

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner

v.

SECURE COMMUNICATION TECHNOLOGIES, LLC,
Patent Owner

Case IPR2026-00446
U.S. Patent No. 11,443,344

**PETITION FOR *INTER PARTES* REVIEW
OF U.S. PATENT NO. 11,443,344**

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 '344 PATENT	2
	A. Summary	2
	B. Person of Ordinary Skill in Art (POSITA)	4
III.	CLAIM CONSTRUCTION	4
IV.	FOUNDATIONS	5
V.	GROUND 1: RIBAUDO-WATANABE RENDERS OBVIOUS CLAIMS 1, 11, 13, 15, 20, AND 30	6
	A. Ribaudó.....	6
	B. Watanabe	8
	C. Motivation to Combine	11
	D. Independent Claims 1 and 30	15
	1. 1[pre]/30[pre]	15
	2. 1[a]/30[a].....	16
	a. Receiving, at a wireless device, a first plurality of beacon transmissions via Bluetooth	16
	b. Overview of beacon transmission components	21
	c. MAC address	22
	d. Unique identifier.....	23
	e. Beacon service identifier identifies a wireless beacon service as opposed to identifying a communication network or a device accessible using Bluetooth.....	24
	3. 1[b]/30[b]	26
	a. Receiving, at the wireless device, stored information from a server	26
	b. Using a second wireless protocol different from Bluetooth.....	28
	c. Stored information relates to an entity or object associated with a first unique identifier.....	30

4.	1[c]/30[c].....	31
a.	Filtering the beacon transmissions that include a particular beacon service identifier	31
b.	Selecting one or more unique identifiers from the beacon transmissions	33
5.	1[d]/30[d]	34
E.	Dependent Claims 11, 13, 15, and 20	38
1.	Claim 11	38
2.	Claim 13	40
3.	Claim 15	40
4.	Claim 20	40
VI.	GROUND 2: RIBAUDO-WATANABE-BEHRENS RENDERS OBVIOUS CLAIMS 2-10, 12, 14, 16-19, 21-26, 28, AND 29	41
A.	Behrens	42
B.	Motivation to Combine	43
C.	Independent Claim 29	47
1.	29[pre]	47
2.	29[a]	48
3.	29[b]	50
4.	29[c]	51
5.	29[d]	53
6.	29[e]	54
7.	29[f]	54
8.	29[g]	54
9.	29[h]	54
10.	29[i]	56
11.	29[j]	57
a.	Taking second further action relating to the stored information, if a second unique identifier is present among the one or more unique identifiers selected from the second plurality of beacon transmissions	57

b.	Wherein the second unique identifier is associated with the same entity or object, and wherein the second unique identifier is not equal to the first unique identifier.....	57
c.	Received beacon transmissions including the first and second unique identifiers are received from a same transmitting device	59
12.	29[k]	60
a.	MAC address received in beacon transmission including the second unique identifier is different from MAC address received in beacon transmission including the first unique identifier	60
b.	Each beacon transmission includes the same particular beacon service identifier	61
D.	Dependent Claims 2-10, 12, 14, 16-19, 21-26, and 28	61
1.	Claim 2	61
a.	2[pre].....	61
b.	2[a]	62
c.	2[b].....	62
d.	2[c].....	62
2.	Claim 3	62
a.	Different MAC addresses received in different beacon transmissions but each beacon transmission includes the same beacon service identifier	62
b.	A plurality of beacon transmissions including the particular service identifier and the first unique identifier are received in the first time period	62
c.	No beacon transmissions including the same service identifier and the second unique identifier are received in the first time period.....	63
3.	Claim 4	63
4.	Claim 5	64
5.	Claim 6	65

6.	Claim 7.....	66
7.	Claim 8.....	67
8.	Claim 9.....	67
9.	Claim 10.....	68
10.	Claim 12.....	71
11.	Claim 14.....	72
12.	Claim 16.....	72
13.	Claim 17.....	73
14.	Claim 18.....	73
15.	Claim 19.....	74
16.	Claim 21.....	75
17.	Claim 22.....	75
18.	Claim 23.....	75
19.	Claim 24.....	77
20.	Claim 25.....	77
21.	Claim 26.....	78
22.	Claim 28.....	78
VII.	GROUND 3: RIBAUDO-WATANABE-BEHRENS-NORDMAN RENDERS OBVIOUS CLAIM 27	78
VIII.	CERTIFICATION UNDER RULE 42.104(A)	81
IX.	MANDATORY NOTICES (37 C.F.R. § 42.8(A)(1)).....	81
A.	Real Party-in-Interest (37 C.F.R. § 42.8(b)(1)):	81
B.	Related Matters (37 C.F.R. § 42.8(b)(2)).....	81
C.	Lead and Back-up Counsel (37 C.F.R. § 42.8(b)(3)).....	82
D.	Service Information (37 C.F.R. § 42.8(b)(4))	83
X.	CONCLUSION.....	83

PETITIONER'S EXHIBIT LIST

Exhibit No.	Description
1001	U.S. Patent No. 11,443,344 (“the ’344 Patent”)
1002	Declaration of Dr. Sundeep Rangan
1003	<i>Curriculum Vitae</i> of Dr. Sundeep Rangan
1004	Prosecution History of U.S. Patent No. 11,443,344
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) (“Bluetooth Specification v.2.0 + EDR”)
1022-1024	<i>Intentionally Left Blank</i>

Exhibit No.	Description
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 802.15 Specification IEEE Standard 802.15.1, Part 15.1: Wireless medium access control and physical layer (PHY) specifications for wireless personal area networks (WPANs) (June 2005) (“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”)
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”)

Exhibit No.	Description
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 method comprising:
1[a]	receiving, at a wireless device, via a short range wireless protocol, a first plurality of beacon transmissions, each beacon transmission comprising three fields (a) a MAC address, (b) a unique identifier, wherein the unique identifier of each respective beacon transmission does not directly identify a location of a beacon transmitter, and (c) a beacon service identifier, wherein the beacon service identifier of each respective beacon transmission identifies a wireless beacon service as opposed to identifying a communication network or a device accessible using the short range wireless protocol;
1[b]	receiving, at the wireless device via a second wireless protocol, stored information from one or more servers, the stored information relating to a particular entity or object associated with a first unique identifier, and wherein the second wireless protocol is different from the short range wireless protocol;
1[c]	causing selection of one or more of the unique identifiers from the first plurality of beacon transmissions, by filtering the beacon transmissions which include a particular beacon service identifier indicating that a particular received beacon transmission is associated with a particular wireless beacon service; and
1[d]	taking first further action relating to the stored information, if the first unique identifier is present among the selected one or more unique identifiers.

2[pre]	The method of claim 1, wherein the receiving, at the wireless device, via a short range wireless protocol, of the first plurality of beacon transmissions occurs in a first time period, and wherein the method further comprises,
2[a]	during a second time period: receiving, at the wireless device, via a short range wireless protocol, a second plurality of beacon transmissions, each of the second plurality of beacon transmissions comprising three fields (a) a MAC address, (b) a unique identifier, wherein the unique identifier of each respective beacon transmission does not directly identify a location of a beacon transmitter, and (c) a beacon service identifier, wherein the beacon service identifier of each respective beacon transmission identifies a wireless beacon service as opposed to identifying a communication network or a device accessible using the short range wireless protocol;
2[b]	causing selection of one or more of the unique identifiers from the second plurality of beacon transmissions, by filtering the beacon transmissions which include the same particular beacon service identifier indicating that the particular received beacon transmission is associated with the same particular wireless beacon service; and
2[c]	taking second further action relating to the stored information, if a second unique identifier is present among the one or more unique identifiers selected from the second plurality of beacon transmissions, wherein the first unique identifier and the second unique identifier is are both associated with the same particular entity or object, and wherein the second unique identifier is not equal to the first unique

	identifier, and further wherein the received beacon transmissions including the first and second unique identifiers are received from a same transmitting device.
3	The method of claim 2 wherein the MAC address received in a beacon transmission including the second unique identifier is different from the MAC address received in a beacon transmission including the first unique identifier, but each such beacon transmission includes the same beacon service identifier, and wherein a plurality of beacon transmissions including the particular service identifier and the first unique identifier are received in the first time period, and no beacon transmissions including the same service identifier and the second unique identifier are received in the first time period.
4	The method of claim 3 wherein the second further action is based upon a function currently being performed on a device associated with the wireless beacon service.
5	The method of claim 4 wherein the function is related to a current phone call, music being played, a video being played, a multi-player game, or a shared application.
6	The method of claim 2 wherein the first or the second further action is related to receiving advertising information for presentation to a user of the wireless device, based upon the first or the second unique identifiers, or information derived from the first or second unique identifier.

7	The method of claim 2 wherein the first further action includes retrieving content from a server based upon information derived from either the first unique identifier or the second unique identifier.
8	The method of claim 2, wherein the first or second further action includes sending a message to another device associated with an account related to the first and the second unique identifiers.
9	The method of claim 2 wherein following the performance of the first or second further action, a server associated with an account for a user of the wireless device performs a step of sending a message to an email address associated with the account for the user, the email relating to the same particular entity or object associated with the first or second unique identifier.
10	The method of claim 2 wherein the second further action includes preventing sending of the second unique identifier or information derived from the second unique identifier by the wireless device to at least one of the one or more servers.
11	The method of claim 1 wherein the first further action comprises: determining, based upon at least a portion of the stored information, that at least one beacon transmitter is associated with a predetermined location.
12	The method of claim 2 wherein the step of taking first further action further includes, causing the wireless device to: send the first unique identifier or information derived from the first unique identifier to at least one of the one or more servers, and receive the stored information in response.

13	The method of claim 1 wherein the stored information is received by at the wireless device from at least one of the one or more servers prior to the performing of the first further action.
14	The method of claim 2 wherein the stored information is received at the wireless device from at least one of the one or more servers prior to the performing of the first further action.
15	The method of claim 1 further comprising: using the stored information to determine if the first unique identifier is present among the first selected one or more unique identifiers.
16	The method of claim 2 wherein all beacon transmitter devices participating in the particular wireless beacon service have the same particular beacon service identifier.
17	The method of claim 2 wherein the second further action comprises: determining, based upon at least a portion of the stored information, that the beacon transmitter is associated with a predetermined location.
18	The method of claim 2 wherein one or more of the steps performed by at the wireless device are performed as a result of an application program executing on the wireless device.
19	The method of claim 2 wherein the second further action is related to either a product tied to a location or an advertisement tied to a location.
20	The method of claim 1 wherein the first further action includes determining an address or location associated with the wireless device based at least in part upon the first unique identifier being associated

	with a pre-determined location, and wherein the wireless device is located indoors where a GPS signal may not be available.
21	The method of claim 2 wherein the second further action includes determining an address or location associated with the wireless device based at least in part upon the second unique identifier being associated with a pre-determined location, wherein the wireless device is located indoors where a GPS signal may not be available.
22	The method of claim 2 wherein the second further action includes allowing a user associated with the wireless device to be provided access to an object or device associated with the wireless beacon service.
23	The method of claim 2 wherein the step of taking second further action additionally comprises: controlling further communications between the wireless device and at least one device or server associated with an entity or object in proximity to the wireless device.
24	The method of claim 3 further comprising: receiving, at the wireless device, timing notification information for coordination of active times for beacon transmissions.
25	The method of claim 24 wherein the receiving, the wireless device of the timing notification information is not directly from the beacon transmitter.
26	The method of claim 2 further comprising: using the stored information to determine if the second unique identifier is present

	among the selected one or more of the unique identifiers from the second plurality of beacon transmissions.
27	The method of claim 1 wherein the MAC address is a randomly generated 48 bit number matching a format of a Bluetooth BD_ADDR.
28	The method of claim 3 wherein the short range protocol is derived from Bluetooth.
29[pre]	A mobile wireless device comprising:
29[a]	one or more radios for providing reception and transmission for each of a Bluetooth wireless protocol and a second wireless protocol;
29[b]	one or more processors; and
29[c]	one or more memory devices coupled to the one or more processors, the one or more non- transitory 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:
29[d]	receiving from a beacon transmitter, using the Bluetooth wireless protocol, a first plurality of beacon transmissions during a first time period, each of the beacon transmissions including (a) a MAC address, (b) a unique identifier, wherein the first unique identifier does not directly identify a location of the beacon transmitter, and (c) a beacon service identifier, wherein the beacon service identifier of each respective beacon transmission identifies a wireless beacon service as opposed to identifying a communication network or a device accessible using the Bluetooth wireless protocol;

29[e]	receiving from one or more servers, using the second wireless protocol, stored information related to a entity or object associated with a first unique identifier;
29[f]	selecting one or more unique identifiers from the first plurality of beacon transmissions, by filtering the beacon transmissions which include a particular beacon service identifier indicating that a particular received beacon transmission is associated with the particular wireless beacon service;
29[g]	taking first further action relating to the stored information, if the first unique identifier is present among the selected one or more unique identifiers;
29[h]	receiving, by the wireless device, using the Bluetooth wireless protocol, during a second time period, a second plurality of beacon transmissions, each of the second plurality of beacon transmissions comprising three fields (a) a MAC address, (b) a unique identifier, wherein the unique identifier of each respective beacon transmission does not directly identify a location of a beacon transmitter, and (c) the beacon service identifier, wherein the beacon service identifier of each respective beacon transmission identifies a wireless beacon service as opposed to identifying a communication network or a device accessible using the Bluetooth wireless protocol;
29[i]	selecting one or more of the unique identifiers from the second plurality of beacon transmissions, by filtering the beacon transmissions which include the same particular beacon service identifier indicating

	that a particular received beacon transmission is associated with the same particular wireless beacon service;
29[j]	taking second further action relating to the stored information, if a second unique identifier is present among the one or more unique identifiers selected from the second plurality of beacon transmissions, wherein the second unique identifier is associated with the same entity or object, and wherein the second unique identifier is not equal to the first unique identifier, and further wherein the received beacon transmissions including the first and second unique identifiers are received from a same transmitting device; and
29[k]	wherein the MAC address received in a beacon transmission including the second unique identifier is different from the MAC address received in a beacon transmission including the first unique identifier, but each such beacon transmission includes the same particular beacon service identifier.
30[pre]	A computer program product for installation in a non-transitory medium in a wireless device, the computer program product comprising computer program instructions that, when executed by one or more processors in the wireless device, cause the wireless device to:
30[a]	process a first plurality of beacon transmissions, received at the mobile wireless device via a Bluetooth protocol, each beacon transmission comprising three fields (a) a MAC address, (b) a unique identifier, wherein the unique identifier of each respective beacon transmission

	does not directly identify a location of a beacon transmitter, and (c) a beacon service identifier, wherein the beacon service identifier of each respective beacon transmission identifies a wireless beacon service as opposed to identifying a communication network or a device accessible using the Bluetooth wireless protocol;
30[b]	process stored information transferred from one or more servers to the mobile wireless device via a second wireless protocol, wherein the stored information relates to an entity or object associated with a first unique identifier, and wherein the second wireless protocol is different from the Bluetooth wireless protocol;
30[c]	select one or more of the unique identifiers from the first plurality of beacon transmissions, by filtering the beacon transmissions which include a particular beacon service identifier indicating that a particular received beacon transmission is associated with the a particular wireless beacon service; and
30[d]	perform a further action, the further action relating to the stored information, if the first unique identifier is present among the selected one or more unique identifiers.

