

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

SAMSUNG ELECTRONICS CO., LTD.;
SAMSUNG ELECTRONICS AMERICA, INC.,
Petitioner

v.

SECURE COMMUNICATION TECHNOLOGIES, LLC,
Patent Owner.

Case No. IPR2025-01049
U.S. Patent No. 11,334,918

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

TABLE OF CONTENTS

	Page
I. INTRODUCTION	1
II. MANDATORY NOTICES UNDER 37 C.F.R. §42.8.....	1
III. FEE AUTHORIZATION	3
IV. GROUNDS FOR STANDING.....	3
V. PRECISE RELIEF REQUESTED	3
VI. THE CHALLENGED PATENT	4
VII. PROSECUTION HISTORY OF THE '918 PATENT.....	6
VIII. LEVEL OF ORDINARY SKILL IN THE ART	7
IX. PRIORITY DATE	7
X. CLAIM CONSTRUCTION	8
XI. BRIEF DESCRIPTION OF THE APPLIED PRIOR ART	8
A. Ribaudó (Ex-1007).....	8
B. Watanabe (Ex-1005, Ex-1006).....	10
C. Behrens (Ex-1008)	13
D. Mgrdechian (Ex-1010)	14
XII. DETAILED EXPLANATION OF THE UNPATENTABILITY GROUNDS	16
A. Ground 1: Claims 1, 4-6, 9, 14, 16-20, 22, and 24-30 are obvious over Ribaudó.	16
1. Independent Claim 1	16
a. Element 1[pre]: A mobile wireless device comprising:	16
b. Element 1[a]: a first radio;.....	17
c. Element 1[b]: a second radio;.....	18
d. Element 1[c]: one or more processors;.....	18

TABLE OF CONTENTS

(continued)

	Page
e. Element 1[d]: one or more memory devices coupled to the one or more processors, the one or more memory devices storing a set of instructions that when executed by the one or more processors cause the one or more processors to perform operations including:	20
f. Element 1[e]: receiving, using the first radio, identifier related information associated with a proximity beacon service, from one or more servers;	22
g. Element 1[f]: [1] receiving, using the second radio, a plurality of short range transmissions, including a plurality of proximity beacon transmissions when the device is located within a detection range of one or more beacon transmitter devices associated with the proximity beacon service, [2] each of the proximity beacon transmissions including a respective MAC address, a respective unique identifier, and a Proximity Beacon Service Identifier (PBSI);	25
h. Element 1[g]: determining if a particular short range transmission of the plurality of short range transmissions a) includes a MAC address, and b) includes the proximity beacon service identifier (PBSI) and if c) the PBSI indicates the particular short range transmission is a proximity beacon transmission associated with the proximity beacon service; then:	32
i. Element 1[h]: determining if an entity or object associated with the proximity beacon service is in proximity to the mobile wireless device by utilizing the identifier related information and the unique identifier.....	34
2. Independent Claim 9	37

TABLE OF CONTENTS

(continued)

	Page
a. Element 9[pre]: A method for facilitating the use of proximity beacons, the method executing within a mobile device, and the method comprising:	37
b. Element 9[a]:	37
c. Element 9[b]:	38
d. Element 9[c]:	38
e. Element 9[d].	38
3. Dependent Claims 4-6, 14, 16-20, 22, and 24-30	38
a. Claim 4: The mobile wireless device of claim 1, wherein the one or more processors further execute the instructions to perform operations including: further determining that at least one beacon transmitter device associated with the proximity beacon service is in proximity to the mobile wireless device, by utilizing an action function including one or more previously downloaded unique identifiers.	38
b. Claim 5: The mobile wireless device of claim 1, wherein the one or more processors further execute the instructions to perform operations including determining, based upon at least a portion of the identifier related information, that at least one beacon transmitter is a broadcast device having a predetermined location.	40

TABLE OF CONTENTS
(continued)

Page

c.	Claim 6: The mobile wireless device of claim 1, wherein the identifier related information comprises application software for execution upon the mobile wireless device, and the one or more processors further execute the instructions to perform operations including sending of the unique identifier by the mobile wireless device to at least one server of the one or more servers; and in response to the sending of the unique identifier, downloading the application software.....	41
d.	Claim 14/19: [The mobile wireless device of claim 1, wherein the instructions further comprise/The method of claim 9, additionally comprising]: sending the unique identifier, using the first radio, to at least one server of the one or more servers, and receiving further information relating to an object or entity associated with being within proximity to the mobile device.....	43
e.	Claim 16/24: [The mobile wireless device of claim 1, wherein the instructions further comprise/ The method of claim 9, additionally comprising:] controlling further communications between the mobile device and at least one device or server associated with an entity or object in proximity to the mobile device.....	44
f.	Claim 17: The method of claim 9, further comprising: receiving, using the first radio, access code information by the mobile device from at least one of the servers; and utilizing the access code information to gain access to the entity or object determined to be in proximity to the mobile device.....	46

TABLE OF CONTENTS

(continued)

Page

g.	Claim 18/28: [The method of claim 9/The mobile wireless device of claim 1], wherein receiving the identifier related information, using the first radio, is performed in response to [the one or more processors executing instructions for:] sending at least the unique identifier to at least one of the one or more servers using the first radio.....	47
h.	Claim 20: The method of claim 19, wherein the further information relates to one or more of the following: a loyalty program; a payment service; or a coupon relating to an entity in proximity to the mobile device; or advertising content.....	48
i.	Claim 22: The method of claim 19, wherein the further information relates to a nearby user of an application on another device, in common with an application on the mobile device.....	49
j.	Claim 25: The method of claim 9, wherein the step of determining that an entity or object is within proximity further comprises: comparing the identifier related information with the unique identifier or information derived from the unique identifier.....	49
k.	Claim 26:	50
l.	Claim 27: The mobile wireless device of claim 1, wherein the one or more processors further execute the instructions to perform the operations for determining that an entity or object is within proximity by further: comparing the identifier related information with the unique identifier or information derived from the unique identifier.....	53

TABLE OF CONTENTS

(continued)

	Page
m. Claim 29: The method of claim 9, wherein the proximity beacon transmissions are received, at the mobile device, without requiring the mobile device to first perform a step of transmitting to the one or more beacon transmitter devices from which the plurality of proximity beacon transmissions are received.....	53
n. Claim 30:	54
B. Ground 2: Claims 1, 4-6, 9, 14, 16-20, 22, and 24-30 are obvious over Ribaudo in view of Watanabe.....	57
1. A POSITA would have been motivated to combine Ribaudo’s teachings with Watanabe’s teachings and would have had a reasonable expectation of success.	57
2. Independent Claim 1	60
a. Element 1[f]: ... each of the proximity beacon transmissions including ... a Proximity Beacon Service Identifier (PBSI);:	61
b. Element 1[g]:	61
3. Independent Claim 9	62
4. Dependent Claims 4-6, 14, 16-20, 22, and 24-30	62
a. Claim 5:	63
C. Grounds 3 and 4: Claims 2-3, 7-8, 10-13, 15, and 31 are obvious over Ribaudo in view of Behrens (Ground 3), or Ribaudo in view of Watanabe and Behrens (Ground 4).....	64
1. A POSITA would have been motivated to combine Ribaudo’s teachings, or Ribaudo-Watanabe’s teachings, with Behrens’ teachings and would have had a reasonable expectation of success.....	64
2. Dependent Claims 2-3, 7-8, 10-13, 15, and 31	67

TABLE OF CONTENTS

(continued)

	Page
a. Claim 2: The mobile wireless device of claim 1, wherein the MAC address is a randomly generated 48 bit number matching a format of a Bluetooth BD_ADDR.	67
b. Claim 3:	68
c. Claim 7:	72
d. Claim 8:	73
e. Claim 10:	73
f. Claim 11: The mobile wireless device of claim 9 wherein the MAC address is selected from a group consisting of (a) a randomly generated 48 bit number matching a format of a MAC address and (b) a Bluetooth BD_ADDR.	75
g. Claim 12:	75
h. Claim 13/15: The [method of claim 9, / mobile wireless device of claim 1, wherein the instructions] further compris[ing / e]: preventing the sending of the unique identifier, using the first radio, to the one or more servers, based upon previous detections of the respective unique identifier associated with the proximity beacon transmission.	76
i. Claim 31:	77
D. Grounds 5 and 6: Claim 23 is obvious over Ribaud in view of Mgrdechian (Ground 5), or Ribaud in view of Watanabe and Mgrdechian (Ground 6).....	78
1. Claim 23: The method of claim 22, wherein the application is a multiuser game.....	78
XIII. CONCLUSION.....	80

TABLE OF CONTENTS
(continued)

Page

LIST OF EXHIBITS¹

Ex. No.	Description
Ex-1001	U.S. Patent No. 11,334,918 (“the ’918 Patent”)
Ex-1002	Declaration of Dr. Sundeep Rangan
Ex-1003	Curriculum Vitae of Dr. Sundeep Rangan
Ex-1004	Prosecution History of U.S. Patent No. 11,334,918
Ex-1005	JP Patent Publication No. 2005/12973 to Watanabe
Ex-1006	Certified translation of JP Patent Publication No. 2005/12973 to Watanabe (“Watanabe”)
Ex-1007	U.S. Patent Publication No. 2007/0030824 to Ribaudó (“Ribaudó”)
Ex-1008	PCT Patent Publication No. WO2008/132241 to Behrens (“Behrens”)
Ex-1009	PCT Patent Publication No. WO2008/076827 to Krikorian (“Krikorian”)
Ex-1010	U.S. Patent Publication No. 2005/00174975 to Mgrdechian (“Mgrdechian”)
Ex-1011	Declaration of James A. Proctor, Jr.
Ex-1012	INTENTIONALLY LEFT BLANK
Ex-1013	INTENTIONALLY LEFT BLANK
Ex-1014	INTENTIONALLY LEFT BLANK
Ex-1015	INTENTIONALLY LEFT BLANK

¹ Four-digit pin citations that begin with 0 are to the branded numbers added by Samsung in the bottom right corner of the exhibits. All other pin citations are to original page, column, paragraph, or line numbers.

