to each other, EX1010, ¶¶2-3, where each device exchanges information with a remote server via Internet, EX1010, ¶92, and communicates with other devices via Bluetooth or Wi-Fi, based on “unique identifications” or “unique IDs” stored in a remote database. EX1010, ¶¶21, 91-92; *see also* FIG. 8; EX1002, ¶¶87-89. Mgrdechian discloses “gaming

applications operating on mobile devices.” EX1010, ¶¶45, 86.

Accordingly, it would have been obvious to use the Ribaudo-Watanabe system with Mgrdechian’s “gaming application” played by multiple nearby users, where “further information” about one device’s user (e.g., playing a particular game) is received by another mobile device. EX1002, ¶¶277-282. A POSITA would have been motivated to implement Mgrdechian’s “gaming application” scenario with Ribaudo-Watanabe, as such an application is consistent with Ribaudo’s goal of “allow[ing] mobile device users with one or more commonalities or other reasons for interacting to detect each other when they are or have been proximity,” EX1007, ¶6. A POSITA would have had a reasonable expectation of successfully implementing Mgrdechian’s gaming application with Ribaudo-Watanabe, since all three references aim to detect nearby wireless devices and establish communications over Bluetooth and Internet, and since Ribaudo contemplates that gaming applications may be used with its system, teaching that its “mobile devices” may be “game consoles.” EX1007, ¶18; EX1002, ¶¶277-282.

IX. CERTIFICATION UNDER RULE 42.104(A)

Petitioner certifies that the ’918 patent is available for IPR and Petitioner is not barred or estopped from requesting IPR of any claim.

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

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

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

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

The '918 patent is at issue in:

- *Secure Comm'n Techs., LLC v. Apple Inc.*, Case No. 1:25-cv-01579 (W.D. Tex.), filed September 30, 2025.

The '918 patent was at issue in the following proceedings, which have been terminated:

- *Secure Comm'n Techs., LLC v. Samsung Elecs. Co., Ltd.*, Case No. 2:24-cv-00484 (E.D. Tex.), filed July 3, 2024 (terminated August 14, 2025);
- *Secure Comm'n Techs., LLC v. Apple Inc.*, Case No. 2:25-cv-00763 (E.D. Tex.), filed August 4, 2025 (terminated October 3, 2025);
- *Secure Comm'n Techs., LLC v. Google LLC*, Case No. 1:25-cv-01207 (W.D. Tex.), filed August 4, 2025 (terminated June 30, 2026);
- *Samsung Elecs. Co., Ltd. v. Secure Comm'n Techs., LLC*, IPR2025-01049 (P.T.A.B.), filed May 30, 2025 (terminated pre-institution August 27, 2025); and
- *Google LLC v. Secure Comm'n Techs.*, Case No. IPR2025-01181 (P.T.A.B.), filed July 2, 2025 (institution denied December 23, 2025).

Petitioner is concurrently filing petitions for *inter partes* review of Patent Owner's U.S. Patent Nos. 11,443,344 (IPR2026-00446) and 11,687,971 (IPR2026-

00447).

The '918 patent claims the benefit of U.S. Patent Nos. 9,161,164, 8,849,698, 8,385,896, and 8,090,359. U.S. Patent Nos. 11,074,615, 11,443,344, 11,687,971, 11,995,685, and 12,430,667 and pending U.S. Patent Application Nos. 19/027,075, 19/027,020, and 19/549,933 claim the benefit of the '918 patent.

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

Lead Counsel for Petitioner is:

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

Back-up Counsel for Petitioner are:

Timothy L. Tang (Reg. No. 75,187)
STERNE, KESSLER, GOLDSTEIN & FOX PLLC
1101 K Street, NW, 10th Floor
Washington, DC 20005
202-772-8758 (telephone)
202-371-2540 (facsimile)
ttang-PTAB@sternekessler.com; and

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

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

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

XI. CONCLUSION

The Board should find all claims to be unpatentable.

Respectfully submitted,

STERNE, KESSLER, GOLDSTEIN & FOX PLLC

/Richard M. Bemben/

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

Date: August 25, 2026

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

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

1. This Petition for *Inter Partes* Review complies with the type-volume limitation of 14,000 words, comprising 13,986 words, excluding the parts exempted by 37 C.F.R. § 42.24(a)(1).

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

Respectfully submitted,

STERNE, KESSLER, GOLDSTEIN & FOX PLLC

/Richard M. Bemben/

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

Date: August 25, 2026

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

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

I certify that the above-captioned **PETITION FOR *INTER PARTES***
REVIEW FOR U.S. PATENT NO. 11,334,918 and associated Exhibits
1001-1012, 1021-1042, and 1046 were served in their entireties upon the Patent
Owner on August 25, 2026, via Fedex® Express at the following addresses:

Thomas Cecil
CECIL LAW PLLC
10300 N. Central Expressway
Suite 290
Dallas, TX 75231

Correspondence Address of Record for U.S. Patent No. 11,334,918

Timothy E. Grochocinski
C. Austin Ginnings
NELSON BUMGARDNER CONROY PC
745 McClintock Drive, Suite 340
Burr Ridge, Illinois 60527

Christopher G. Granaghan
NELSON BUMGARDNER CONROY PC.
3131 West Seventh Street, Suite 300
Fort Worth, Texas 76107

Additional Addresses Known to Petitioner as Likely to Effect Service

Respectfully submitted,

STERNE, KESSLER, GOLDSTEIN & FOX PLLC

/Richard M. Bemben/

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

Date: August 25, 2026

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