I. INTRODUCTION

Apple Inc. petitions for *inter partes* review of claims 1-30 of U.S. Patent No. 11,443,344 (“the ’344 patent”).

The ’344 patent describes a mobile device that facilitates short-range communications between devices (e.g., via Bluetooth or Wi-Fi) and long-range communications with a server (e.g., via a cellular network). The claims recite the mobile device detecting “beacon transmissions” that include a MAC address, a unique identifier, and a beacon service identifier and filtering the beacon transmissions based on the beacon service identifier. For example, the mobile device may detect a beacon transmission from a museum exhibit (short-range) and subsequently retrieve content related to that exhibit from a server (long-range).

But before the ’344 patent, using an identifier to signal short- and long-range communication capabilities was already well known. For example, Ribaudó in combination with Watanabe teaches such identifiers and filtering beacon transmissions that include these identifiers. In view of Ribaudó’s and Watanabe’s teachings, independent claims 1 and 30 are unpatentable. Independent claim 29 and other dependent claims are similarly unpatentable in view of Ribaudó, Watanabe, Behrens, and Nordman. Thus, Petitioner respectfully requests that the Board institute trial and determine that all claims of the ’344 patent are unpatentable.

II. THE '344 PATENT

A. Summary

The '344 patent relates to techniques for mobile wireless devices (e.g., cellular phones) in proximity with one another to exchange information utilizing both a short range, first wireless capability and a second wireless capability that allows the devices “to communicate with a central server via the internet.” EX1001, 1:49-63. The '344 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, 1:11-36. The '344 patent proposes utilizing these two wireless capabilities to broker the exchange of information between two wireless devices. EX1001, 1:51-63.

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 respectively” (green), via a combination of the Internet and a cellular network. EX1001, 3:44-55, FIG. 1. The devices are also able to communicate directly with

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

each other via “a short range wireless link 107” (yellow). EX1001, 4:36-47.

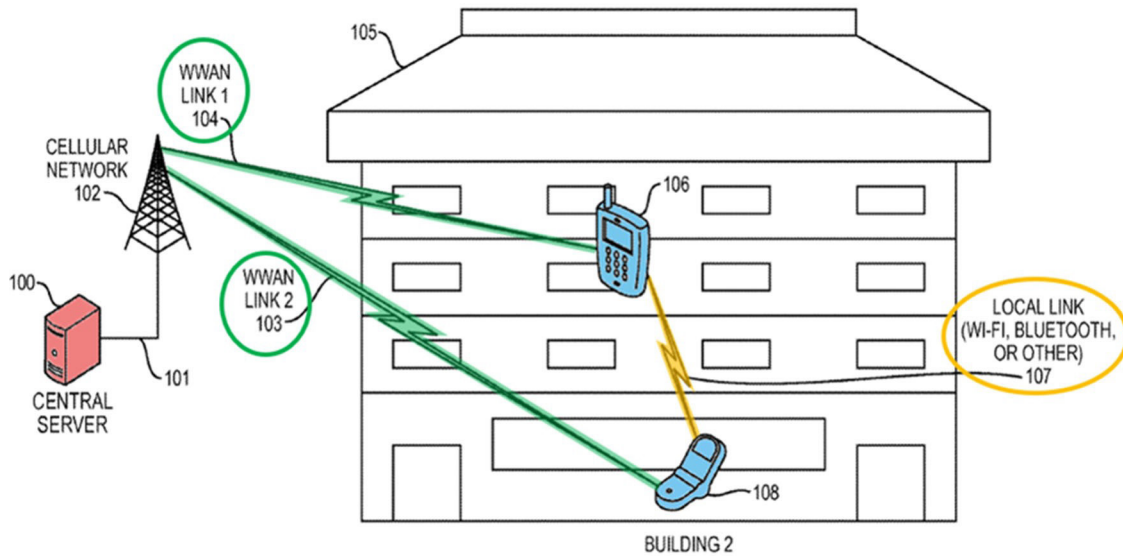


Figure 1

EX1001, FIG. 1 (annotated).

The '344 patent uses the concept of “beacon service” transmissions to facilitate communications between nearby devices over the short-range link first, before establishing communications using a cellular link. EX1001, Abstract, 1:49-67. As shown in Figure 6, the 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, 8:25-38, FIG. 6 (annotated); EX1002, ¶¶64-70. While Figure 6 provides an example of multiple identifiers, the '344 patent does not explicitly define the claim terms *beacon service identifier* or *unique identifier*.

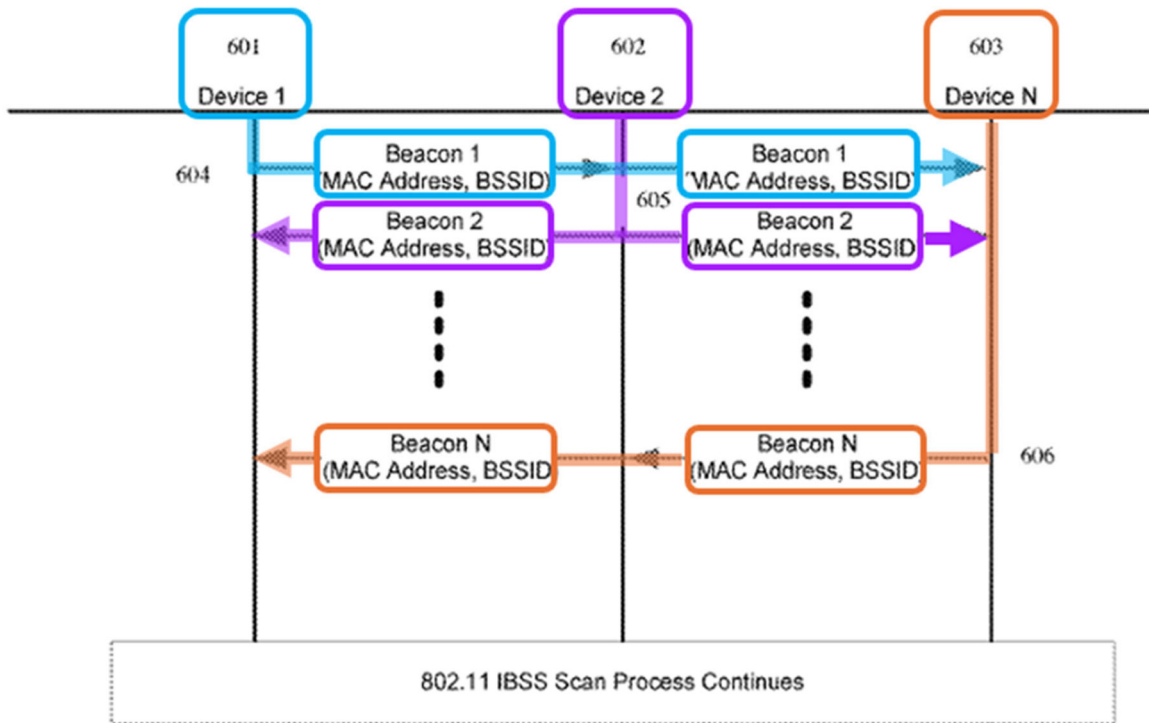


Figure 6 - 802.11 IBSS Beacon Process

EX1001, FIG. 6 (annotated).

B. 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, 11, 13, 15, 20, 30	Ribaud-Watanabe
2	2-10, 12, 14, 16-19, 21-26, 28-29	Ribaud-Watanabe-Behrens
3	27	Ribaud-Watanabe-Behrens-Nordman

Each reference is prior art:

- U.S. Patent Publication No. 2007/0030824 (“Ribaud”) 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 to the ’344 patent 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).

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 ’344 patent, is reasonably pertinent to the problems (e.g., detecting wireless devices in close proximity to exchange information) of the ’344 patent, or both. EX1002, ¶¶28, 72.

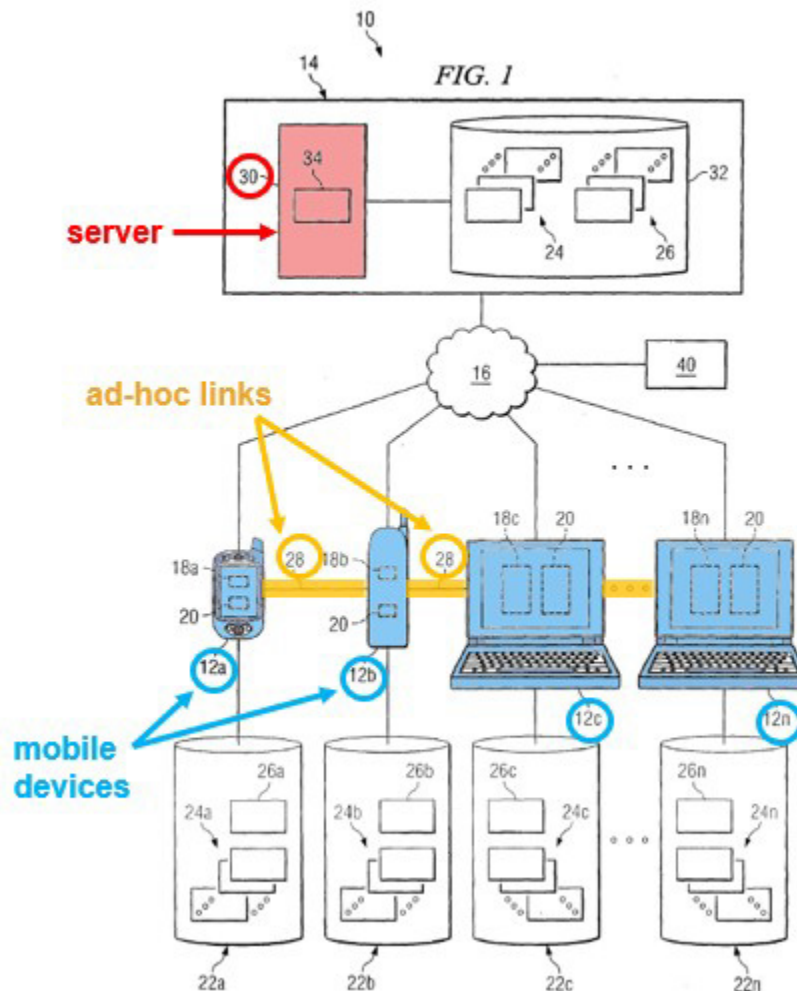
V. GROUND 1: RIBAUDO-WATANABE RENDERS OBVIOUS CLAIMS 1, 11, 13, 15, 20, AND 30

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. Ribaudó teaches “providing communication services to mobile device users incorporating proximity determination.” EX1007, ¶¶2, 8; EX1002, ¶¶73-76. Specifically, “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.

Ribaudo’s system, illustrated in Figure 1 below, “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).

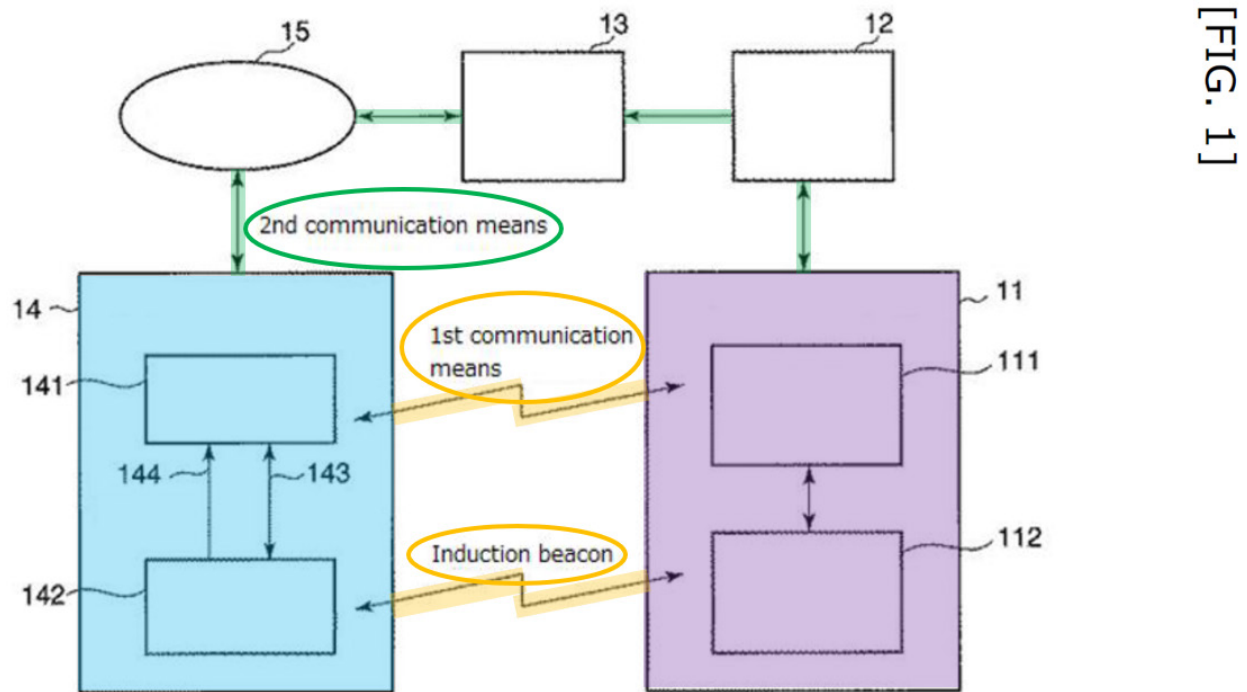
As Ribaudo explains, “a user (e.g., of mobile device 12a) may be associated

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. In operation, 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. Watanabe teaches a system that “reduce[s] power consumption when a mobile terminal is not communicating data with an access point.” EX1006, ¶7, Abstract; EX1002, ¶¶77-80. 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 (annotated below). “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.

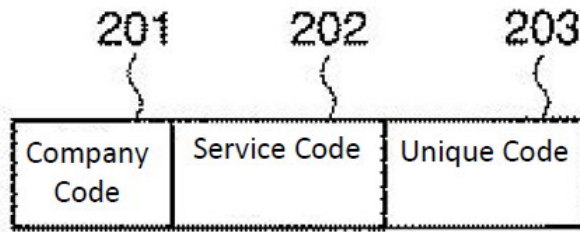


EX1006, FIG. 1 (annotated).