Ex. No.	Description
Ex-1016	INTENTIONALLY LEFT BLANK
Ex-1017	INTENTIONALLY LEFT BLANK
Ex-1018	INTENTIONALLY LEFT BLANK
Ex-1019	INTENTIONALLY LEFT BLANK
Ex-1020	Claim Mapping Table
Ex-1021	Bluetooth Specification v.2.0 + EDR (Nov. 2004)
Ex-1022	Telecom Dictionary (2007) (“beacon channel,” “beaconing”)
Ex-1023	Webster’s New World Telecom Dictionary (2008) (“beaconing”)
Ex-1024	Wikipedia, “ <i>Radio beacon</i> ”
Ex-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”)
Ex-1026	IEEE Standard 802.15.1, Part 15.1: Wireless medium access control and physical layer (PHY) specifications for wireless personal area networks (WPANs) (“Bluetooth Specification”)
Ex-1027	US Patent No. 7,000,001 to Lazaridis et al. (“Lazaridis”)
Ex-1028	US Patent Publication No. 2009/0239467 to Gulin et al. (“Gulin”)
Ex-1029	US Patent Publication No. 2004/0248569 to Kondou et al. (“Kondou”)
Ex-1030	US Patent Publication No. 2006/0287813 to Quigley et al. (“Quigley”)
Ex-1031	US Patent Publication No. 2005/0130634 to Godfrey (“Godfrey”)
Ex-1032	Wayne Jansen et al., Proximity Beacons and Mobile Device Authentication NISTIR 7200 (June 2005) (“Jansen”)

Ex. No.	Description
Ex-1033	US Patent Publication No. 2003/0220114 to Langensteiner et al. (“Langensteiner”)
Ex-1034	US Patent Publication No. 2008/0261526 to Suresh (“Suresh”)
Ex-1035	US Patent Publication No. 2009/0059878 to Tamura (“Tamura”)
Ex-1036	US Patent No. 8,411,662 (“Saund”)
Ex-1037	US Patent Publication No. 2008/0045181 to Suzuki (“Suzuki”)
Ex-1038	PCT Patent Publication No. WO2006/028640 to Briancon et al. (“Briancon”)
Ex-1039	Sorte et al., <i>Service publishing to support an efficient network selection in an 802.11 multi-access environment</i> (Jan. 2006) (“Sorte”)
Ex-1040	US Patent No. 6,928,263 to Blake et al. (“Blake”)
Ex-1041	Yeong, J. H., et al., <i>802.11 a MAC layer: firmware/hardware co-design.</i> , FOURTH INTERNATIONAL CONFERENCE ON INFORMATION, COMMUNICATIONS AND SIGNAL PROCESSING, 2003 (“Yeong”)
Ex-1042	Huang, L. et al., <i>Enhancing wireless location privacy using silent period</i> , IEEE WIRELESS COMMUNICATIONS AND NETWORKING CONFERENCE, (Vol. 2, pp. 1187-1192) (March, 2005) (“Huang”)
Ex-1043	IEEE 802 Specification IEEE Standard 802: IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture (Mar. 2002) (“IEEE 802 2002”)
Ex-1044	IEEE 802 Specification IEEE Standard 802.11g, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, Amendment 4: Further Higher Data Rate Extension in the 2.4 GHz Band (June 2003) (“IEEE 802.11g”)

Ex. No.	Description
Ex-1045	IEEE 802 Specification IEEE Standard 802.15.4, Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs) (Oct. 2003) (“IEEE 802.15.4”)

I. INTRODUCTION

Samsung Electronics Co., Ltd. and Samsung Electronics America, Inc. (collectively, “Petitioner”) request *inter partes* review of Claims 1-20 and 22-31 of U.S. Patent No. 11,334,918 (“the ’918 Patent”).

II. MANDATORY NOTICES UNDER 37 C.F.R. §42.8

Real Parties-in-Interest: Petitioner identifies the following real parties-in-interest: Samsung Electronics Co., Ltd. and Samsung Electronics America, Inc.

Related Matters: Patent Owner (“PO”) has asserted the ’918 Patent against Petitioner in *Secure Communication Technologies, LLC v. Samsung Electronics Co., Ltd., et al.*, No. 2:24-cv-484 (E.D. Tex.) (“Samsung litigation”).

Lead and Back-Up Counsel:

- Lead Counsel:

William M. Fink (Reg. No. 72,332)
O’Melveny & Myers LLP
1625 Eye Street, NW
Washington, DC 20006
Telephone: (202) 383-5300
Fax: (202) 383-5414
E-Mail: tfink@omm.com

- Backup Counsel:

Brian Cook (Reg. No. 59,356)
O’Melveny & Myers LLP
400 South Hope Street, 18th Floor
Los Angeles, CA 90071
Telephone: (213) 430-6000
Fax: (213) 430-6407

E-Mail: bcook@omm.com

Nicholas Whilt (Reg. No. 72,081)
O'Melveny & Myers LLP
400 South Hope Street, 18th Floor
Los Angeles, CA 90071
Telephone: (213) 430-6000
Fax: (213) 430-6407
Email: nwhilt@omm.com

Benjamin M. Haber (Reg. No. 67,129)
O'Melveny & Myers LLP
400 South Hope Street, 18th Floor
Los Angeles, CA 90071
Telephone: (213) 430-6000
Fax: (213) 430-6407
Email: bhaber@omm.com

Caitlin P. Hogan (Reg. No. 61,515)
O'Melveny & Myers LLP
1301 Avenue of the Americas, Suite 1700
New York, NY 10019
Telephone: (212) 326-2000
Fax: (212) 326-2061
Email: chogan@omm.com

Raj Paul (Reg. No. 64,492)
O'Melveny & Myers LLP
1625 Eye Street, NW
Washington, DC 20006
Phone: (202) 383-5300
Fax: (202) 383-5414
E-Mail: rpaul@omm.com

Service Information: Petitioner consents to electronic service by email to the following addresses:

- tfink@omm.com

- bcook@omm.com
- nwhilt@omm.com
- bhaber@omm.com
- chogan@omm.com
- rpaul@omm.com
- ommsamsungsecurecommunicationsedtx@omm.com

III. FEE AUTHORIZATION

The PTO is authorized to charge any fees due during this proceeding to Deposit Account No. LA500639.

IV. GROUNDS FOR STANDING

Petitioner certifies that the '918 Patent is available for review, and Petitioner is not barred or estopped from requesting review.

V. PRECISE RELIEF REQUESTED

Petitioner requests review and cancellation of Claims 1-20 and 22-31 as unpatentable based on the following grounds, supported by a declaration from Dr. Rangan. Ex-1002 ¶¶28, 260; Ex-1003.

Ground	Summary
1 & 2	Claims 1, 4-6, 9, 14, 16-20, 22, and 24-30 are obvious over Ribaudó (Ground 1) or Ribaudó in view of Watanabe (Ground 2)
3 & 4	Claims 2-3, 7-8, 10-13, 15, and 31 are obvious over Ribaudó in view of Behrens (Ground 3) or Ribaudó in view of Watanabe and Behrens (Ground 4)
5 & 6	Claim 23 is obvious over Ribaudó in view of Mgrdechian (Ground 5) or Ribaudó in view of Watanabe and Mgrdechian (Ground 6)

VI. THE CHALLENGED PATENT

The '918 Patent describes mobile wireless devices (e.g., cellular phones) exchanging information “utilizing both a short range and long range wireless capability.” Ex-1001, 2:66-3:3. Conventional cellular 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. Ex-1001, 2:25-48. The '918 Patent proposes both wireless capabilities to allow peer-to-peer communication for proximity detection using identifiers, while using a server to broker the exchange of information between two wireless devices. *Id.*, 2:58-3:14.

As shown in Figure 1 below,² “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. Ex-1001, 5:62-6:6, Fig. 1 (annotated). The devices are also able to communicate directly with each other via “a short range wireless link 107” (yellow). *Id.*, 6:55-66.

² Throughout, emphasis and annotations are added unless otherwise specified.

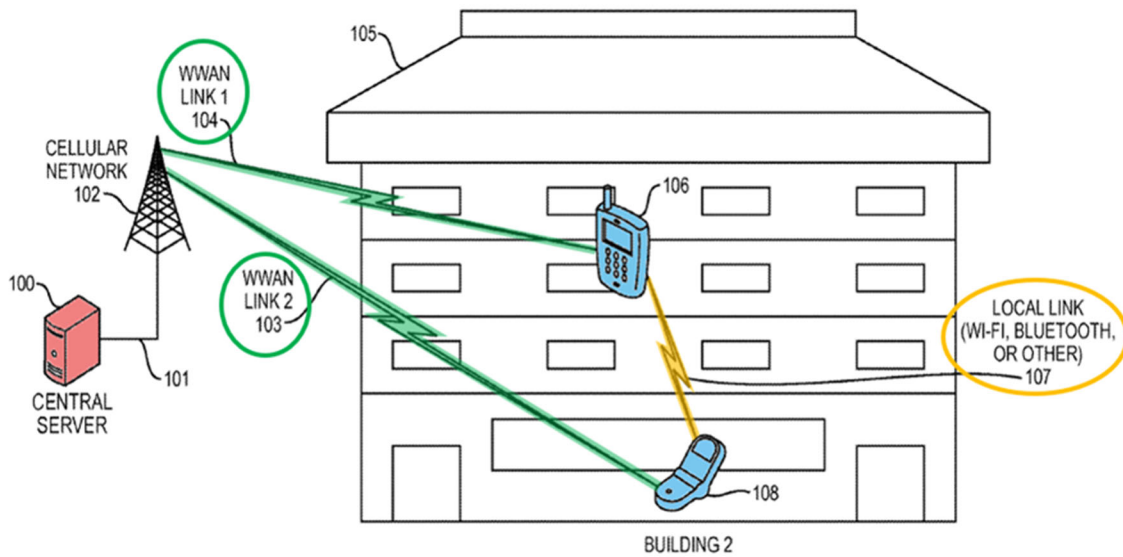


Figure 1

One example of the short-range wireless capability, shown in Figure 6, is an “independent basic service set or IBSS,” involving an “ad-hoc network” of wireless devices that “transmit identifiers called *beacons*.” Ex-1001, 10:31-44. Beacon transmissions include MAC address, basic service set identifier (BSSID), and ad-hoc network name or (SSID), where “one or both of the BSSID and the SSID may be used to indicate these particular beacons are associated with a [given] service.” *Id.*, 10:44-57, Fig. 6 (annotated); Ex-1002 ¶¶64-66.