“[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.

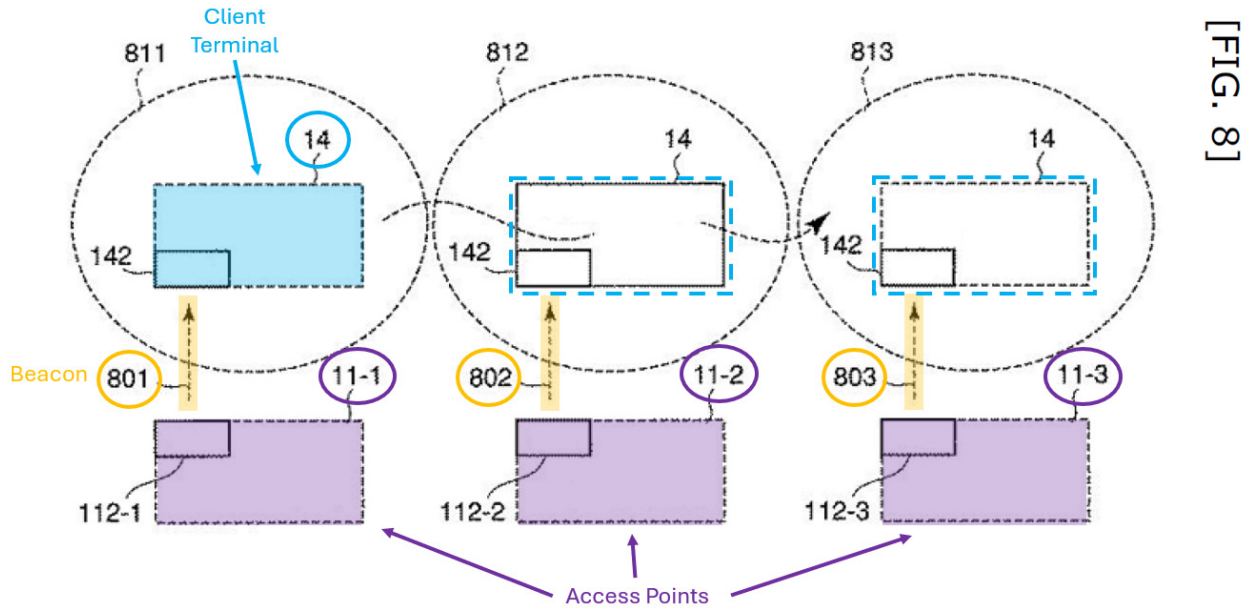
[FIG. 2]



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 (below), 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.



EX1006, FIG. 8 (annotated).

C. Motivation to Combine

A POSITA would have been motivated to combine the teachings of Ribaud and Watanabe to enhance Ribaud’s beacon transmission processing and filtering capabilities. EX1002, ¶¶85-88. A POSITA would have also had a reasonable expectation of success in combining Ribaud and Watanabe because each relates to detecting nearby wireless devices via beacon transmissions and establishing communications using ad-hoc (e.g., Bluetooth) and cellular networks. EX1006, Abstract, ¶27; EX1007, Abstract, ¶18; EX1002, ¶¶89-92.

Ribaud describes a beacon service identifier in the form of an SSID. In Ribaud, 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). *See, e.g.*, EX1007, ¶¶97-104, 138 (discussing “dating” related services). Ribauda 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 (describing additional implementation contexts). “Once a desirable SSID is detected... the two mobile devices 12a and 12b may establish a connection on the same network.” EX1007, ¶71. Ribauda therefore describes filtering beacon transmissions based on a particular beacon service identifier.

Thus, Ribauda 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, ¶87. 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 services corresponding to the service code. EX1006, ¶¶41-42, 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, ¶¶41-42, 48-51.

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 further enhance Ribaud’s processing of beacon transmissions and filtering capabilities. Ribaud specifically contemplates this combination. EX1002, ¶88; 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 Ribaud, would identify beacon transmissions corresponding to a “dating” service, which would allow receiving mobile devices to more efficiently filter beacon transmissions based on desired services as described in both Watanabe and Ribaud. EX1002, ¶88. Thus, a POSITA would have been motivated to combine Ribaud and Watanabe to further enhance Ribaud’s

processing of beacon transmissions.

A POSITA would have had a reasonable expectation of success in combining the teachings of Watanabe and Ribaud. EX1002, ¶¶89-91. Both describe mobile devices that receive beacon transmissions comprising identification information associated with a transmitting device, receiving information relating to an entity associated with the identification information from a server using the Internet, comparing the beacons identification information to preset identification information stored at the mobile device to identify matches, and taking further action relating to matching stored information. EX1006, ¶¶46-57; EX1007, ¶¶6-7. Further, Ribaud 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, ¶¶89-92. Implementing Watanabe’s service code and filtering techniques based on that service code would have amounted to combining prior art elements according to known methods to yield predictable results. *Id.* At bottom, Ribaud teaches the system and

functionality for sending and receiving beacon transmissions that include identifiers, and Watanabe describes certain information (a specific identifier) that would have been obvious and within the skill of a POSITA to include in Ribaudó's beacon transmissions. *Id.*

D. Independent Claims 1 and 30²

1. 1[pre]/30[pre]

Ribaudó in view of Watanabe (“Ribaudó-Watanabe”) teaches³ the preamble. EX1002, ¶¶93-94. Both teach wireless devices configured to communicate with other devices in proximity. Ribaudó teaches mobile devices 12 that “each have an associated memory module 22,” which includes “any suitable memory, database, or other data storage arrangement” (EX1007, ¶32), wherein “each include any suitable combination of hardware, software, and firmware to provide the

² Independent claims 1 and 29-30 contain substantially similar limitations with claim 29 adding additional limitations, as discussed in Ground 2.

Substantially similar claim elements are discussed together in the below element-by-element analysis.

³ Petitioner uses the term “teaches” to include 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 (C.C.P.A., 1981).

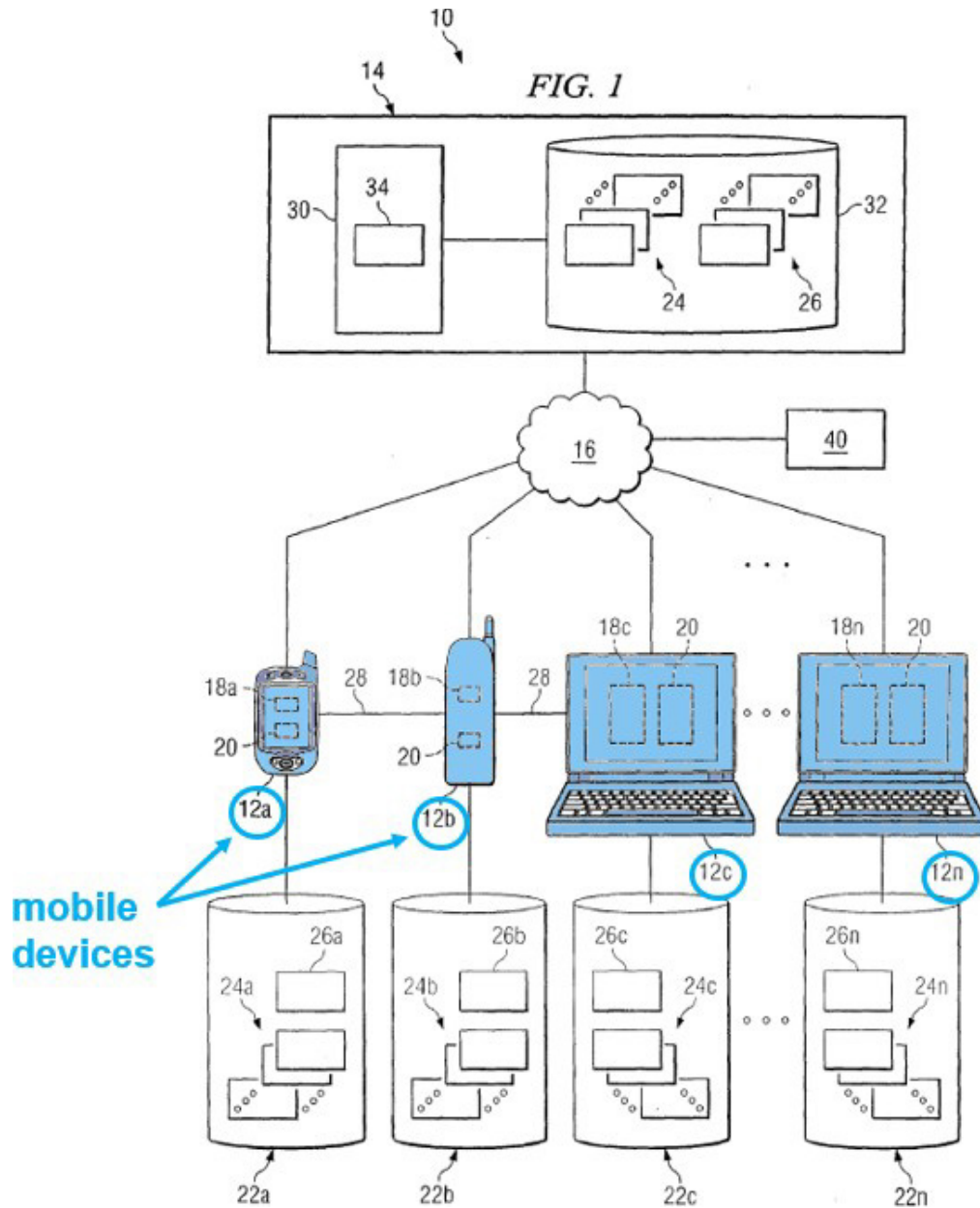
functionality described” including “one or more applications 20 that are based on one or more programming languages” to “facilitate communication with other mobile devices 12” and the data center. EX1007, ¶19. This includes “magnetic media, optical media,” and “read-only memory (ROM).” EX1007, ¶32. This teaches non-volatile memory so that software or firmware program instructions are not lost when the device loses power. EX1002, ¶¶93-94.

2. 1[a]/30[a]

Ribaudo-Watanabe teaches Elements 1[a]/30[a]. EX1002, ¶¶95-115.

a. Receiving, at a wireless device, a first plurality of beacon transmissions via Bluetooth

Ribaudo teaches mobile devices (*wireless device*) configured to receive beacon transmissions via a short-range protocol, such as Wi-Fi or Bluetooth. Figure 1 of Ribaudo 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* ¶15, FIG. 1.

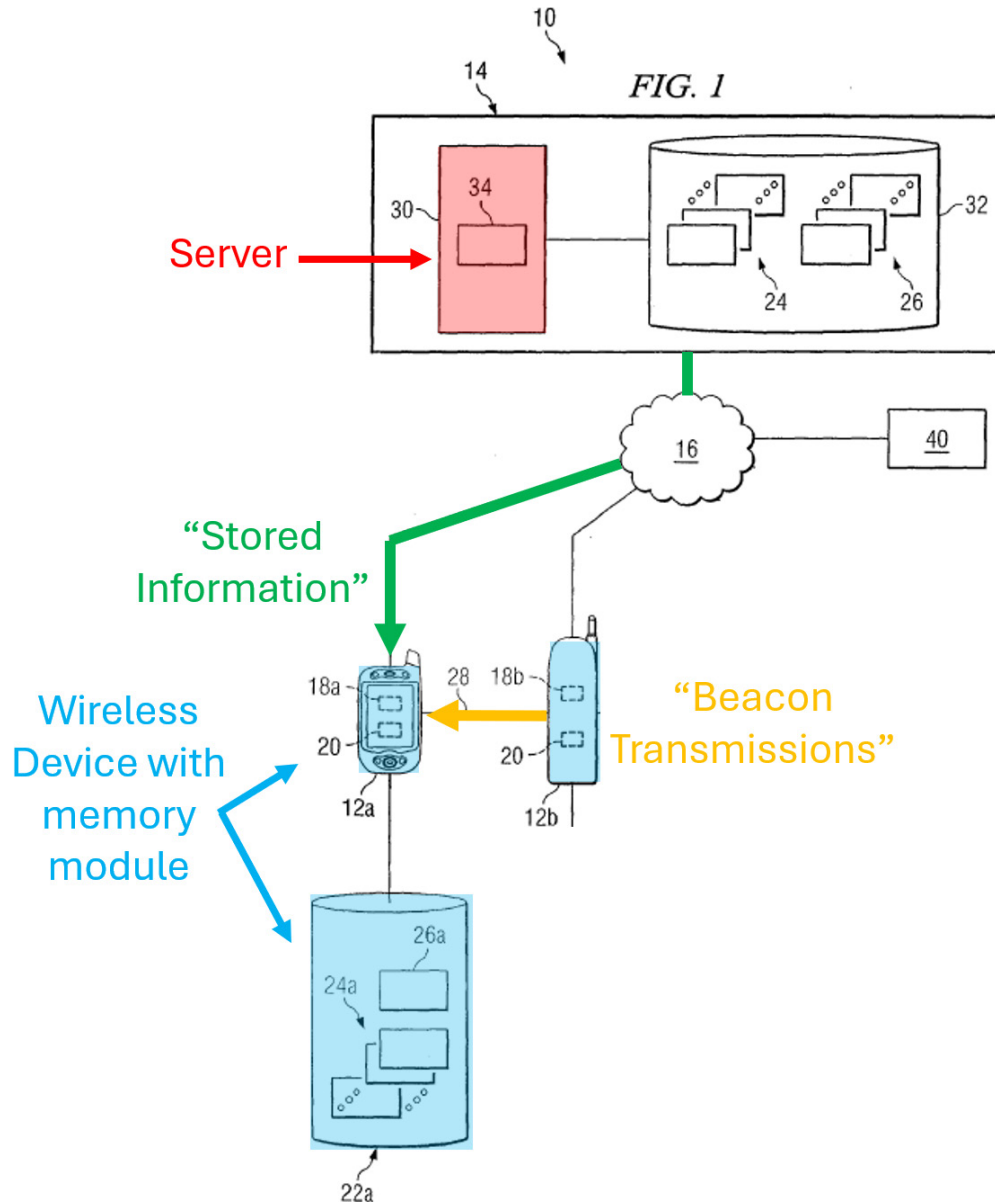


EX1007, FIG. 1 (annotated).

“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 (discussing NIC), 205, FIG. 1.

Ribaudo’s mobile devices receive a plurality of 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, 12b may be an “other mobile device[]” in the detection range. The Bluetooth radio of mobile device 12a receives beacon transmissions from mobile device 12b, and such beaconing is performed using short-range transmissions. “In Fig. 1, links 28” (below, yellow) “illustrate example ad-hoc connections between mobile devices 12,” in which “*Wi-Fi technology* may be utilized 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 also* ¶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/WWAN transmissions. EX1002, ¶99.

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, ¶100. 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, which teaches that John’s device *receives a plurality of* short-range, proximity beacon transmissions. EX1002, ¶101.

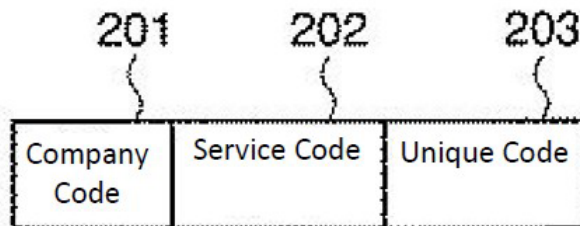
b. Overview of beacon transmission components

As shown below, the Ribaud-Watanabe combination further teaches that each of the plurality of beacon transmissions include a MAC address, a unique identifier that does not directly identify a location of a beacon transmitter, and a beacon service identifier that identifies a wireless beacon service as opposed to a communication network or a device, as follows:

Claim Element	Ribaud-Watanabe
“MAC address”	Ribaud’s MAC address of transmitting device
“unique identifier”	Ribaud’s client ID and potentially other suitable information for uniquely identifying a user or entity (e.g., Watanabe’s company code)
“beacon service identifier”	Watanabe’s service code

Additionally, the Ribaud-Watanabe combination teaches each beacon transmission including these three elements. EX1002, ¶¶102-105. For example, Watanabe teaches a beacon transmission including multiple identifiers. EX1006, FIG. 2, ¶¶14-15, 33, 49, 63.

[FIG. 2]



EX1006, FIG. 2.

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 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 (i.e., a company rather than a device)—is therefore similar to Ribaudó’s client ID and the claimed “unique identifier,” which also 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 “beacon service identifier.” EX1006, ¶15; EX1002, ¶104. In this manner, Ribaudó in view of Watanabe renders obvious a beacon transmission including each of the claimed identifiers. EX1002, ¶104.

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 more efficient processing and filtering of received beacon transmissions. Section V.C.

c. MAC address

As Ribaudó explains, “[t]he adaptor 18 of a mobile device 12 that includes

an NDIS-compliant and IEEE 802.11-compliant NIC 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** associated with the NIC, an IP address, a cell tower ID.”), ¶¶27, 68-69. Ribauda 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 understand Ribauda as teaching that each of the other mobile devices (12b, 12c, etc.), may likewise beacon its unique MAC address. EX1002, ¶106.

d. Unique identifier

Ribauda 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 (same). Ribauda 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 information⁴ included in Ribaudó’s beacons that uniquely identifies a user is thus a “*unique identifier*.” EX1002, ¶¶107-108. Because the client ID identifies a user, the client ID also *does not directly identify a location of a beacon transmitter* as recited in the claims. *C.f.* EX1007, ¶¶78, 117, 213 (Ribaudó using MAC addresses or SSIDs to identify locations); EX1002, ¶¶107-108.

e. Beacon service identifier identifies a wireless beacon service as opposed to identifying a communication network or a device accessible using Bluetooth

The term “*beacon service identifier*” is not a term of art and is not defined in the specification but encompasses an identifier of a service using beacons based on the plain language of the term. EX1002, ¶109. The Ribaudó-Watanabe combination teaches a *beacon service identifier*. Specifically, Watanabe discloses the transmission of beacons containing a plurality of fields, including a “*service code 202* indicating the type of service that can be provided” via that device. *See* EX1006, ¶15. Such a service code 202 teaches the claimed “*beacon service*

⁴ An example of other suitable information may include Watanabe’s company code. EX1006, ¶15; EX1002, ¶108.

identifier” because it identifies a type of service available via the beacon transmitter device as opposed to identifying a communication network or a device accessible using Bluetooth. EX1002, ¶109; 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., a user matching or dating service that provides matches to users within a given area—as described in Ribaudó. EX1007, ¶¶97-104, 123; EX1006, ¶15; EX1002, ¶110. 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 or dating service). EX1002, ¶110.

A POSITA would have been motivated to beacon a service code together with Ribaudó’s MAC addresses and client IDs to filter beacon transmissions based on service codes (i.e., services the user is interested in). EX1002, ¶111. For example, as further described with reference to claim elements 1[c]/30[c], including a service code would allow mobile devices receiving beacon transmissions to more efficiently filter beacon transmissions as described in both Watanabe and Ribaudó. EX1002, ¶111; Sections V.C, V.D.4. 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, ¶112.

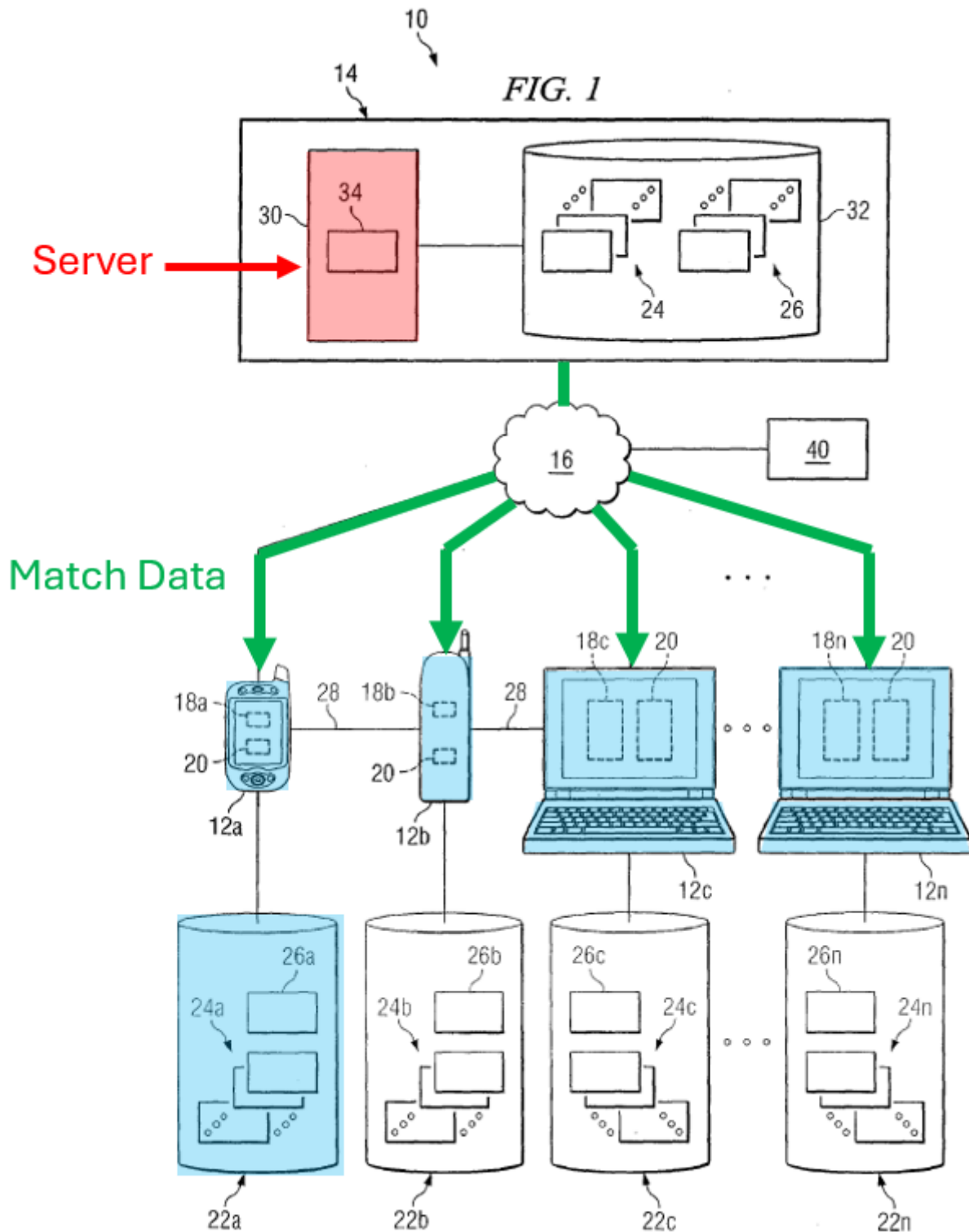
A POSITA would have had a reasonable expectation of success in applying Watanabe's teachings to Ribaudó. EX1002, ¶113; Section V.C. Both describe receiving beacon transmissions comprising identification information from a nearby device, via Bluetooth, receiving preset identification information relating 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, ¶¶113-115.

3. 1[b]/30[b]

Ribaudó-Watanabe teaches Elements 1[b]/30[b]. EX1002, ¶¶116-124.

a. Receiving, at the wireless device, stored information from a server

Ribaudó's "[d]ata center 14 includes a server system 30" (red) as shown in Figure 1. EX1007, ¶34, FIG. 1.



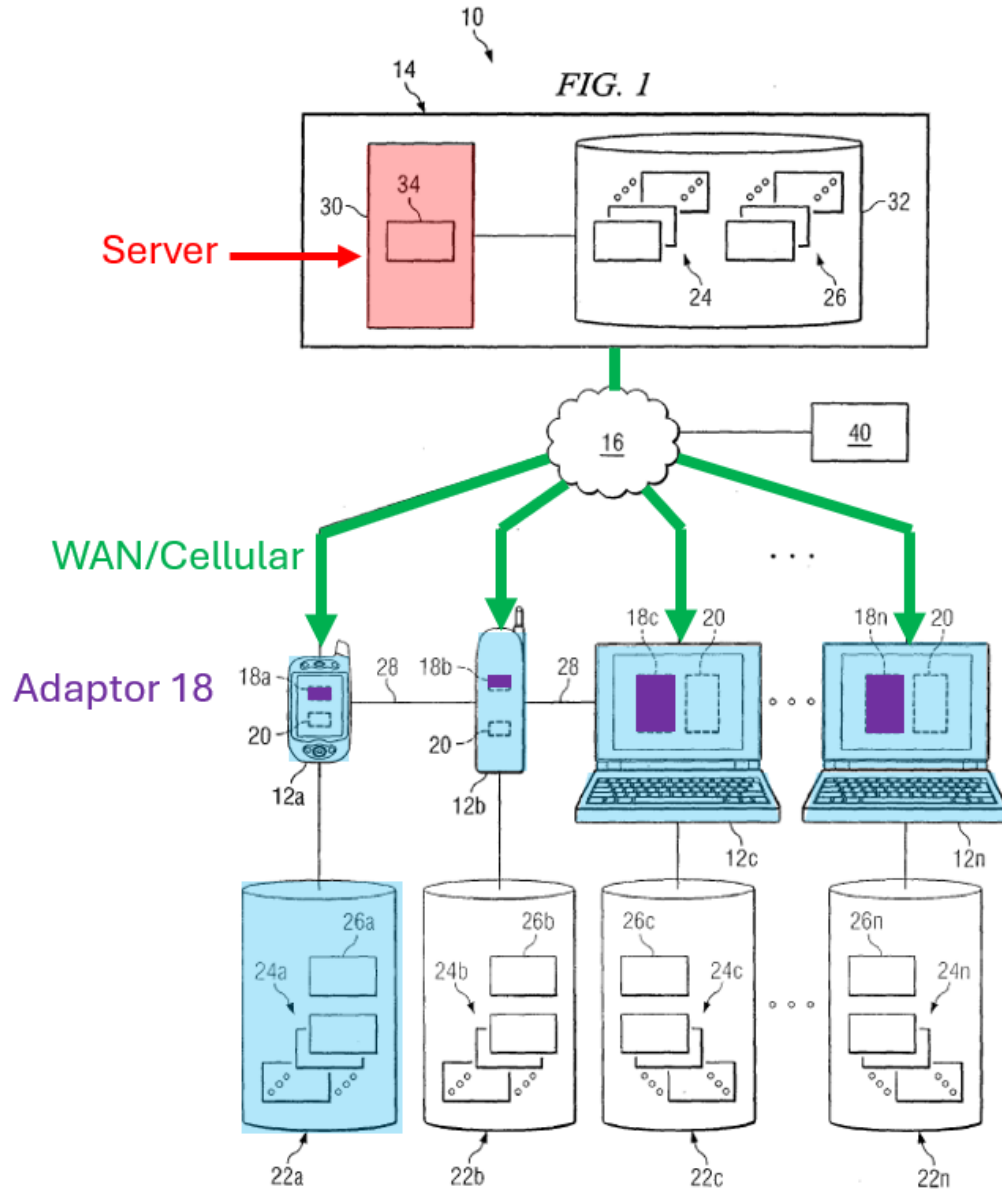
EX1007, FIG. 1 (annotated).

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." EX1007, ¶¶16, 33 ("memory module 22 may store match data 26"); *see also* ¶¶53, 204-205 (also describing proximity detection before downloading match data from the server). Ribaudó's match data is stored at the data center prior to transmission by server system 30 to a mobile device. EX1007, ¶¶26, 34, 53, 82-83. Ribaudó's match data therefore teaches the claimed *stored information from one or more servers* being transmitted and received at a wireless device as claimed. EX1002, ¶¶117-118.

b. Using a second wireless protocol different from Bluetooth

Ribaudó teaches a mobile device receiving match data via a *second wireless protocol* that is *different from the short range wireless protocol*. For example, Ribaudó describes this transmission and reception occurring via a WAN or cellular protocol. EX1007, ¶24.



EX1007, FIG. 1 (annotated).

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 also “employ[] a *cellular* connection ... to download from data center 14.” EX1007, ¶204. In this manner, Ribaudó describes receiving the stored information using adaptor 18a’s cellular/WWAN radio protocol, which is different from a short-range or Bluetooth protocol. EX1002, ¶¶119-121.

c. Stored information relates to an entity or object associated with a first unique identifier

Ribaudó’s match data also teaches the claimed *stored information relating to a particular entity or object associated with a first unique identifier*. Ribaudó’s match data includes match IDs and client IDs that identify an entity such as a user. EX1007, ¶¶16, 40, 46, 53, 57, 82-85; *see also* ¶6 (“match data contain[s] match identifiers and other information for the other users determined to be matches for the user.”), ¶¶49-51 (example of match data and a match ID including a “client ID”), ¶52 (“Each user may receive the other user’s hash value from data center 14 as a part of the match data 26 downloaded to the user’s mobile device 12.”). “This pre-processed match data for the user is stored locally on the user’s mobile device.” EX1007, ¶6. Then, when in proximity with another user, the user’s mobile

device “compares the received identifier with the pre-processed match data ... to determine whether the other user is one of the user’s predetermined matches.” *Id.*

Ribaudo explains that “***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.*** ... Mobile device 12 may ***beacon data such as the client ID of the user associated with mobile device 12.***” EX1007, ¶57; *see also* ¶¶123, 157, 173 (further describing beaconing by mobile devices 12). The match data relates to “commonalities or other reasons for interacting” between two users of a given internet service (e.g., online dating) and therefore relates to a particular *entity* associated with a *unique identifier*. *See* EX1007, ¶¶29, 97-105; *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”), 204-205, 221-223; EX1002, ¶¶122-124.