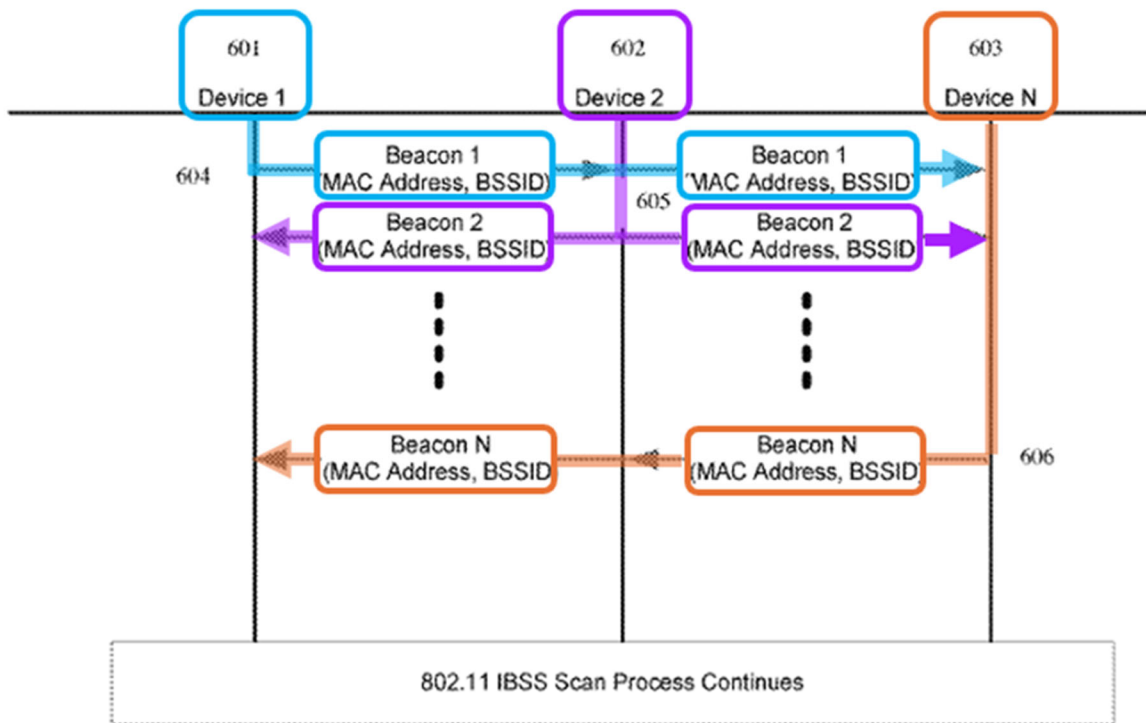


Figure 6 - 802.11 IBSS Beacon Process

VII. PROSECUTION HISTORY OF THE '918 PATENT

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

To overcome written description rejections, the inventor submitted a declaration asserting that the claimed requirement that “beacon transmissions” comprise a “PBSI,” “MAC address,” and “unique identifier” is supported by the specification’s discussion of the “IBSS beacon process” (*i.e.*, Ex-1001, 10:31-11:6,

Fig. 6)—where, in one embodiment, “‘PBSI’ is the BSSID field of the beacon,” and in another embodiment, “‘PBSI’ is the SSID.” *See* Ex-1004 at 1546-1556 (Proctor Decl., ¶¶73-84, 120-124); Ex-1011.

The prior art combinations and arguments in this Petition were not before the PTO during prosecution. Ex-1004; Ex-1002 ¶¶67-70.

VIII. LEVEL OF ORDINARY SKILL IN THE ART

A person of ordinary skill in the art at the relevant time (“POSITA”) 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. Ex-1002 ¶¶25-27.

IX. PRIORITY DATE

For purposes of this proceeding only, Petitioner applies the earliest alleged priority date of the ’918 Patent: September 8, 2008.³ Accordingly, pre-AIA 35 U.S.C. §103 applies and the ’918 Patent was never eligible for PGR.

³ Petitioner respectfully reserves the right to challenge the priority date in other proceedings.

X. CLAIM CONSTRUCTION

Petitioner interprets the claims according to *Phillips*. 37 C.F.R. §42.100(b). To resolve this Petition, Petitioner does not believe that any term requires express construction.⁴ CTPG, 44; Ex-1002 ¶71.

XI. BRIEF DESCRIPTION OF THE APPLIED PRIOR ART

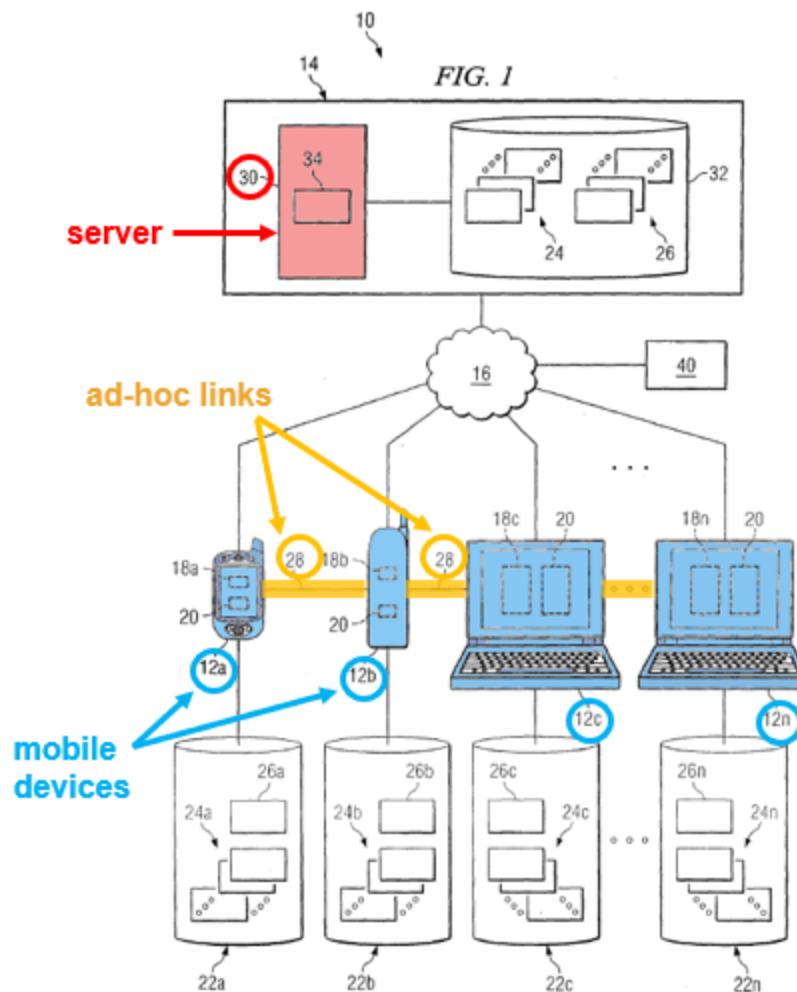
A. Ribaudó (Ex-1007)

Ribaudó (U.S. Patent Publication No. 2007/0030824) was published on February 8, 2007 and is prior art under §102(b).

Ribaudó teaches “a system and method for providing communication services to mobile device users incorporating proximity determination” to facilitate social networking. Ex-1007 ¶¶2, 8. 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.” Ex-1007 ¶6.

⁴ The Samsung litigation is in its infancy and claim construction proceedings have not yet begun. Petitioner respectfully reserves all rights to raise claim construction and other arguments in district court and will request leave to submit the district court’s claim construction as soon as it becomes available. Additionally, should PO raise claim construction arguments in its Preliminary Response, Petitioner will respectfully seek a Preliminary Reply to respond. CTPG, 44-45.

Ribaudo’s system, illustrated in Figure 1, “includes one or more mobile devices 12” (blue) with “links 28” (yellow) indicating “ad-hoc connections between [the] devices,” “a data center 14” that “includes a server system 30” (red), “and a network 16” that connects the mobile devices to the server. Ex-1007 ¶¶15, 34, 66, Fig. 1.



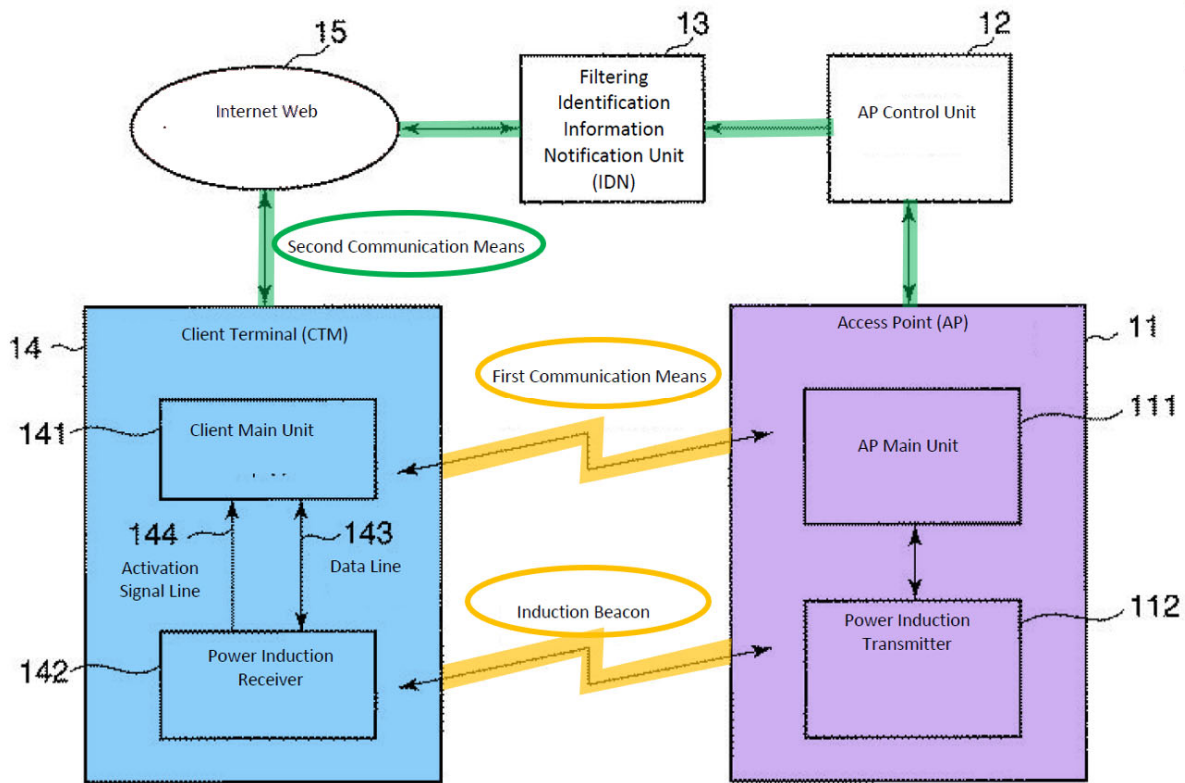
As Ribaudo explains, “a user (e.g., of mobile device 12a) may be associated with one or more client IDs, which may identify the user publicly,” which “may be

the unique MAC address[es] of the Wi-Fi NIC of the user's mobile device[s] 12.” Ex-1007 ¶68. The mobile device “may beacon data such as the client ID of the user associated with [the] mobile device” (Ex-1007 ¶57) and “an SSID” of a proprietor of system 10. Ex-1007 ¶123. Moreover, “[t]he unique MAC address of mobile device 12a may be beacons when the BLUETOOTH interface of mobile device 12a is active.” Ex-1007 ¶157; Ex-1002 ¶¶72-75.

B. Watanabe (Ex-1005, Ex-1006)

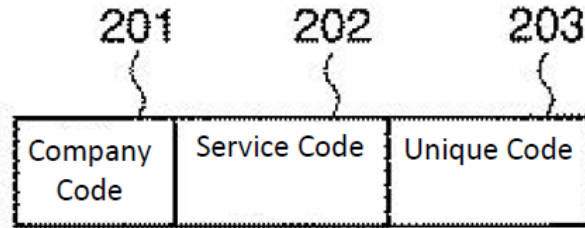
Watanabe (JP Patent Publication No. 2005/12973) was published January 13, 2005 and is prior art to the '344 Patent under 35 U.S.C. §102(b). Watanabe citations herein are to the certified English translation of Ex-1005, attached as Ex-1006.