4. 1[c]/30[c]

Ribaudo-Watanabe teaches Elements 1[c]/30[c]. EX1002, ¶¶125-136.

a. Filtering the beacon transmissions that include a particular beacon service identifier

The Ribaudo-Watanabe combination teaches filtering beacon transmissions that include a particular beacon service identifier. Watanabe’s “filtering identification information notification unit 13 selects and combines the proper

codes to generate filtering identification information for the client terminal 14.”

EX1006, ¶41. Watanabe describes filtering beacon transmissions based on “service codes” corresponding to a particular service. EX1006, ¶¶41, 48-49.

For example, Watanabe describes filtering beacon transmissions based on 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, ¶¶126-129. For example, 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 a “filter” code). Watanabe therefore teaches filtering beacon transmissions using a service code corresponding to a particular type of service. EX1002, ¶128.

In view of Ribaudó’s filtering teachings (e.g., based on work or recreation) (EX1007, ¶¶29, 55, 58, 61, 64, 71, 97-104, 123, 162, 223, 226), a POSITA would have found it obvious and would have been motivated to implement and beacon Watanabe’s service code together with beaconing a MAC address, client ID, and/or SSID in Ribaudó’s system to further enhance Ribaudó’s processing of beacon transmissions and filtering capabilities. EX1002, ¶¶129-132. A POSITA would have included a service code corresponding to the type of match data beaconed in Ribaudó. EX1007, ¶90 (describing “nine categories” of matching including

“dating” and “employment”); *see also* ¶¶55, 97-104, 223. Including such a service code would distinguish between different types of match data. For example, the service code would identify beacon transmissions corresponding to a “dating” service, which would allow receiving mobile devices to more efficiently filter beacon transmissions described in both Watanabe and Ribaudó. EX1002, ¶132. Thus, the Ribaudó-Watanabe combination teaches the claimed “*filtering*” based on particular beacon service identifiers.

b. Selecting one or more unique identifiers from the beacon transmissions

In addition to filtering beacon transmissions based on beacon service identifiers, the Ribaudó-Watanabe combination also teaches selecting one or more unique identifiers based on this filtering. As previously explained, Ribaudó selects a unique identifier (e.g., “client ID”) when extracting the client ID from a received beacon transmission to compare the client ID “with the pre-processed match data stored on the user’s mobile device” to determine matches. EX1007, ¶¶6, 45-46, 65-68, 84-85; *see also* cl. 9. “[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.” EX1007, ¶85. Ribaudó therefore teaches selecting one or more unique identifiers from beacon transmissions when identifying a received client ID to compare with stored match data as explained for 1[b]-

1[c]/30[b]-30[c].

In Ribaud-Watanabe, this selection would have occurred in response to filtering beacon transmissions based on a particular beacon service identifier. Section V.D.4.a (1[c]/30[c]). For example, this filtering may be performed based on Watanabe's service code as implemented with Ribaud to identify a particular service (e.g., work or dating). EX1002, ¶¶133-136. Performing this filtering based on a service identification would allow receiving mobile devices to more efficiently process beacon transmissions (as described in both Watanabe and Ribaud) and perform a unique identifier comparison only for beacon transmissions corresponding to a particular service (e.g., work or dating). *Id.*

5. 1[d]/30[d]

Ribaud-Watanabe teaches Elements 1[d]/30[d]. In view of the broad and generic claim term “*first further action*,”⁵ Ribaud teaches performing a first further action relating to the stored information, if the first unique identifier is present among the selected one or more unique identifiers. EX1002, ¶137.

For example, Ribaud teaches determining that a first unique identifier is present among the selected one or more unique identifiers when matching detected

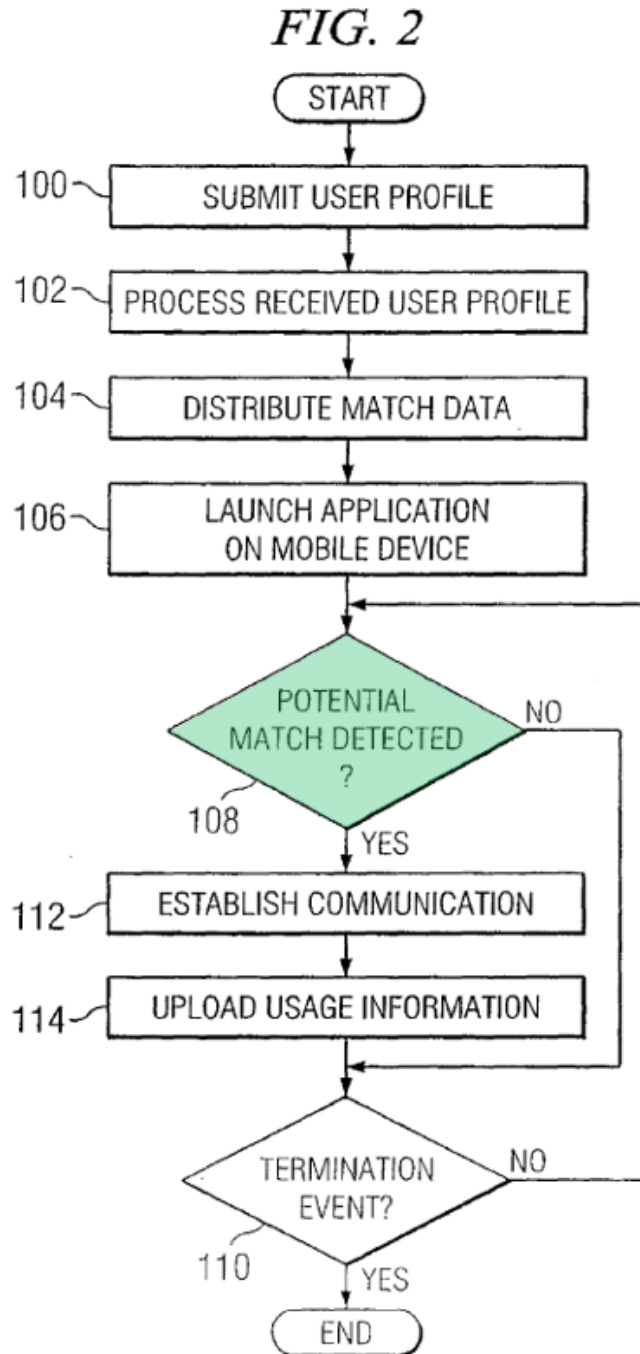
⁵ Dependent claims 7, 11-12, 20 additionally describe examples of “first further actions” and are further addressed below.

client IDs and previously stored match data. EX1002, ¶¶138-139. 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]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; *see also* ¶¶80-83.



EX1007, FIG. 2 (annotated).

Then:

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, on the basis of pre-processed match data and identifiers received from the data center ("*first unique identifier*") and the user's client ID (the "one or more unique identifiers") detected from the beacon transmissions. EX1002, ¶140. This proximity determination is an example *first further action*.

As seen from Ribaudó's Figure 2, Ribaudó describes additional examples of a *first further action* that may occur in response to this determination. EX1002, ¶¶141-143. For example, at step 112, if a match is detected "communication between matched users of mobile devices 12 may be established." EX1007, ¶87. Similarly, "if a match is determined, then mobile device 12a may notify its associated user of the match." EX1007, ¶87. Additionally, "usage information may be uploaded to data center 14." EX1007, ¶87. Ribaudó also teaches retrieving

content from a server as well as displaying a match value on a mobile device (e.g., displaying that both users have a “Harvard” match). EX1007, ¶¶17, 47, 78, 134.

Thus, Ribaudo describes several *first further action* examples that may occur related to the match data (i.e., “*stored information*”) in response to detecting that a *first unique identifier* is present among *one or more unique identifiers* detected from the beacon transmissions. EX1002, ¶¶141-143.

E. Dependent Claims 11, 13, 15, and 20

1. Claim 11

Ribaudo-Watanabe teaches claim 11. EX1002, ¶¶144-149.

Ribaudo teaches “location” tag information that can associate detected matches with particular locations. EX1007, ¶¶117, 160-161, 166, 185-186, 202, 213, 216. For example, “a user may tag particular locations based on hardware signatures such as network identifiers ... particular locations can be tagged with useful information by users of mobile devices 12.” EX1007, ¶117. Users can edit this tag information to “include more useful information about the location, such as ‘CES-ConferenceRoom4,’ ‘MainStreetCafe,’ ‘DFWAirport-Terminal3,’ or other suitable keywords.” EX1007, ¶117. Using this location tag information, mobile devices detecting matches (*based upon at least a portion of the stored information*) can associate a detected matching mobile device with the predetermined tagged location: “tagged information for a location may be shared with other users who

use the location to *provide context for the other users' detected matches at the location.*” EX1007, ¶117. Thus, Ribaudó’s correlation of a detected mobile device and a user match with a location tag teaches *determining that a beacon transmitter is associated with a predetermined location.* EX1002, ¶145.

Additionally, Ribaudó describes matching users attending an event at a “particular location and/or time.” EX1007, ¶160. For example, “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. Ribaudó describes example locations like “a coffee shop, an airport, a university, a wedding, or any other suitable gathering of users that is known or scheduled in advance.” EX1007, ¶160. Users at these locations may detect and communicate with one another and “locate each other at the event” based on proximity. EX1007, ¶161.

Additionally, Ribaudó describes detecting mobile devices at “specific locations based on the wireless access points associated with those locations.” EX1007, ¶216. Using a MAC address corresponding to such an access point allows mobile devices to view users “currently near that MAC address” and “see which other users are at the location associated with the MAC address.” EX1007, ¶¶186, 202.

Thus, Ribaudó’s location-based match detection and user detection also teach claim 11. EX1002, ¶¶144-149.

2. Claim 13

Ribaudo-Watanabe teaches claim 13. The explanation provided for claim 1 accounts for Ribaudo-Watanabe teaching the stored information being received *prior to* performing the first further action. Sections V.D.3-V.D.5 (1[b]/30[b]-1[d]/30[d]); *see e.g.*, EX1007, ¶¶6, 16, 80-85, 87, FIG. 2; EX1002 ¶150.

3. Claim 15

Ribaudo-Watanabe teaches claim 15. As explained for 1[b]/30[b]-1[d]/30[d], Ribaudo teaches determining if a first unique identifier is present among the first selected one or more unique identifiers when comparing a received client ID with client IDs from downloaded match data. *See* Sections V.D.3-V.D.5 (1[b]/30[b]-1[d]/30[d]); EX1007, ¶¶6, 16, 33, 83-85; EX1002, ¶151.

4. Claim 20

Ribaudo-Watanabe teaches claim 20. EX1002, ¶¶152-154.

As described for claim 11, Ribaudo teaches a mobile device associating location tag information with a detected match. Section V.E.1; EX1007, ¶¶117, 160-161, 166, 185-186, 202, 213, 216. When associating a location tag with a detected match—e.g., “to provide context for ... detected matches at the location”—Ribaudo also determines a location associated with the detecting wireless device. EX1007, ¶117. For example, when a wireless device uses match data to detect a match in proximity that corresponds to a location like “CES-ConferenceRoom4,” “MainStreetCafe,” or “DFWAirport-Terminal3,” the wireless

device has also determined its own location. EX1007, ¶117. Thus, the wireless device determines an associated location based on matches and corresponding location tags. EX1002, ¶153.

Ribaudo also teaches the wireless device being *located indoors where a GPS signal may not be available*. Ribaudo describes several indoor locations where matching and location determination may occur: “a hotel, coffee shop, airport” or “ConferenceRoom.” EX1007, ¶¶117, 231. Additionally, Ribaudo explains that its proximity and location detection may occur without needing to rely on GPS signals. EX1007, ¶¶185, 228 (detecting “matched users based on their proximity to one another rather than using triangulation or GPS data”); EX1002 ¶154.

VI. GROUND 2: RIBAUDO-WATANABE-BEHRENS RENDERS OBVIOUS CLAIMS 2-10, 12, 14, 16-19, 21-26, 28, AND 29

Independent claim 29 takes the limitations of independent claims 1 and 30 and recites them twice. Specifically, claim 29 recites the same first plurality of beacon transmissions as claims 1 and 30 and adds a second plurality of beacon transmissions (29[h]) that have unique identifiers and MAC addresses different from those in the first plurality of beacon transmissions but are received from the same transmitting device and have the same beacon service identifier (29[i]-29[j]).

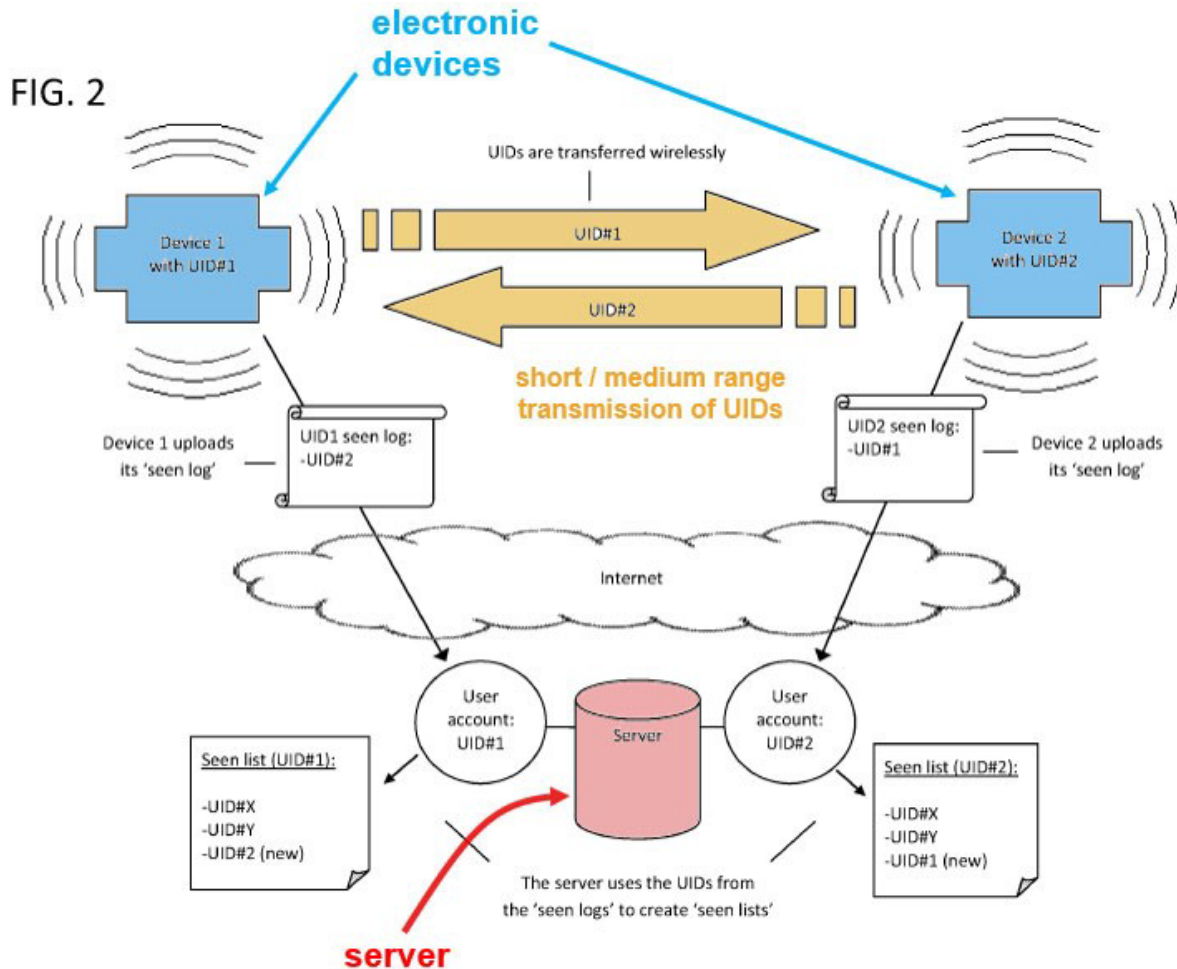
Claim 29 thus recites a system with a beacon transmitter that is like that of claims 1 and 30 in a first time period, but during a second time period, the beacon transmitter transmits the same service identifier with a different unique identifier

and a different MAC address. The '344 patent does not explain why the beacon transmitter would behave this way, but the prior art demonstrates why such a configuration would have been obvious. EX1002, ¶¶155-156.

A. Behrens

Behrens teaches portable electronic devices 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, ¶¶81-82. The UID “contains information for identifying the device (and thus its user).” EX1008, 6:6-8. Specifically, 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 also teaches a user having “multiple or changing UIDs and, therefore, different online identities.” EX1008, 23:2-5.

Figure 2 shows mobile 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, 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, 61-62, 68; EX1002, ¶¶157-161. 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 supra* Sections V.C-V.D; EX1002, ¶¶162-165.

As explained for Ground 1, Ribaud and Watanabe teach a mobile device receiving a plurality of proximity beacon transmissions, each including a MAC address, unique identifier, and beacon service identifier. EX1002, ¶158.

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. 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.” 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, ¶159.

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 the client ID may “shield” or “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).” *Id.* 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.*; EX1002, ¶160.

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* (e.g., MAC addresses or other unique IDs) may be associated with the same transmitting device. EX1002, ¶161. Combining Behrens’ teachings would have provided a mechanism for Ribaudo 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, for example, “create a new online identity for an event or party he attends or has attended.” EX1008, 23:2-4. This would enable a user or mobile device to associate multiple unique identifiers with the same entity/object (*i.e.*, the same mobile device user) to facilitate Ribaudo’s teaching of using multiple client IDs. EX1007, ¶¶45-46, 61-62, 68; EX1002, ¶161. 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.

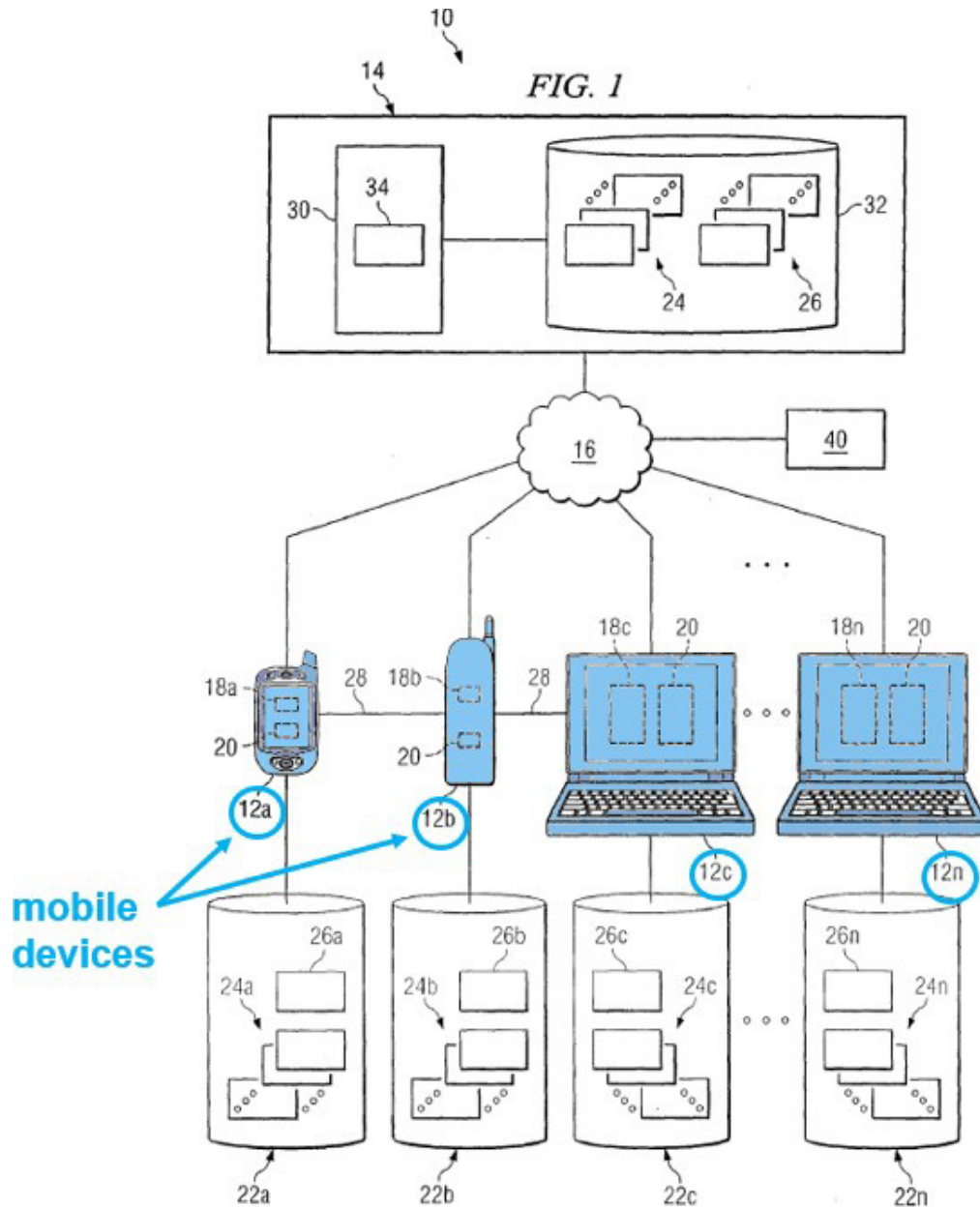
A POSITA would have had a reasonable expectation of success in combining Ribaudo-Watanabe with Behrens. EX1002, ¶¶162-165. All three describe similar proximity detection techniques in wireless systems that feature both short- range, Bluetooth communication as well as communication to a central server over the Internet. EX1006, ¶¶46-55; EX1007, ¶¶6-7; EX1008, Abstract, 6:1-30, 19:5-14. And Ribaudo 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, 68. A POSITA would thus have understood that applying Behrens’ teachings to the Ribaudo-Watanabe system would have yielded predictable results. EX1002 ¶¶162-165. 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. Independent Claim 29

1. 29[pre]

Ribaudo in view of Watanabe and Behrens (“Ribaudo-Watanabe-Behrens”) teaches the preamble. Section V.D.1 (1[pre]/30[pre]); EX1002, ¶166. Figure 1 of Ribaudo 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 id.*, ¶15, FIG. 1.



EX1007, FIG. 1 (annotated).

2. 29[a]

Ribaudo-Watanabe-Behrens teaches 29[a]. Sections V.D.2-V.D.3 (1[a]/30[a]-1[b]/30[b]); EX1002, ¶¶167-172. 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, FIG. 1. Ribaudó explains that “the present invention contemplates any other suitable wireless platforms, including but not limited to BLUETOOTH, ZIGBEE, WiMax, RFID, UWB, GSM, CDMA, a proprietary platform, cell tower triangulation, and GPS.” EX1007, ¶76.

For example, Ribaudó describes a radio for providing reception and transmission via a “Bluetooth” wireless protocol, such as an “adaptor 18” that “may facilitate communication with other mobile devices 12 (e.g., mobile devices 12b through 12n).” EX1007, ¶¶18-19, 154, 157, 181-184, 205, FIG. 1. Ribaudó also explains that “BLUETOOTH-enabled mobile devices 12 may use BLUETOOTH technology to detect matches in proximity.” EX1007, ¶¶66-67, 73. Adaptor 18a’s Bluetooth radio teaches the Bluetooth aspects of 29[a]. EX1002, ¶169; *see also* EX1011 (Proctor Decl.), ¶¶73-89.

Ribaudó also describes additional radio functionality for a second wireless protocol, such as a cellular protocol among other wireless protocols. EX1007, ¶¶76, 79, 184. For example, “mobile devices 12 may each be coupled to data center 14 via network 16”—which may include “*wide area networks (WANs)*, [or] all or a portion of a global computer network such as the Internet”—and that the

connection may be through a “*wireless link*.” EX1007, ¶¶24-25. Ribaudó’s system may “employ[] a *cellular* connection ... to download from data center 14.”

EX1007, ¶204. Adaptor 18a’s cellular/WWAN radio therefore teaches the claimed *second wireless protocol*. EX1002, ¶170; *see also* EX1011 (Proctor Decl.), ¶¶73-89.

3. 29[b]

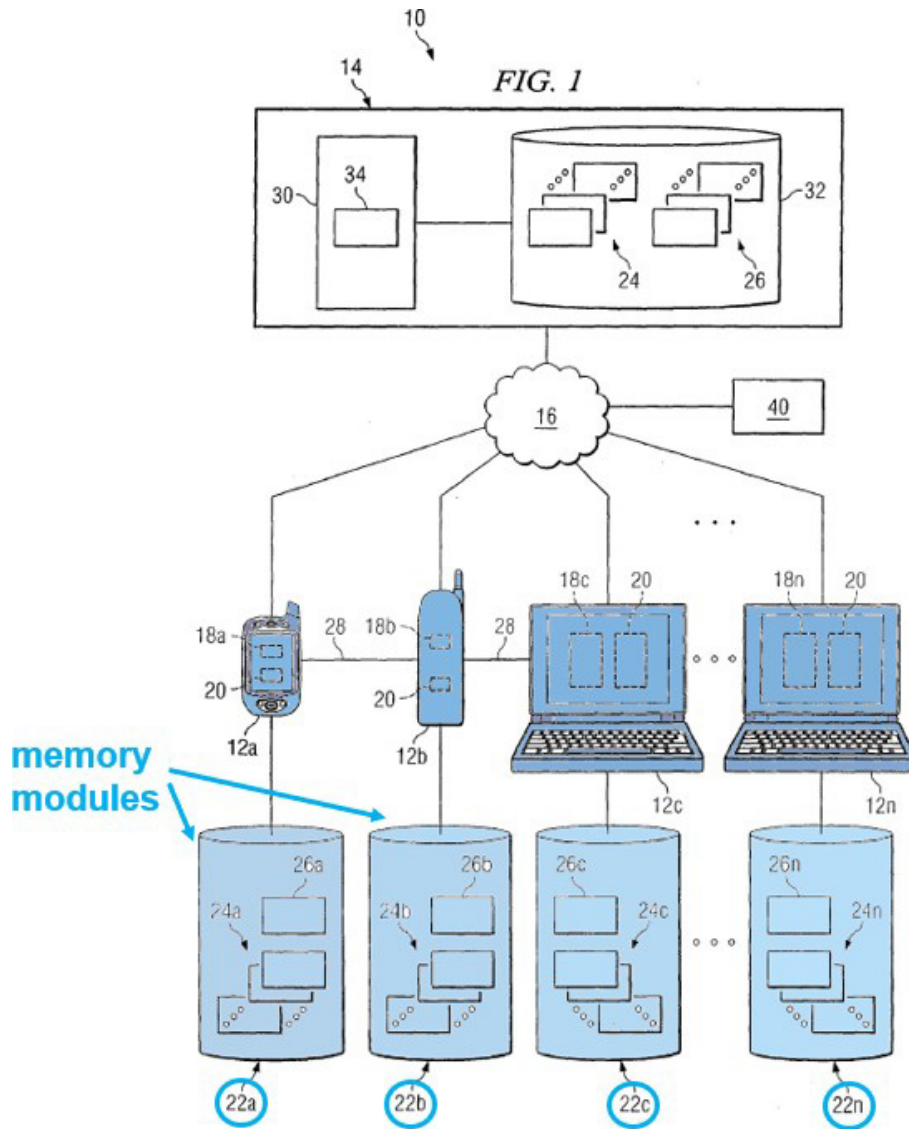
Ribaudó-Watanabe-Behrens teaches 29[b]. Section V.D.1 (1[pre]/30[pre]); EX1007, ¶19; EX1002, ¶¶173-175. Ribaudó teaches mobile devices 12 “may include, for example, ‘laptop’ computers, ‘palmtop’ computers, personal digital assistants, pagers, cellular telephones, game consoles, cameras, or any other suitable types of portable devices.” EX1007, ¶18. Mobile devices 12 also “each include any suitable combination of hardware, software, and firmware to provide the functionality described” including “one or more applications 20 that are based on one or more programming languages” to “facilitate communication with other mobile devices 12” and the data center. EX1007, ¶19.

While Ribaudó does not explicitly state that mobile devices 12 include processors, a POSITA would have understood that Ribaudó’s mobile devices 12 would have included one or more processors to perform the described functionality. EX1002, ¶174. Behrens confirms this understanding and describes hardware used to implement mobile telephones or other “small, battery-powered

handheld device[s].” EX1008, 20:31-21:15. Behrens explains that such devices include “*at least one microprocessor* for managing the wireless radio transmissions as well as for processing and storing data.” EX1008, 20:31-21:15.

4. 29[c]

Ribaudo-Watanabe-Behrens teaches 29[c]. Section V.D.1 (1[pre]/30[pre]); EX1007, ¶¶19, 32; EX1002, ¶¶176-179. Ribaudo explains that its “[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.



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 “any other suitable information.” EX1007, ¶33; *see also* ¶84. Along with data, the memory module stores software instructions for performing the functions described below. EX1007, Cl. 31 (“[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 understood Ribaudo as teaching that its memory modules are coupled to one or more processors and store a set of software instructions that when executed by the processors, cause them to perform the operations described below. EX1002, ¶¶177-179. Behrens also confirms this understanding and teaches a mobile phone including “memory” and “at least one microprocessor for managing the wireless radio transmissions as well as for processing and storing data.” EX1008, 20:31-21:15.