Watanabe's wireless communication system “reduce[s] power consumption by a mobile terminal when not communicating with an access point.” Ex-1006, Abstract. As shown in Figure 1 below, “client terminal 14” (blue) “communicates with an electronic information device (e.g., server), not illustrated, connected to the network via the access point 11” (purple). Ex-1006 ¶¶12, 53, Fig. 1 (annotated). “Each of the access points 11 has an AP main unit ... 111 as a first communication means” (yellow) “for [short or medium-distance] wireless communication (data communication) with the client terminal 14” (i.e., mobile device). Ex-1006 ¶¶14, 27. Client terminal 14 also has a “second communication means” (green) “for communicating, through the internet 15.” Ex-1006 ¶26.



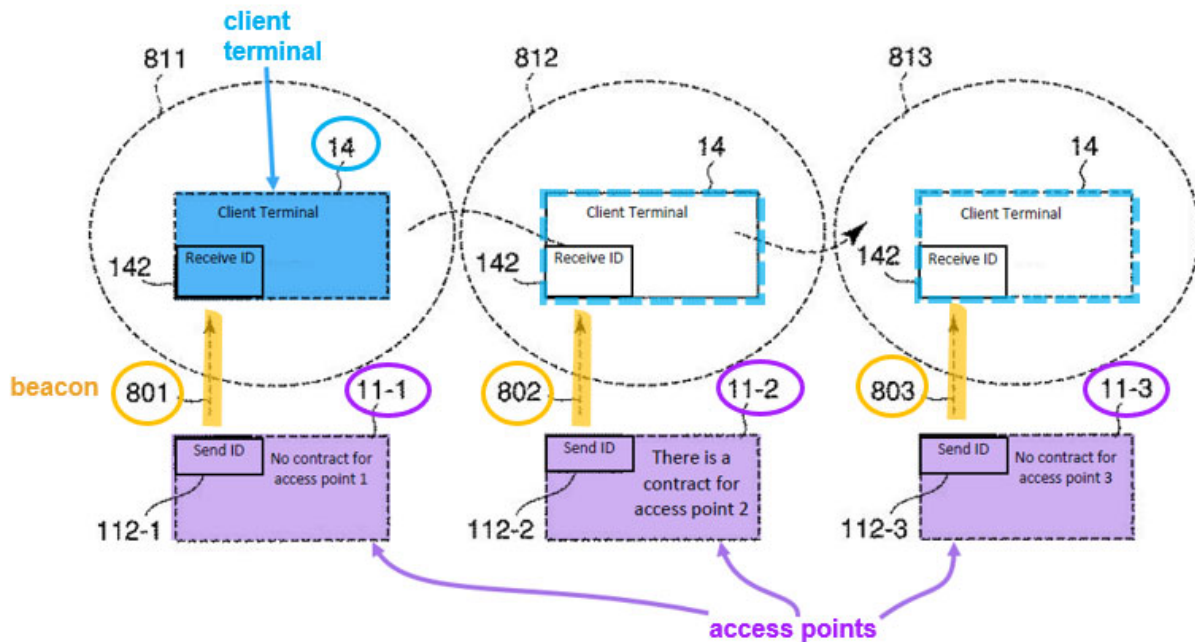
“[E]ach access point 11... generates an induction *beacon* (power supply signal) that uses the first communication means to supply power” and report “transmitter identification information,” which includes a “service code 202 indicating the type of service that can be provided via that access point.” Ex-1006 ¶¶14-15, 49, Fig. 2.

[FIG. 2]



“When the power induction receiver 142 of a client terminal 14 receives the beacon, the transmitter identification information included therein is extracted and compared to identification information for filtering that has been set in advance,” and, “[i]f the comparison result is a match, the client main unit 141 is started up.” Ex-1006 ¶47.

Watanabe’s wireless system is illustrated in Figure 8, where “access points 11-1, 11-2, and 11-3” (purple) “transmit induction beacons 801, 802, and 803” (yellow) “to provide a power supply to the client terminal 14” (blue) “at locations within the areas [811, 812, and 813] that are covered by each” access point. Ex-1006 ¶49; Fig. 8; Ex-1002 ¶¶76-80.



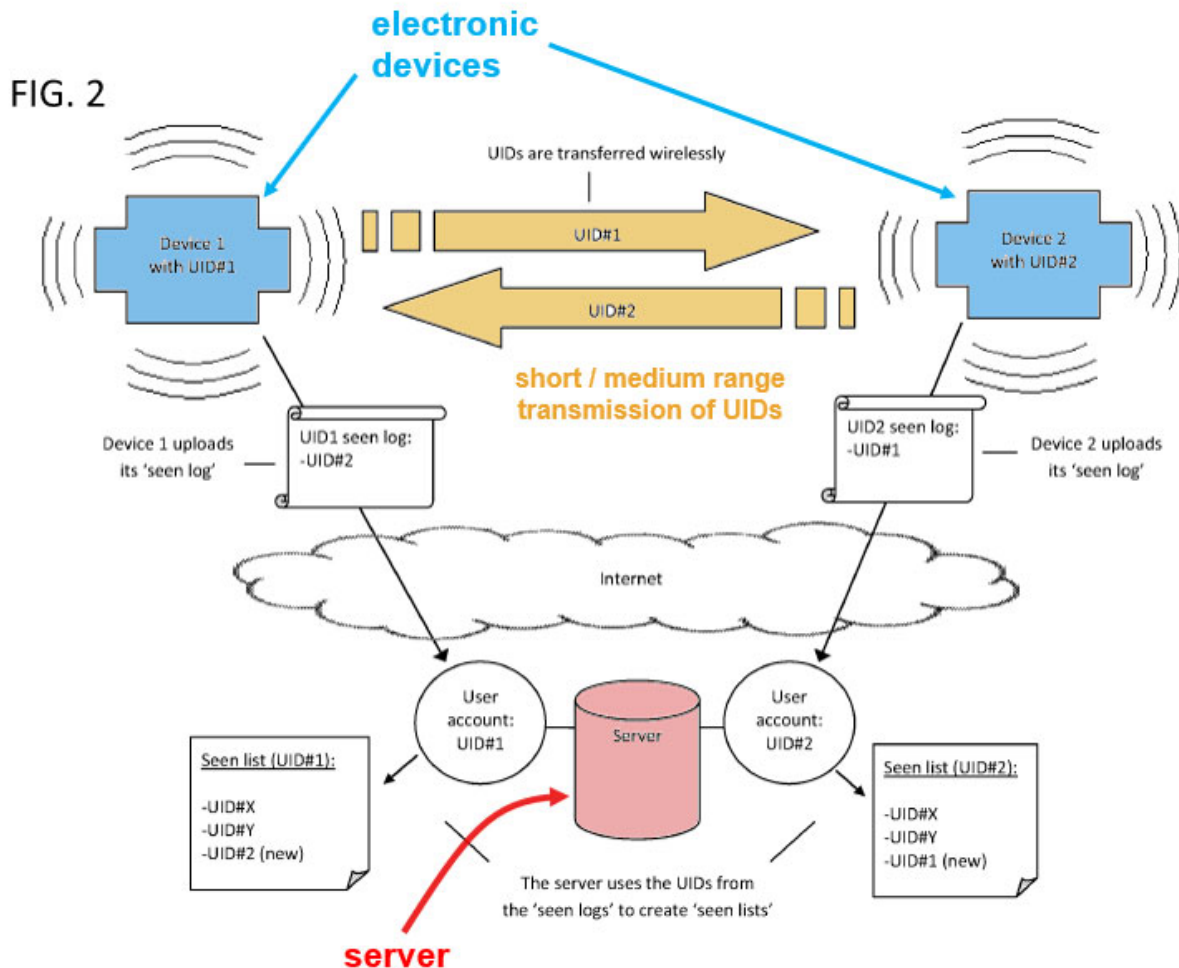
C. Behrens (Ex-1008)

Behrens (PCT Patent Publication No. WO2008/132241) was filed as a PCT application on April 30, 2008, designating the United States, published in English November 6, 2008, and is prior art under §102(e).

Behrens teaches portable electronic devices (mobile phones) that “continuously/repeatedly transmit” and scan for “unique identifiers (UID) via non-directed wireless radio frequency transmission” to establish social networks. Ex-1008, Title, 11:1-5. The UID “contains information for identifying the device (and thus its user).” Ex-1008, 6:6-8. The UID “may consist of or include a MAC (media access control) address, Bluetooth Device Address (i.e., BD_ADDR), or other unique or quasi-unique identifier.” Ex-1008, 11:21-26. Behrens’s system “may even

allow a user to have multiple or changing UIDs and, therefore, different online identities,” which “may also be linked to a single user account.” Ex-1008, 23:1-5.

Figure 2 shows electronic devices (blue) in communication with a server (red), where the “two devices send[] out UIDs” via short- and medium range transmission (yellow). Ex-1008, Fig. 2; Ex-1002 ¶¶81-83.



D. Mgrdechian (Ex-1010)

Mgrdechian (U.S. Patent Publication No. 2005/0174975) was published on August 11, 2005, and is prior art under §102(b).

Mgrdechian discloses a “wireless communication system ... that provides an exchange of information between wireless devices” whose users are “previously unknown” to each other (Ex-1010, ¶¶2-3), where each device exchanges information with a remote server via Internet (*id.*, ¶92), and where the devices communicate with each other via Bluetooth or Wi-Fi, based on “unique identifications” or “unique IDs” stored in a remote database. *Id.*, ¶¶21, 91, 92, Fig. 8 (annotated).

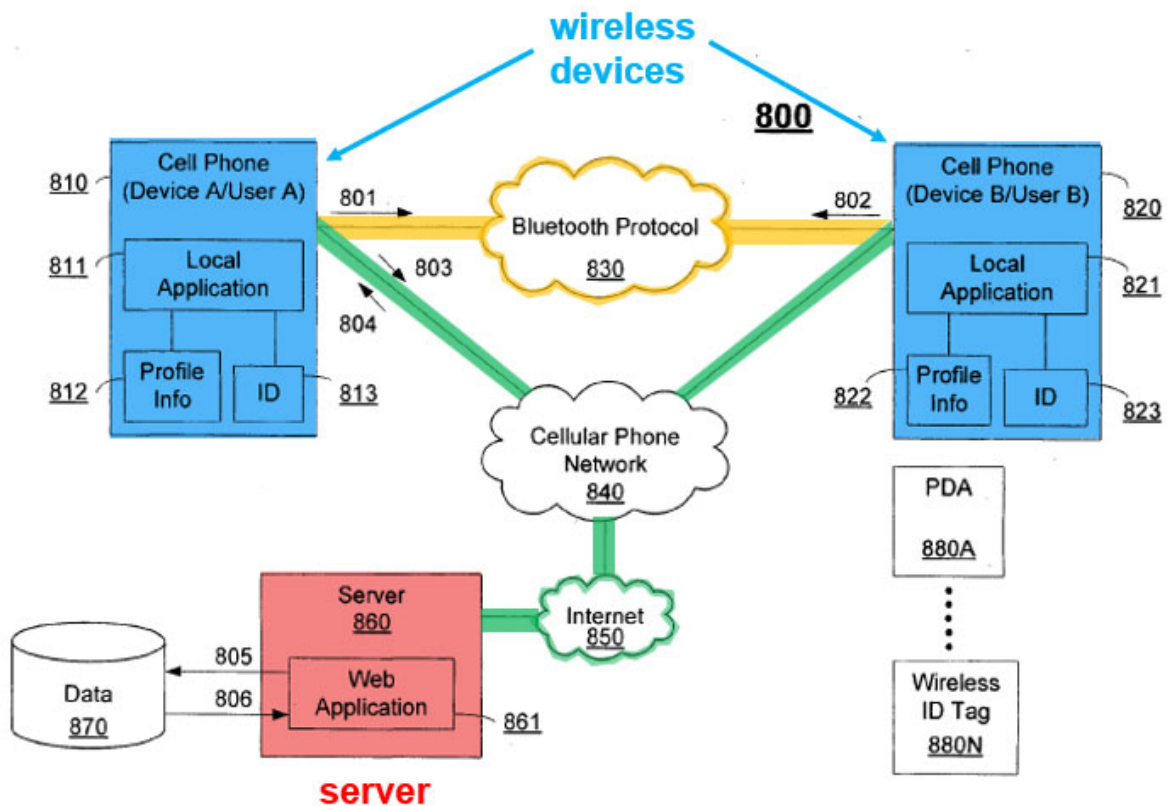


Fig. 8

Mgrdechian’s system can be applied to “gaming applications operating on mobile devices.” Ex-1010, ¶86. Ex-1002 ¶¶84-86.