5. 29[d]

Ribaudo-Watanabe-Behrens teaches 29[d]. Section V.D.2 (1[a]/30[a]). EX1002, ¶¶180-185. In addition to the reasons provided for claim elements 1[a]/30[a], the combination also teaches that the first plurality of beacon transmissions are received *during a first time period*. 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. *See, e.g.*, EX1007, ¶¶45-46, 58, 60-61, 64, 68, 72 (describing “time-slicing”), 78, 148, 162-164, FIG. 2; EX1002, ¶181. Watanabe corroborates this. *See* EX1006, ¶¶14, 46, 49 (explaining that a plurality of beacons can be transmitted “continuously” or “periodically”).

Behrens also 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, ¶182. As will be further described with reference to claim elements 29[h]-29[k], the Ribaud-Watanabe-Behrens combination also teaches changing unique identifiers and MAC addresses over different time periods. *See* Section VI.B; *infra* Sections VI.C.9-12.

6. 29[e]

Ribaud-Watanabe-Behrens teaches 29[e]. Section V.D.3 (1[b]/30[b]). EX1002, ¶¶186-187.

7. 29[f]

Ribaud-Watanabe-Behrens teaches 29[f]. Section V.D.4 (1[c]/30[c]). EX1002, ¶¶188-189.

8. 29[g]

Ribaud-Watanabe-Behrens Element 29[g]. Section V.D.5 (1[d]/30[d]). EX1002, ¶¶190-191.

9. 29[h]

Ribaud-Watanabe-Behrens teaches 29[h]. As explained in the Section VI introduction, claim 29 repeats the “receiving” step of claims 1 and 30, but during a

second time period, the beacon transmitter transmits the same service identifier but with a different unique identifier and a different MAC address. As explained in Sections VI.B and VI.C.5 (29[d]), a mobile device in the Ribaud-Watanabe-Behrens combination would receive a second plurality of beacon transmissions during the claimed “*second time period.*”

Again, Behrens describes receiving unique identifiers (UIDs) beacons at different time periods. EX1008, 30:23-31:13. For example, Behrens describes a portable electronic device that scans “continuously/repeatedly for UIDs sent out by other devices” and records these UIDs in a log. EX1008, 10:24-11:9, 28:19-20, 31:6-13. “When such a device receives another device’s UID, it records that UID and measures the length of time during which it continues to receive that UID. The device stores the received UID, along with the time, date and duration of the reception.” EX1008, 11:11-17. Behrens further describes the mobile device determining that the UID is no longer received but then 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, ¶¶192-197. In the Ribaud-Watanabe-Behrens combination, this would include receiving a *second plurality of beacon transmissions* during a *second time period*, where each beacon transmission would

include a MAC address, a unique identifier, and a beacon service identifier as explained for 1[a]/30[a]. Section V.D.2 (1[a]/30[a]); EX1002, ¶¶192-197.

10. 29[i]

Ribaudo-Watanabe-Behrens teaches 29[i] as explained for 1[c], 30[c], and 29[f]. Sections V.D.4 (1[c]/30[c]), VI.C.7 (29[f]). Namely, the selection of unique identifiers based on filtering beacon transmissions including a beacon service identifier occurs in the same way. Ribaudo describes filtering while Watanabe describes filtering based on particular service codes. EX1007, ¶¶6-7, 58, 61, 64; EX1006, ¶¶41, 48-49, 51-52, 57. In view of these teachings, a mobile device would have performed filtering for the *same particular beacon service identifier* regardless of whether the mobile device detected a first or second plurality of beacon transmissions. EX1002, ¶¶198-199. For example, when the mobile device is configured to identify a beacon service identifier corresponding to a matching or “dating” service in Ribaudo, the mobile device would detect this “dating” service identifier (e.g., via Watanabe’s service code) in any plurality of beacon transmissions. EX1007, ¶¶55, 90, 97-104, 223; EX1002, ¶¶198-199. The selection of the unique identifier would also occur in the same manner and would be subsequently used to identify a match. Sections V.D.4 (1[c]/30[c]), VI.C.7 (29[f]); EX1002, ¶¶198-199.

11. 29[j]

Ribaudo-Watanabe-Behrens teaches 29[j] as explained for 1[d], 30[d], and 29[g] and as further explained below. Sections V.D.5 (1[d]/30[d]), VI.C.8 (29[g]); EX1002, ¶¶200-210.

- a. Taking second further action relating to the stored information, if a second unique identifier is present among the one or more unique identifiers selected from the second plurality of beacon transmissions**

The Ribaudo-Watanabe-Behrens combination teaches taking the claimed *second further action*. As explained for 1[d]/30[d], Ribaudo and Watanabe teach performing further actions relating to the stored information based on the detection of a particular unique identifier. Sections V.D.5 (1[d]/30[d]), VI.C.8 (29[g]). Thus, Ribaudo-Watanabe-Behrens teaches the claimed *second further action* for the same reasons presented for taking the *first further action*. Sections V.D.5 (1[d]/30[d]), VI.C.8 (29[g]); EX1002, ¶201.

- b. Wherein the second unique identifier is associated with the same entity or object, and wherein the second unique identifier is not equal to the first unique identifier**

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 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,

61-62; EX1008, 23:1-5.

Behrens teaches electronic devices that transmit unique identifiers (UIDs) that “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 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.

In light of Behren’s teachings, it would have been obvious for Ribaudó’s mobile devices to beacon different client IDs (i.e., claimed *unique identifiers*) at different times for at least masking, context, or privacy purposes. *See* EX1007, ¶62 (describing using different user IDs with different masks), ¶46 (client ID may be user ID); EX1002, ¶¶202-206.

Thus, Ribaudó and Behrens describe a *second unique identifier* that is *associated with the same entity or object* as the *first unique identifier* and that the second and first identifiers are *not equal*. *Id.*

c. Received beacon transmissions including the first and second unique identifiers are received from a same transmitting device

Ribaudo-Watanabe-Behrens teaches that the received beacon transmissions including the first and second unique identifiers are received from the same transmitting device. Ribaudo describes assigning multiple IDs to a mobile device. EX1007, ¶¶45-46, 68, 72, 84-85. Ribaudo describes generating “one or more identifiers (IDs) for a user” and assigning at least two types of client IDs to a mobile device: a public client ID and a user ID that “may reveal the true identity of the user.” EX1007, ¶¶45-46. Ribaudo therefore teaches a mobile device transmitting beacons using different identifiers.

Behrens describes assigning “*multiple or changing UIDs*” to a mobile device where each UID may be linked to a single user account. EX1008, 23:1-5. Behrens further describes the mobile device transmitting a particular UID “via short or medium range wireless transmission.” EX1008, 22:24-25, 23:7-24:5. That is, when a device has multiple or changing UIDs, the mobile device may select one or more of them to transmit. EX1008, 22:24-29.

Thus, the Ribaudo-Watanabe-Behrens combination teaches a mobile device (i.e., the same mobile device or the *same transmitting device*) that sends beacon transmissions using different unique identifiers. EX1002, ¶¶207-210.

12. 29[k]

Ribaudo-Watanabe-Behrens teaches 29[k]. EX1002 ¶¶211-214.

- a. **MAC address received in beacon transmission including the second unique identifier is different from MAC address received in beacon transmission including the first unique identifier**

Behrens teaches multiple or changing MAC addresses. Namely, Behrens teaches changing UUIDs—such as MAC addresses.⁶ EX1008, 11:21-26, 19:8-14, 22:25-27, 23:1-5. For example, Behrens describes using a “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. Thus, Behrens describes multiple or changing MAC addresses that may be used in beacon transmissions and that multiple MAC addresses and unique identifiers may be associated with the same user and/or mobile device that transmits beacons. EX1002, ¶212. In light of Behrens’s teachings, it would have been obvious for Ribaudo’s mobile devices to beacon different MAC addresses at different times. *Id.*; Section VI.B.

⁶ As explained for 1[a]/30[a] and 29[j], Petitioner relies on Ribaudo’s client IDs to teach the claimed “*unique identifiers*.” The Ribaudo-Behrens combination renders obvious client IDs changing over time.

b. Each beacon transmission includes the same particular beacon service identifier

As explained for 29[i], 1[c]/30[c], and 29[f], Ribaud-Watanabe-Behrens teaches multiple beacon transmissions including the same particular beacon service identifier. Sections V.D.4 (1[c]/30[c]), VI.C.7 (29[f]), VI.C.10 (29[i]). Taken with Behrens's teaching of multiple changing unique identifiers and/or MAC addresses, Ribaud-Watanabe-Behrens teaches the beacon transmissions maintaining the same particular beacon service identifier (e.g., a particular service code from Watanabe). Sections V.D.4 (1[c]/30[c]), VI.C.7 (29[f]), VI.C.10 (29[i]); EX1008, 11:21-26, 22:25-27, 23:1-5. For example, if the particular service is a "dating" service or business networking, as described in Ribaud, the beacon transmissions in the combination would still include an identification of this service even when unique identifiers and/or MAC addresses are changing. Sections V.C, V.D.4, VI.C.10 (explaining the beacon transmission filtering provided by Watanabe based on a type of service). Thus, Ribaud-Watanabe-Behrens teaches each beacon transmissions including *the same particular beacon service identifier*. EX1002, ¶¶213-214.

D. Dependent Claims 2-10, 12, 14, 16-19, 21-26, and 28

1. Claim 2

a. 2[pre]

Ribaud-Watanabe-Behrens teaches the preamble. Section VI.C.5 (29[d]);

EX1002, ¶215.

b. 2[a]

Ribaudo-Watanabe-Behrens teaches 2[a]. Section VI.C.9 (29[h]). EX1002, ¶216.

c. 2[b]

Ribaudo-Watanabe-Behrens teaches 2[b]. Section VI.C.10 (29[i]). EX1002, ¶217.

d. 2[c]

Ribaudo-Watanabe-Behrens teaches 2[c]. Section VI.C.11 (29[j]). EX1002, ¶218.

2. Claim 3

Ribaudo-Watanabe-Behrens teaches claim 3. Sections VI.C.5 (29[d]), VI.C.12 (29[k]); EX1002, ¶¶219-223.

a. Different MAC addresses received in different beacon transmissions but each beacon transmission includes the same beacon service identifier

Ribaudo-Watanabe-Behrens teaches this limitation for the reasons explained in Section VI.C.12 (29[k]). EX1002, ¶220.

b. A plurality of beacon transmissions including the particular service identifier and the first unique identifier are received in the first time period

As explained in Sections V.D.2 (1[a]/30[a]), VI.C.5 (29[d]), VI.C.7 (29[f]), VI.C.12 (29[k]), Ribaudo-Watanabe-Behrens describes the first plurality of beacon

transmissions received during the first time period including a particular service identifier and a first unique identifier. EX1002, ¶¶221-222.

c. No beacon transmissions including the same service identifier and the second unique identifier are received in the first time period

As explained in Section VI.C.9 (29[h]), the plurality of beacon transmissions sent during the *second* time period would include the same service identifier and the second unique identifier in view of Behrens’s teachings. For example, the combination teaches beacon transmissions in the first time period having a particular service identifier, a unique identifier, and a MAC address. Section VI.C.5 (29[d]). The combination also teaches beacon transmissions in the second time period including the same service identifier but different unique identifiers and MAC addresses. Sections VI.C.11-12 (29[j]-29[k]). Based on these teachings, no transmissions during the first time period include both a second unique identifier and the same service identifier. EX1002, ¶223.

3. Claim 4

Ribaudo-Watanabe-Behrens teaches claim 4 because, as explained in Sections V.D.5 (1[d]/30[d]), VI.C.9 (29[h]), and VI.C.11 (29[j]), Ribaudo’s mobile device determines whether an entity associated with a proximity beacon service (e.g., a matching or “dating” service) is in proximity based on a beacon service identifier such as Watanabe’s service code. EX1002, ¶224. Ribaudo describes

performing various actions (e.g., a *second further action*) in response to this determination. *Id.* These actions include establishing communication between users of mobile devices 12, notifying a mobile device 12 of a match, uploading match data to data center 14, and retrieving content from data center 14 to display a match value on the mobile device 12. EX1007, ¶¶17, 47, 78, 87, 134. Further, Ribaudo also describes an “application” that has been launched on the mobile device to provide such functionality. EX1007, ¶¶84-85, 120-125, 141. Ribaudo therefore teaches a second further action based upon a function currently being performed on a device (e.g., operating a matching or dating application).

4. Claim 5

Ribaudo-Watanabe-Behrens teaches claim 5. EX1002, ¶¶225-226.

Ribaudo teaches that the *function* is related to a *shared application*. For example, Ribaudo’s shared application performs a number of functions including a filter/comparison function to identify a match and authenticate users. EX1007, ¶¶22 (“application 20 may perform certain functions to facilitate communication”), 84 (“user of mobile device 12a *launches application 20* on mobile device 12a”), 141 (“application 20 ... may access match data”), FIG. 1 (showing application 20 on multiple devices). Ribaudo also teaches allowing “users of mobile devices 12 who have installed application 20 *to distribute copies of application 20 to other users.*” EX1007 ¶120; *see also* ¶¶123, 139 (second user may “acquire application

20 from another user ... to engage in messaging”), 220.

5. Claim 6

Ribaudo-Watanabe-Behrens teaches claim 6. EX1002, ¶¶227-229.

Ribaudo teaches receiving advertising information for presentation to a user of the wireless device. Ribaudo teaches that data center 14 “may collect and store content generated by users of mobile devices 12” such as by associating URLs corresponding to “personal advertisements, classified advertisements, advertisements, and other suitable content to the MAC addresses and cell tower IDs that the user encounters.” EX1007, ¶215; *see* ¶16 (match data includes “other information”). Ribaudo also teaches that “advertisements, *personal advertisements*, and classified advertisements may be served on a per wireless access point basis” and “displayed on mobile devices 12 using application 20.” EX1007, ¶217. Ribaudo also describes that these advertisements may be provided upon a match, by which its data center 14 enables the mobile device 12 to receive advertisement content “based on implied proximity.” EX1007, ¶¶215-217. A POSITA would have also found such personalized advertising obvious in view of the Ribaudo’s delivering business-related communications (e.g., “sales,” “facilitation of business transactions,” “finding a doctor or other service,” etc.) based on matching commonalities. EX1007, ¶¶140, 152, 223-224; EX1002, ¶¶227-229.

6. Claim 7

Ribaudo-Watanabe-Behrens teaches claim 7.