XII. DETAILED EXPLANATION OF THE UNPATENTABILITY GROUNDS

A. Ground 1: Claims 1, 4-6, 9, 14, 16-20, 22, and 24-30 are obvious over Ribaudó.

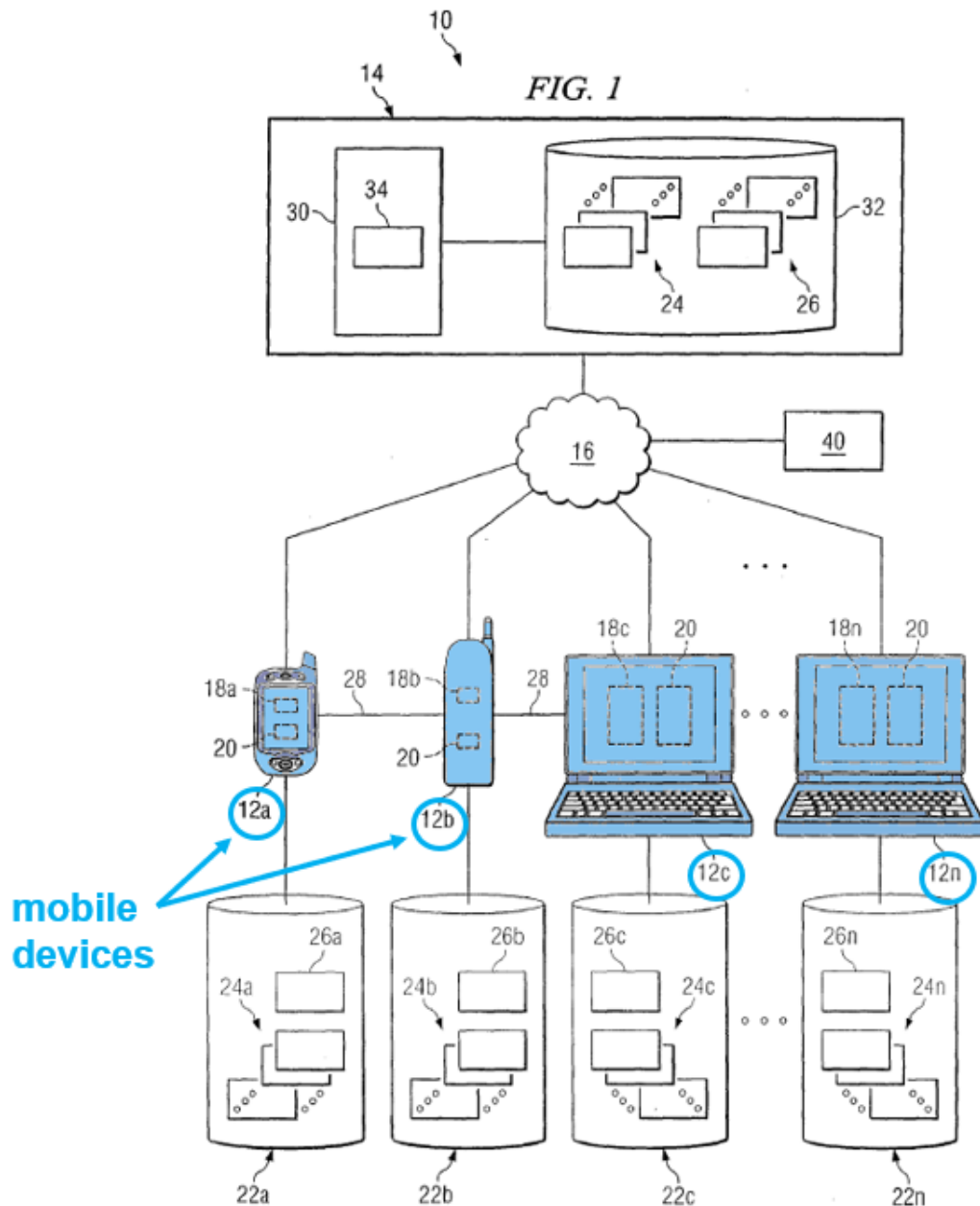
1. Independent Claim 1

a. Element 1[pre]: A mobile wireless device comprising:

Ribaudó teaches⁵ the preamble, to the extent it is limiting. Ex-1002 ¶¶87-88.

Figure 1 of Ribaudó includes “[m]obile devices 12” (blue), where each device (*e.g.*, 12a) “may include one or more suitable devices for wireless communication.” Ex-1007, ¶18; *see also id.*, ¶15, Fig. 1.

⁵ 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 (CCPA, 1981) (“The test for obviousness is...what the combined teachings of the references would have suggested to those of ordinary skill in the art.” (citations omitted)).



b. Element 1[a]: a first radio;

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 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.” Ex-1007, ¶¶18-19, Fig. 1. Further, “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*.” *Id.*, ¶¶24-25. Ribaudó’s system may also “employ a *cellular* connection ... to download from data center 14.” *Id.*, ¶204. Mobile 12a is the recited wireless mobile device, and adapter 18a’s cellular/WWAN radio is the recited first radio. Ex-1002, ¶¶89-90; *see also* Ex-1011 (Proctor Decl.), ¶¶73-89 (explaining how the ’918 specification discloses “first” and “second radio[s]”).

c. Element 1[b]: a second radio;

Further, “[e]ach mobile device 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).” Ex-1007, ¶¶18-19, 205, Fig. 1.

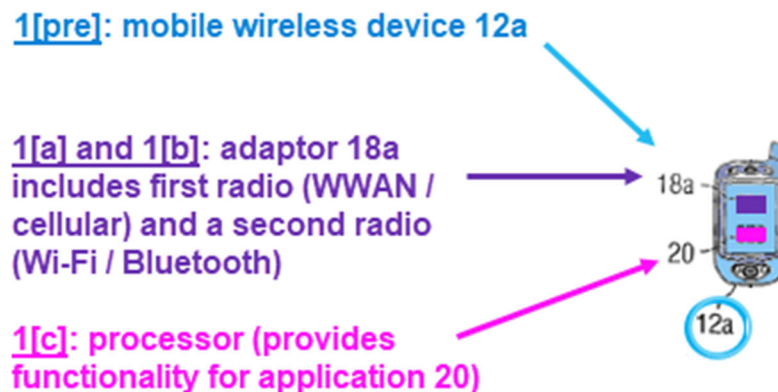
Adapter 18a’s Wi-Fi (or Bluetooth) radio is the “second radio.” Ex-1002, ¶¶91-93; *see also* Ex-1011 (Proctor Decl.), ¶¶73-89.

d. Element 1[c]: one or more processors;

Ribaudó’s mobile devices 12 “each include any suitable *combination of*

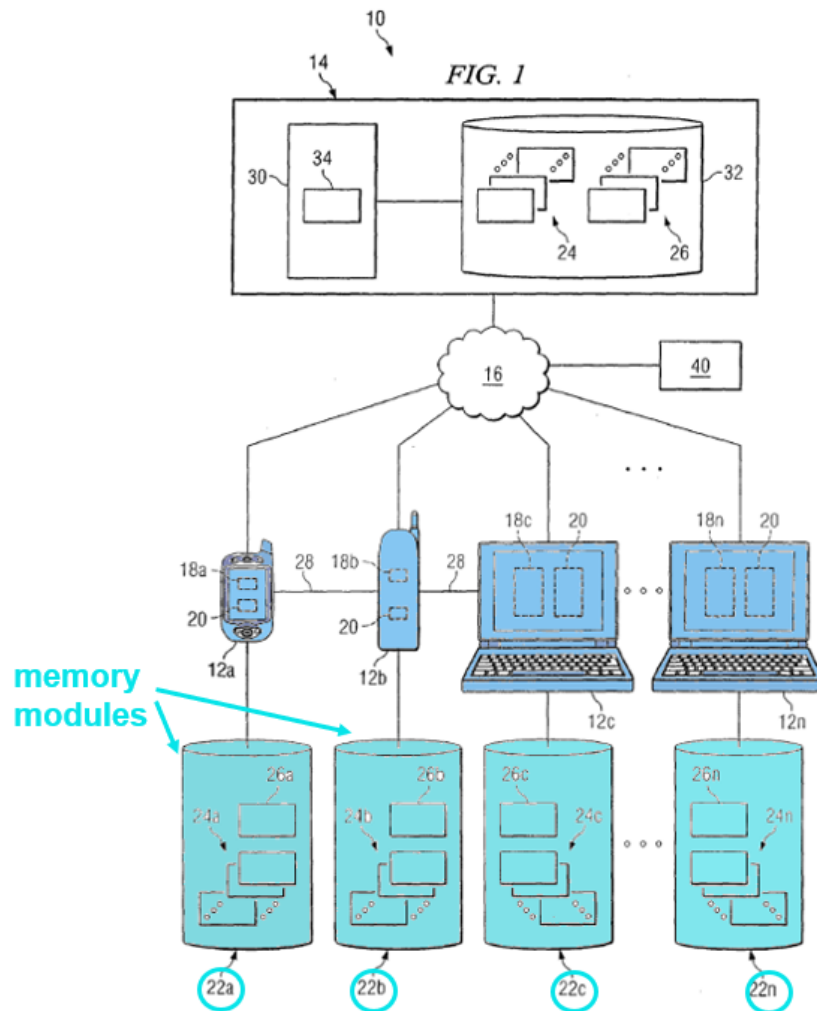
hardware, software, and firmware to provide the functionality described” including “one or more applications 20” to “facilitate communication with other mobile devices 12 (*e.g.*, devices 12b through 12n) and between mobile device 12 and data center 14.” Ex-1007, ¶19. “[T]he user of mobile device 12a launches [an] application 20,” so that “mobile device 12a may be operable to detect other mobile devices 12” based on match data, and “may beacon data such as the client ID of the user ... within any suitable range.” *Id.*, ¶84, Fig. 2.

Accordingly, a POSITA would recognize that the mobile device 12a includes at least one processor (*e.g.*, a microprocessor or microcontroller, programmed with software or firmware) as necessary to provide the described functionality of the application 20. Ex-1002 ¶¶94-97. The mobile device 12a of Figure 1 is annotated below to indicate limitations 1[pre]-1[c]:



- e. **Element 1[d]: one or more memory devices coupled to the one or more processors, the one or more memory devices storing a set of instructions that when executed by the one or more processors cause the one or more processors to perform operations including:**

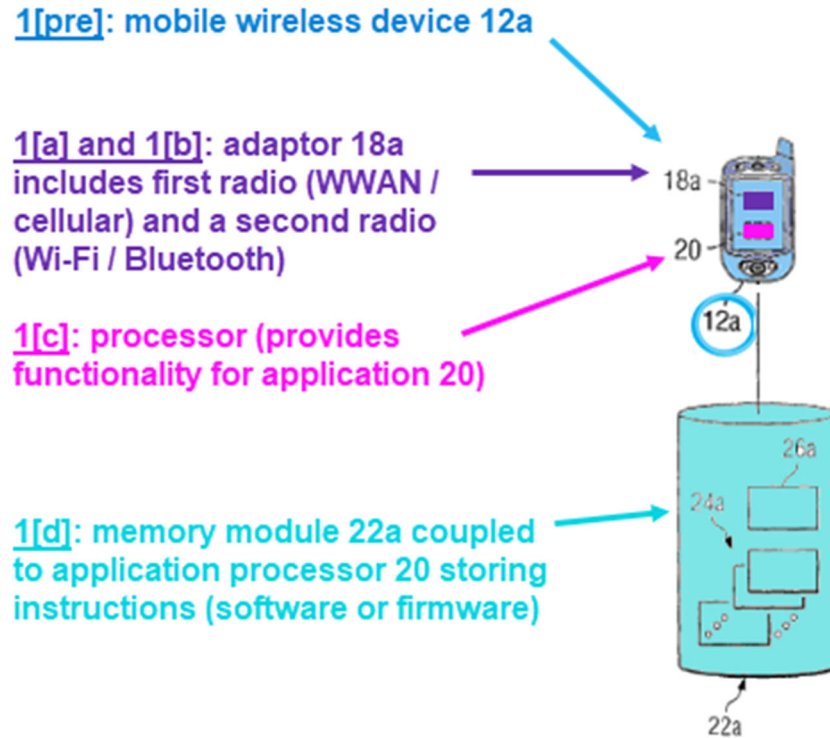
Ribaudo's "[m]obile devices 12 may each have an associated memory module 22"—or "any suitable memory modules 22 according to particular needs"—that may be "operable to store data as one or more compressed binary files." Ex-1007, ¶32; Fig. 1.



Specifically, “[m]emory module 22 may store various data associated with the user of mobile device 12,” including “one or more user profiles 24 for the user of mobile device 12[,] ... match data 26 downloaded from data center 14 and identifying one or more predetermined matches for the user[, and] ... any other suitable information, according to particular needs.” Ex-1007, ¶33; *see also id.*, ¶84 (describing the operations performed by mobile device 12 in connection with the communication services method of Figure 2, including detecting other devices and beaconing data).

Memory module 22 also stores software instructions for performing the functions described below. Ex-1007, Claim 31 (directed to “[s]oftware for proximity determination, the software being embodied in a computer-readable medium and when executed, operable to” perform the claimed functions).

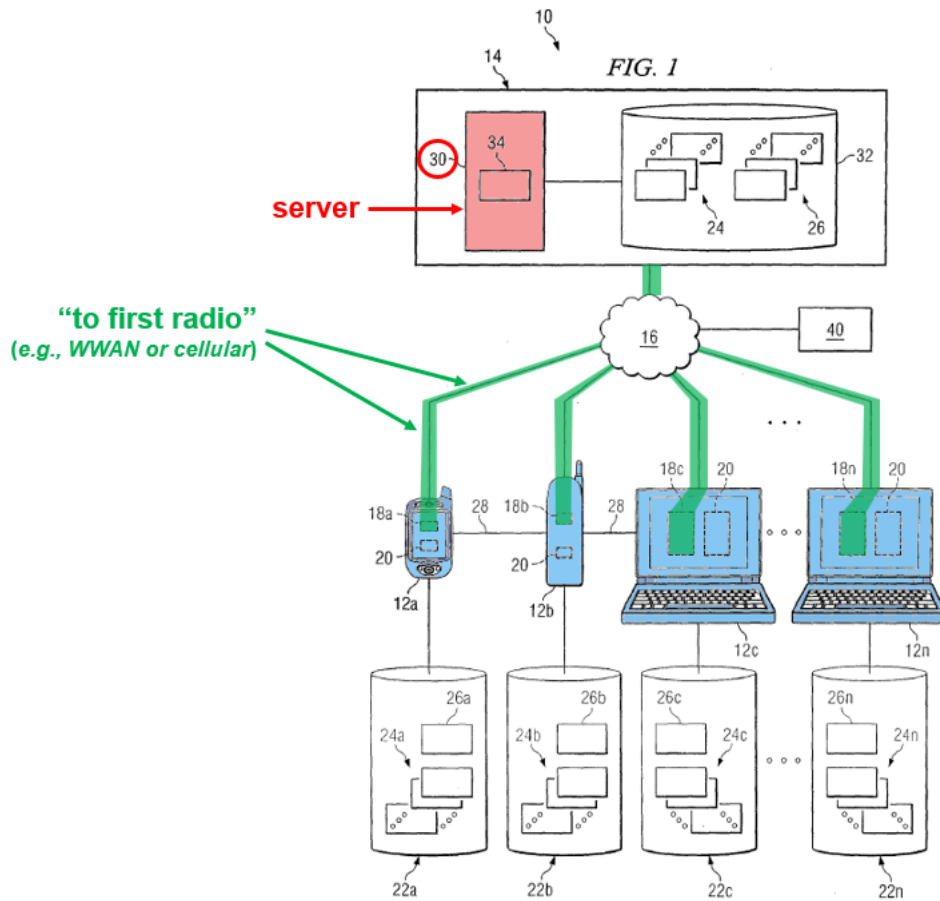
Accordingly, as depicted below, a POSITA would have recognized that the mobile device 12a includes a memory module 22 that is coupled to one or more processors (for running application 20), and that stores a set of software instructions that when executed by the processors, cause the processors to perform the communication services operations described further below. Ex-1002, ¶¶98-102.



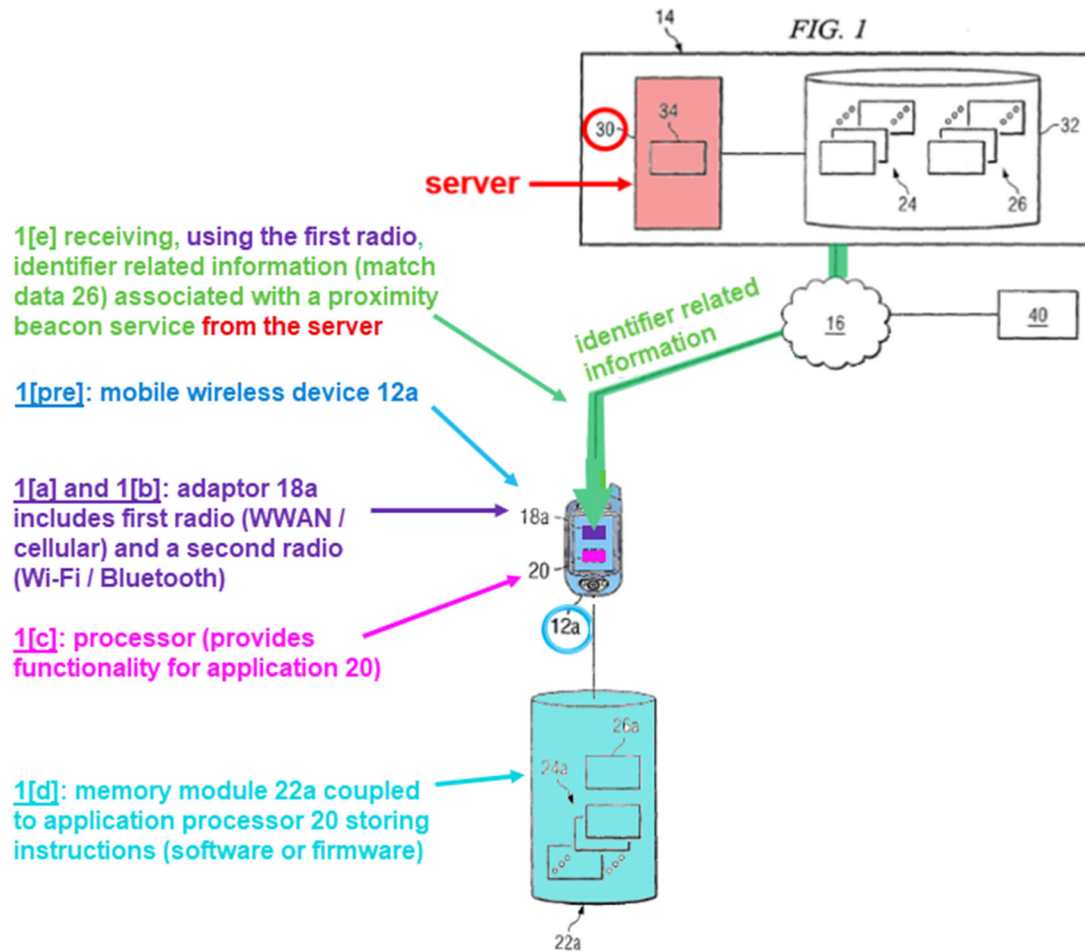
- f. **Element 1[e]: receiving, using the first radio, identifier related information associated with a proximity beacon service, from one or more servers;**

Ribaudo's "[d]ata center 14 includes a server system 30" (red) as shown in

Figure 1. Ex-1007, ¶34, Fig. 1.



Ribaudo’s data center “*transmit[s] to each user match data* containing match identifiers and other information for the other users determined to be matches for the user. This *pre-processed match data* for the user is stored locally on the user’s mobile device 12.” Ex-1007, ¶16, ¶33 (“memory module 22 may store match data 26 downloaded from data center 14 and identifying one or more predetermined matches for the use.”); *see also id.*, ¶53. Further as depicted below, Ribaudo teaches the user’s mobile device receives the transmitted match data via the first radio (i.e., via WWAN or cellular). Ex-1007 ¶24.