Ribaudo teaches retrieving content from a server once a match between mobile devices occurs. Sections V.D.5 (1[d]/30[d]), VI.D.5 (claim 6). The determination of a match using a unique identifier discloses an example of *information derived from a first/second unique identifier*. EX1002, ¶230. After matching, Ribaudo’s mobile device retrieves and displays content related to commonalities with a matching user—e.g., displaying “Harvard” when users have a “University” commonality. EX1007, ¶¶17, 47, 78, 134. Ribaudo further describes mobile devices retrieving commonality content from the server for display based on a client ID match. EX1007, ¶¶130-131, 148-150. These operations may occur as a *first further action*. EX1002, ¶230.

Ribaudo’s “personal URL” discloses another example of *information derived from a first/second unique identifier*. EX1007, ¶¶126-147, FIG. 3. The “personal URL” is derived from a client ID (*unique identifier*) because it is constructed using a client ID. EX1007, ¶¶127-130. Ribaudo discloses that match data may include “any suitable information,” EX1007, ¶¶49-51, and thus it was obvious to include a personal URL in the match data. It was further obvious that a mobile device could then use the personal URL to retrieve content—e.g., commonality information—from data center 14 upon detecting a match. EX1007,

¶¶128, 130-132, 134, 138-144, 146-47; EX1002, ¶231.

7. Claim 8

Ribaudo-Watanabe-Behrens teaches claim 8. EX1002, ¶¶232-233.

Ribaudo teaches sending a message to another device associated with an account. Ribaudo teaches that “adaptor 18a” may transmit “messages and presence information” between matched users—e.g., to determine “a meeting place or other venue for interaction.” EX1007, ¶79. Adaptor 18a may use the “TCP/IP protocol” or other short-range protocols like “Wi-Fi”/“BLUETOOTH” to “create a messaging connection between mobile devices.” EX1007, ¶79. Ribaudo teaches that “each message that a user receives containing match data 26 identifying a match may include instructions for replying to the message” and “[i]f a user replies to the message, the message may be sent anonymously to the identified match.” EX1007, ¶164. Ribaudo indicates that messages between mobile devices 12 are related to the first and second unique identifiers received by the mobile device 12a, and the users may be registered users who have user accounts. EX1007, ¶¶30-31; Section V.D.5 (1[d]/30[d]).

8. Claim 9

Ribaudo-Watanabe-Behrens teaches claim 9. EX1002, ¶¶234-236.

Ribaudo teaches that a server associated with an account for a user of the wireless device sends a message to an email address associated with the account

for the user. EX1007, ¶¶151-153, 157 (describing data center 14 sending an “email” notification to a first user upon detecting a match); *see also* ¶¶30-31 (describing registered users and accounts), 140.

Ribaudo teaches that the first or second further action has already been performed (e.g., determining that a match is in proximity). Section V.D.5 (1[d]/30[d]). Then, the user of mobile device 12a may be notified by data center 14, via email, that communication with mobile device 12b has been established. EX1007, ¶¶148, 157. Ribaudo also teaches that data center 14 may email the user of mobile device 12a in the event that communication between mobile devices was established (i.e., a match) but no messages between the devices were exchanged (referred to as a “missed encounter”). EX1007, ¶¶151-153.

9. Claim 10

Ribaudo-Watanabe-Behrens teaches claim 10, which recites “preventing sending” the second unique identifier (e.g., client ID) or information derived from the second unique identifier to the server(s). EX1002, ¶¶237-241. Other than a single sentence in the “Summary” section that tracks the claim language, the specification provides no description of what this “preventing” entails or how it may be implemented. EX1001, 2:54-56. The patent’s lack of detail demonstrates that this limitation 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 [a POSITA] 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).

Regardless, Ribauda 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, Ribauda teaches that a user may filter 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 in detail 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, ¶238.

Ribauda also teaches preventing the sending of a unique identifier to a server when determining whether a detected identifier matches a client ID that has already been downloaded to a mobile device as “pre-processed match data.” EX1007, ¶¶6-7 (describing match determination “*without consulting the data*

center”); *see also* Abstract, ¶¶16, 48-51, cl. 9; Sections V.D.3-4 (1[b]/30[b]-1[c]/30[c]). When no additional information is needed from the server to detect that a matching mobile device is in proximity, Ribaudo prevents the sending of a unique identifier to a server. EX1002, ¶239. 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. *Id.*

Additionally, Behrens teaches that a user may “instruct the server to ignore specific UIDs,” “tell the server to block specific UIDs, or to have the server instruct his portable device to ignore specific UIDs and vice versa.” EX1008, 20:10-15. Behrens also teaches “blacklists” which can instruct a server or device to ignore certain UIDs. 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 UIDs rather than send them and have them ignored. EX1002, ¶240. Preventing the transmission of such identifiers would beneficially reduce use of transmission bandwidth and power. *Id.*

Ribaudo teaches that the second further action is related to the second unique identifier for the reasons explained in Sections VI.C.11 (29[j]) and VI.D.1.d (2[c]). EX1002, ¶241. In Ribaudo-Watanabe-Behrens, the second further action involving the second unique identifier includes preventing sending of the second

unique identifier to a server. *Id.*

10. Claim 12

Ribaudo-Watanabe-Behrens teaches claim 12. EX1002, ¶¶242-247.

Ribaudo discloses performing proximity detection before downloading match data (*stored information*) from the server. EX1007, ¶¶204-205 (mobile devices first detect another user in proximity and subsequently “download from data center 14 the individual match IDs for those users.”); EX1002, ¶243. This teaches the ability to receive *stored information* (match data) in response to sending a detected unique identifier to a server. EX1007, ¶¶65-68, 204-205; *see also* ¶¶31, 40-42, 53 (describing match data “synchronization” or downloading the newest or “most current match data”).

Ribaudo also 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; EX1002, ¶¶244-246. 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. Accessing the personal URL or summary link transmits the client ID (a “*first unique identifier*”) to the data center. EX1002, ¶¶244-246 (citing EX1012, ¶¶6-7, 9-13).

Ribaudo teaches that the first further action is related to the first unique identifier for the reasons explained in Section V.D.5 (1[d]/30[d]). EX1002, ¶247. In Ribaudo-Watanabe-Behrens, taking a first further action includes causing Ribaudo's mobile device to send the first unique identifier or information derived from it to one or more servers (data center 14) and receive the stored information (match data) in response. EX1007, ¶¶204-205.

11. Claim 14

Ribaudo-Watanabe-Behrens teaches claim 14. Sections V.D.3 (1[b]/30[b]) (receiving stored information at wireless device from server relating to entity/object with first unique identifier), V.D.4 (1[c]/30[c]) (selecting unique identifier(s) by filtering), and V.D.5 (1[d]/30[d]) (taking first further action relating to stored information if first unique identifier is present among selected unique identifier(s)). EX1002, ¶248. This operation and sequence, described with reference to claim 1, teaches stored information being received prior to performing the first further action. *Id.*

12. Claim 16

Ribaudo-Watanabe-Behrens teaches claim 16. Section V.D.2 (1[a]/30[a]); EX1002, ¶¶249-251. For example, Watanabe teaches using a particular service code to identify a service that is usable by multiple beacon transmitter devices.

Watanabe indicates that “AP managing unit 11-1 manages services S1, S2, and S3,” “AP managing unit 11-2 manages services S2 and S3,” and “AP managing unit 11-3 manages service S3.” EX1006, ¶40. This teaches multiple beacon transmitter devices capable of transmitting the same particular beacon service identifier. EX1002, ¶250. In the Ribaud-Watanabe-Behrens combination, Ribaud’s mobile device 12 would beacon one of Watanabe’s service identifiers (e.g., “S3”) based on the type of matching service used by the mobile device 12 (e.g., a dating service). *Id.*

In Ribaud-Watanabe-Behrens, a POSITA would have found it obvious and would have been motivated to use the same “service code” for all mobile devices participating in Ribaud’s matching service to convey participation. EX1007, ¶¶97-104, 123; EX1002, ¶251; Section V.C. All users within a given area would use the same service code to identify the matching service and beacon transmissions from other matching service participants. Section V.C; EX1002, ¶251.

13. Claim 17

Ribaud-Watanabe-Behrens teaches claim 17 for the reasons presented for claim 11. Section V.E.1; EX1002, ¶252.

14. Claim 18

Ribaud-Watanabe-Behrens teaches claim 18. EX1002, ¶¶253-254.

Ribaudo teaches that one or more of the steps performed at the wireless device are as a result of an application program executing on the wireless device. Ribaudo teaches that “*the user of mobile device 12a launches application 20* on mobile device 12a,” which “may attempt to detect other mobile devices 12 in proximity to mobile device 12a” by using match data “(e.g., the match IDs) downloaded from data center 14” and beaconing “data such as the client ID of the user associated with mobile device 12a.” EX1007, ¶84; *see also* ¶¶120, 123, FIG. 1 (application 20); EX1002, ¶¶253-254.

15. Claim 19

Ribaudo-Watanabe-Behrens teaches claim 19.

Ribaudo teaches that the second further action is related to an advertisement tied to a location for the reasons explained in Section VI.D.5 (claim 6). Ribaudo teaches that data center 14 “may collect and store content generated by users of mobile devices 12” such as by associating “the URLs of a user’s ... personal advertisements, classified advertisements, advertisements, and other suitable content to the MAC addresses and cell tower IDs that the user encounters.” EX1007, ¶215. Ribaudo also teaches that “*advertisements*, personal advertisements, and classified advertisements *may be served on a per wireless access point basis* (e.g., a per MAC address basis or per cell tower ID basis)” and “displayed on mobile devices 12 using application 20.” EX1007, ¶217. An

advertisement tied to a cell tower ID would be tied to a location. EX1002, ¶¶255-256.

16. Claim 21

Ribaudo-Watanabe-Behrens teaches claim 21 for the reasons presented for claim 20. Section V.E.4; EX1002, ¶257.

17. Claim 22

Ribaudo-Watanabe-Behrens teaches claim 22. EX1002, ¶¶258-260.

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 amongst each other and access user profile information present on a respective mobile device. EX1007, ¶¶78-79, 81-83, 137, 151-153 (describing delayed communication and access via a website). Thus, a first mobile device is allowed to access a second mobile device (i.e., device associated with the wireless beacon service) to perform further communications.

As described for claim 19, the user is also provided access to an advertisement. EX1007, ¶215; Section VI.D.15. Therefore, Ribaudo also teaches allowing a user associated with the wireless device access to an object (e.g., advertisement) associated with the wireless beacon service. EX1002, ¶260.

18. Claim 23

Ribaudo-Watanabe-Behrens teaches claim 23. Sections VI.D.1.d (2[c]),

VI.C.11 (29[j]); EX1002, ¶¶261-264. Ribaudó teaches *controlling further communications* via, for example, enabling communications between mobile devices, controlling advertising, and/or blocking communications. EX1002, ¶¶261-264.

As discussed for claim 22, when a proximity match is detected, Ribaudó's mobile devices may exchange messages and access user profile information present on a respective mobile device. EX1007, ¶¶78-79, 81-83, 137, 151-153 (delayed communications with fixed period to communicate); Section VI.D.17. Allowing these communications teaches controlling communications between a wireless device and another device associated with an entity in proximity (e.g., the user or owner of the other device). EX1002, ¶¶262-263.

Ribaudó 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. *See, e.g.*, EX1007, ¶¶140, 217.

Ribaudó also discloses "controlling further communications" based on user preferences (e.g., "blocking"), *see, e.g.*, EX1007, ¶¶47, 101, or based on location or time. *See, e.g.*, EX1007, ¶¶117, 160, 163. This preference-based control is yet another example of Ribaudó controlling communications. EX1002, ¶264.

19. Claim 24

Ribaudo-Watanabe-Behrens teaches claim 24. EX1002, ¶¶265-266.

Ribaudo teaches data center 14 distributing match data to mobile devices for beacon detection “at a particular location and/or time” and also allowing match detection to be “scheduled in advance,” which teaches the claimed *timing notification information*. EX1007, ¶¶160-162; *see also* ¶¶84-85. Ribaudo also teaches that “matches may be filtered by time of the detected match in proximity.” EX1007, ¶64 (also describing notification of matches “at different points in time” including “currently in proximity”). Ribaudo further teaches that “the user may be open to sharing more information” based on “the time of day the match is detected.” EX1007, ¶78; *see also* ¶¶152, 229 (describing match “availability settings” based on time of day). Additionally, match data may be distributed to a group according to a “conference schedule.” EX1007, ¶163.

20. Claim 25

Ribaudo-Watanabe-Behrens teaches claim 25 for the reasons explained in Section VI.D.19 (claim 24). EX1002, ¶¶267-268.

Ribaudo also teaches that the wireless device’s receipt of the timing notification information is not directly from the beacon transmitter because it is received from data center 14, not another mobile device. EX1007, ¶¶82-83 (data center 14 distributing match data), 162-163 (match data distributed at “specified

times” or according to a “schedule”), 201; EX1002, ¶268.

21. Claim 26

Ribaudo-Watanabe-Behrens teaches claim 26. Sections VI.C.9-VI.C.11 (29[h]-29[j]), VI.D.1.b-VI.D.1.d (2[a]-2[c]). EX1002, ¶269.

22. Claim 28

Ribaudo-Watanabe-Behrens teaches claim 28. Section V.D.2 (1[a]/30[a]). EX1006 ¶27; EX1002, ¶270.

**VII. GROUND 3: RIBAUDO-WATANABE-BEHRENS-NORDMAN
RENDERS OBVIOUS CLAIM 27**

Ribaudo-Watanabe-Behrens-Nordman teaches claim 27. EX1002, ¶¶271-276.

Ribaudo teaches that “[t]he *unique MAC address* of mobile device 12a *may be beaconed* 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, ¶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. “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. *See* 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 the Ribaud-Watanabe-Behrens-Nordman teaches using such an address as a MAC address for Bluetooth devices. EX1002, ¶¶83-84, 273-274.

A POSITA would have been motivated to implement randomly generated Bluetooth addresses as MAC addresses to advance Ribaud’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 Ribaud-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 Ribaud, 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 Ribaud. 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. CERTIFICATION UNDER RULE 42.104(A)

Petitioner certifies that the '344 patent is available for IPR and Petitioner is not barred or estopped from requesting IPR of any claim.

IX. 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 '344 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 '344 patent was at issue in the following proceedings, which have been terminated:

- *Secure Comm'n Techs., LLC v. Samsung Electronics 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-

01050 (P.T.A.B.), filed May 30, 2025 (terminated August 27, 2025);

and

- *Google LLC v. Secure Comm'n Techs., LLC*, IPR2025-01182

(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. 11,334,918 (IPR2026-00445) and 11,687,971 (IPR2026-00447).

The '344 patent claims the benefit of U.S. Patent Nos. 11,074,615, 11,334,918, 9,161,164, 8,849,698, 8,385,896, 8,090,359. U.S. Patent Nos. 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 '344 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.

X. 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 13,987 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. 11,443,344 and associated Exhibits
1001-1012, 1021, 1025-1042, 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. 11,443,344

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