Further, Ribaudo’s match data is “identifier related information.” 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 (and possibly the user’s availability level and other identification information, such as trust score and status). This beamed data may be broadcast within any

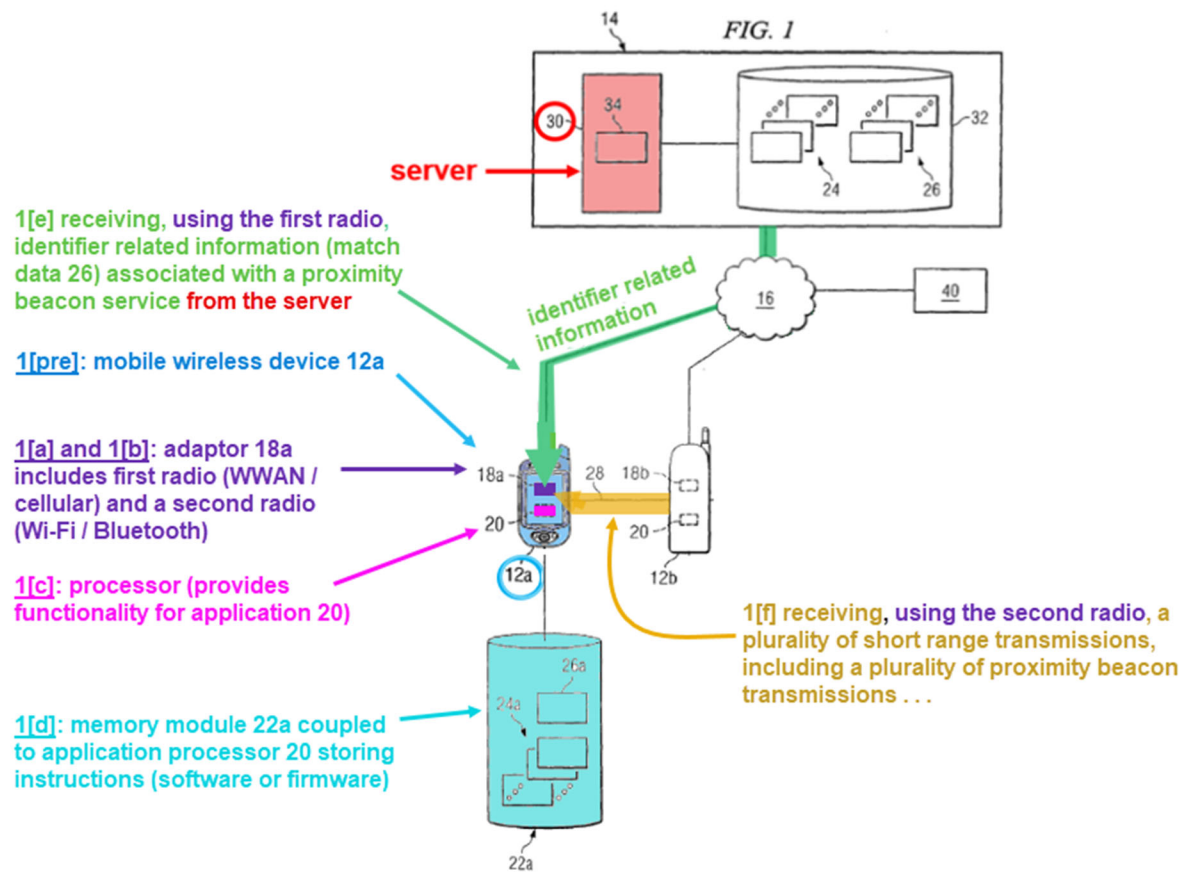
suitable range, depending on the technology being employed.” Ex-1007, ¶57; *see also id.*, ¶¶123, 157, 173 (further describing beaconing by mobile devices 12).

Finally, this pre-processed match data is “associated with” a proximity beacon service given that the mobile device uses the match data “to detect *in proximity* other mobile devices that may be associated with a user who is a potential match,” and does do by “*beacon[ing] data* ... within any suitable range,” Ex-1007, ¶57, and given that the match data relates to “commonalities or other reasons for interacting” between two users of a given internet service (e.g., online dating). *See id.*, ¶¶29, 97-105; Ex-1002, ¶¶103-107.

- g. **Element 1[f]: [1] receiving, using the second radio, a plurality of short range transmissions, including a plurality of proximity beacon transmissions when the device is located within a detection range of one or more beacon transmitter devices associated with the proximity beacon service, [2] each of the proximity beacon transmissions including a respective MAC address, a respective unique identifier, and a Proximity Beacon Service Identifier (PBSI);**

Ribaudo’s mobile devices receive proximity beacon transmissions from other mobile devices that are located within a detection range. Ribaudo explains that “mobile devices 12 are operable to *detect in proximity other mobile devices 12 that may be associated* with a user who is a potential match. ... Mobile device 12 may *beacon data* such as the client ID of the user associated with mobile device 12 (and possibly the user’s availability level and other identification information, such as

trust score and status). As depicted below, 12b may be an “other mobile device[]” in the detection range. The Wi-Fi or Bluetooth radio (i.e., second radio) of mobile device 12a receives short range transmissions from mobile device 12b, and such beaconing is performed using short-range transmissions. “In Fig. 1, links 28” (below, yellow) “illustrate example ad-hoc connections between mobile devices 12,” in which “***Wi-Fi technology*** may be used to implement the detection process. ... Additionally or alternatively, ... mobile devices 12 may use ***BLUETOOTH technology*** to detect matches in proximity.” Ex-1007, ¶66, Fig. 1.



“This *beaconed data may be broadcast within any suitable range*, depending on the technology being employed.” Ex-1007, ¶57; *see also id.*, ¶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. Ex-1002, ¶111.

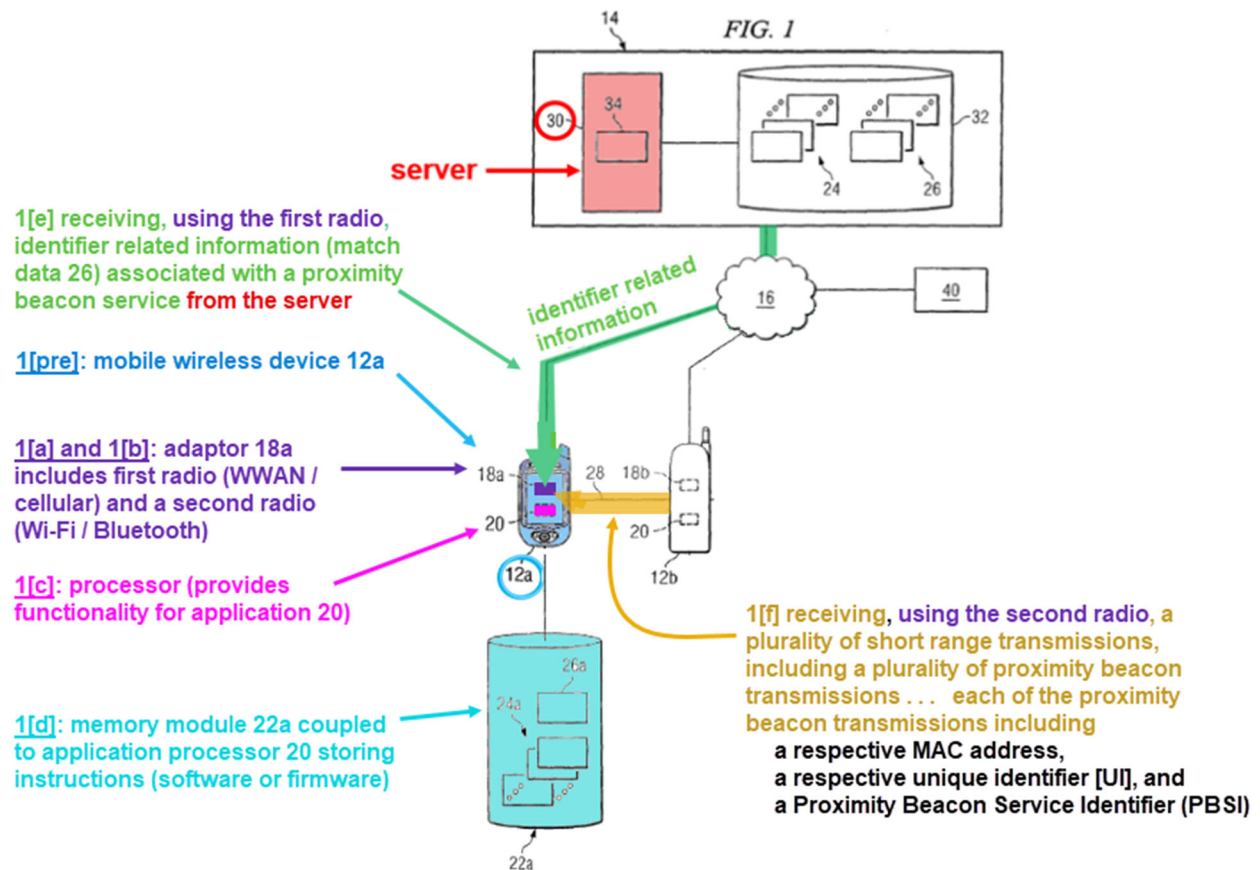
Finally, there are a plurality of such short-range, proximity beacon transmissions. A POSITA would have understood Ribaudó’s explanation that

“[m]obile devices 12 may **beacon** data that can be used to identify them,” Ex-1007, ¶191, along with Ribaudó’s disclosure that Wi-Fi and Bluetooth are the standards used for proximity detection, Ex-1007, ¶66, as teaching that each mobile device transmits **a plurality of** short-range, proximity beacon transmissions, Ex-1002 ¶112. This is because Wi-Fi and Bluetooth beacons are well-known to POSITAs as periodic signals (sent a plurality of times). Ex-1002 ¶¶113-114 (citing Ex-1025 at 420 (“Beacon interval”); Ex-1026 at 131-132 (“beacon train”)). Ribaudó confirms this, explaining 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,” Ex-1007, ¶148, which teaches that John’s device **receives a plurality of** short-range, proximity beacon transmissions. Ex-1002, ¶¶108-116.

Ribaudó also teaches Element 1[f][2]. As shown below, Ribaudó further teaches that each of the proximity beacon transmission include a MAC address, unique identifier, and Proximity Beacon Service Identifier (“PBSI”), as follows:

Claim Element	Ribaudó
“MAC address”	MAC address of transmitting device (12b)
“Unique identifier”	client ID and potentially other suitable information for uniquely identifying a user (12b) ⁶
“PBSI”	SSID of the proprietor of the system (10)

⁶ As discussed below, Ribaudó contemplates that, in addition to “client ID”, other suitable information can be used to uniquely identify a mobile device user.



MAC address: As Ribaudo 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.” Ex-1007, ¶21; *see also id.*, ¶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. Ribaudo further discloses that “[t]he *unique MAC address* of

mobile device 12a *may be beacons* when the BLUETOOTH interface of mobile device 12a is active.” Ex-1007, ¶157. Although specifically referencing device 12a, a POSITA would understand Ribaudó as teaching that each of the other mobile devices (12b, 12c, etc.), may likewise beacon its unique MAC address. Ex-1002 ¶118.

Unique identifier: Ribaudó 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).” Ex-1007, ¶57; *see also id.*, ¶84 (same). Ribaudó 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.” Ex-1007, ¶¶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 information included in Ribaudó’s beacons that uniquely identifies a user, is thus a “*unique identifier*.” Ex-1002, ¶119.

Proximity Beacon Service Identifier (“PBSI”): The term “PBSI” is not a term of art, but in the context of the ’918 Patent, its plain and ordinary meaning encompasses Ribaudó’s “SSID.” For example, Ribaudó discloses that “[i]n ad hoc mode, in certain embodiments, application 20” of a mobile device “may beacon an *SSID of ‘proprietor_name.net’* (e.g., where ‘proprietor_name’ corresponds to the name of a proprietor of system 10).” Ex-1007, ¶123.

Ribaudó’s “SSID of ‘proprietor_name.net’” corresponds to the claimed PBSI for several reasons. *First*, Ribaudó itself teaches that the “proprietor_name.net” may be associated with a particular service—for example, where the proprietor is an online dating platform, the SSID itself may be associated with, and therefore identify, one more services provided by such a proprietor (e.g., providing dating matches). *See, e.g.*, Ex-1007, ¶¶97-104 (discussing “dating” related services). *Second*, as discussed in Section VII above, during prosecution, the inventor of the ’918 Patent submitted a declaration explaining that the claimed “PBSI” may be satisfied by an SSID, citing the specification’s description that “the SSID may be used to indicate that these particular beacons are associated with a service.” Ex-1011 (Proctor Decl.), ¶124, Ex-8, n.5; Ex-1001, 10:52-59; Ex-1002 ¶¶117-122.

- h. Element 1[g]: determining if a particular short range transmission of the plurality of short range transmissions a) includes a MAC address, and b) includes the proximity beacon service identifier (PBSI) and if c) the PBSI indicates the particular short range transmission is a proximity beacon transmission associated with the proximity beacon service; then:**

Ribaudo teaches *determining* if a mobile device received certain identifiers from another mobile device: “a first user’s mobile device detects the presence of a second user’s mobile device in proximity based on *network identifiers* communicated from the mobile devices of the first and second users,” and that this detection is achieved by “*processing* the [received] network identifiers.” Ex-1007, ¶7; *see also id.*, ¶6, cl. 1. An example of such network identifiers is “MAC address.” *E.g.*, Ex-1007, ¶¶117 (“network identifiers (e.g., MAC addresses)”), 186-188, 194, 197. Further, a POSITA would have understood Ribaudo as teaching that an SSID (i.e., the PBSI identified for Element 1[f] above) may also be a “network identifier,” since Ribaudo explains that “SSIDs ... *represent* one or more network identifiers,” and “provide ‘human readable versions of MAC addresses or other network identifiers.” Ex-1007, ¶213.

As discussed for Element 1[f] above, Ribaudo teaches that these identifiers are received via short range transmission in the form of a Wi-Fi or Bluetooth beacon. *E.g.*, Ex-1007, ¶¶66, 142, 157, Fig. 1.

Ribaudo's mobile device "***compares***" the identifiers received via beacon transmission "with the pre-processed match data stored on the user's mobile device" in order to determine matches. Ex-1007, ¶6; *see also* cl. 9 ("comparing the *one or more network identifiers* receiving from the first mobile device to the plurality of network identifiers received from the plurality of other mobile devices."). Ribaudo's teaching of "processing" and subsequently "comparing" network identifiers entails ***determining that such identifiers (MAC and PBSI) are present*** in the beacon transmission. Ex-1002, ¶126.

Finally, in Element 1[g], "c)" the PBSI would indicate that the particular short range transmission is a proximity beacon transmission associated with the proximity beacon service, as required. Ribaudo teaches that a mobile device "SSID of ***may beacon an SSID*** of 'proprietor_name.net' (e.g., where 'proprietor_name' corresponds to the name of a proprietor of system 10)." Ex-1007, ¶123. Thus, Ribaudo's disclosure of the SSID indicates reception via beacon from another device. Further, as discussed for Element 1[f], the SSID itself may be associated with, and therefore identify, one more services provided by a given proprietor. *See, e.g.*, Ex-1007, ¶¶29, 55, 97-104, 162, 223, 226; Ex-1002, ¶¶123-128.

- i. **Element 1[h]: determining if an entity or object associated with the proximity beacon service is in proximity to the mobile wireless device by utilizing the identifier related information and the unique identifier.**

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

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

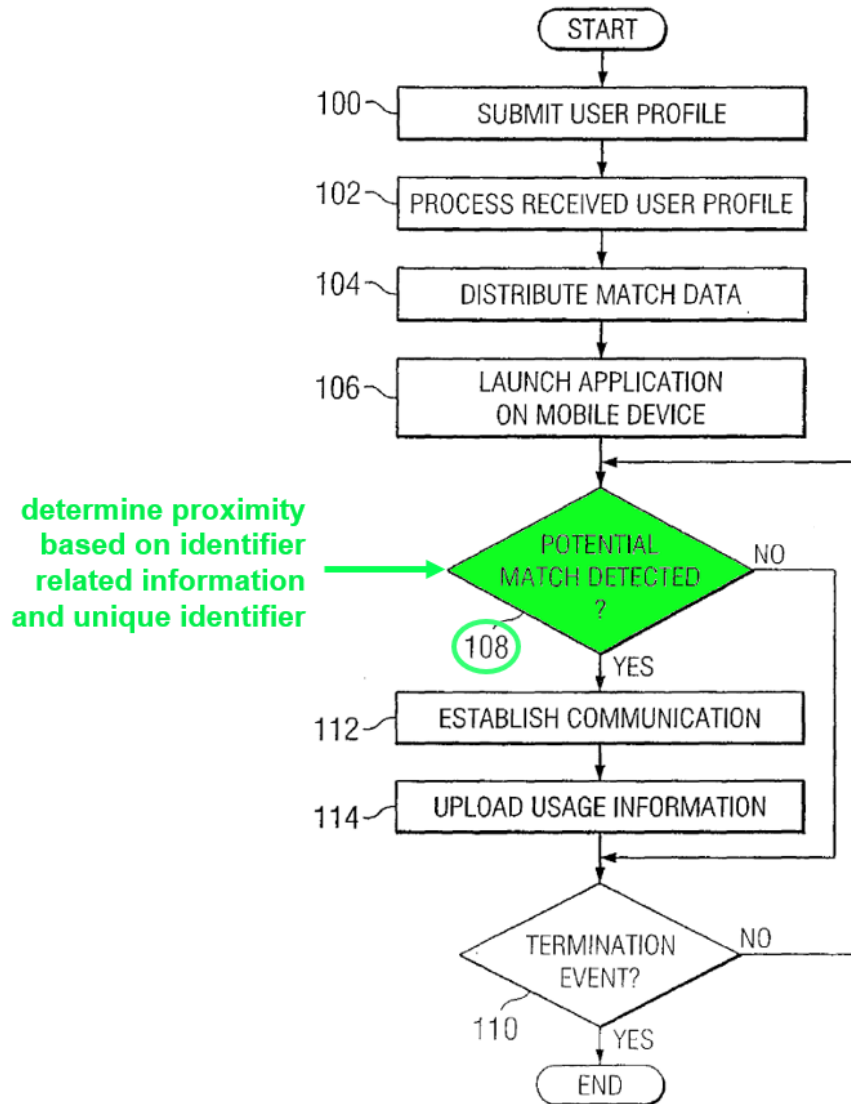
Ribaudo explains that “when the user is in proximity to another user, the user’s mobile device detects the presence of the other user’s mobile device, *receives an identifier associated with the detected other user, and compares* the received identifier *with the pre-processed match data* stored on the user’s mobile device to determine whether the other user is one of the user’s predetermined matches. ... [T]his detection of another user in proximity and determination of whether another detected user is a match is performed locally on the user’s mobile device.” Ex-1007, ¶6; *see also id.*, ¶16 (same).

In Ribaudó's Figure 2, "a user of mobile device 12a submits a user profile 24a to data center 14," which then "pre-processes the information ... to generate match data 26 for the user," and then "distributes the generated match data to one or more appropriate mobile devices 12." Ex-1007, ¶¶80-83, Fig. 2. As shown below, "[a]t step 106, the user of mobile device 12a launches application 20[,]" which:

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

Ex-1007, ¶84.

FIG. 2



Finally:

At step 108, *mobile device 12a determines whether a match is detected in proximity*. ... The detection process may be used, for example, so that a user's mobile device 12 becomes aware that another client ID is on the same or a different network subnet and/or within wireless

proximity. ... [W]hen mobile device 12a *detects another client ID* (or other suitable identifier indicating a potential user of system 10), mobile device 12a may *consult match data 26a to determine* whether the user associated with the detected client ID is identified in the match data 26a for mobile device 12a.

Ex-1007, ¶85; *see also id.*, ¶148 (explaining how to determine whether Steve and Mary are in proximity).

Accordingly, Ribaudó's mobile device determines whether an entity (*i.e.*, user of another mobile device) associated with a proximity beacon service is in proximity, on the basis of pre-processed match data received from the data center ("identifier related information"), and the user's client ID (the "unique identifier"). Ex-1002, ¶¶129-135.

2. Independent Claim 9⁷

- a. **Element 9[pre]: A method for facilitating the use of proximity beacons, the method executing within a mobile device, and the method comprising:**

See Elements 1[pre], 1[c], 1[d], and 1[e] above. Ex-1002 ¶136.

- b. **Element 9[a]:**

See Elements 1[a] (first radio) and 1[e] above. Ex-1002 ¶137.

⁷ The limitations of claim 9 closely map to the limitations of claim 1, as indicated below.

c. Element 9[b]:

See Elements 1[b] (second radio) and 1[f] above. Ex-1002 ¶138.

d. Element 9[c]:

See Element 1[g] above. Ex-1002 ¶139.

e. Element 9[d].

See Element 1[h] above. Ex-1002 ¶140.

3. Dependent Claims 4-6, 14, 16-20, 22, and 24-30

- a. Claim 4: The mobile wireless device of claim 1, wherein the one or more processors further execute the instructions to perform operations including: further determining that at least one beacon transmitter device associated with the proximity beacon service is in proximity to the mobile wireless device, by utilizing an action function including one or more previously downloaded unique identifiers.**

As discussed for Elements 1[f] and 1[h], Ribaudo teaches that a mobile device (a “beacon transmitter device”) broadcasts a client ID and potentially other suitable information to uniquely identify a user (a “unique identifier”), which is then received and used by another mobile device “to detect a match in proximity.” Ex-1007, ¶¶46, 57.

Ribaudo further teaches that proximity determination may be made at a later time, based on previously downloaded unique identifiers:

[U]sers of system 10 may communicate at a later time based on a previous match. For example, when a match occurs, the match may be

logged even if the user does not wish to be notified in real time of the match. Many users may not take action at the time of the encounter. This may be referred to as a missed encounter, ... [which] may be logged with ... the *client ID of the matched user* ... and any other suitable information.”

Ex-1007, ¶¶151-152.

The term “action function” is not a term of art, but a POSITA would have understood Ribaud as teaching that this subsequent determination by the receiving device (e.g., that the beacon transmitting device associated with the proximity beacon service is in proximity) utilizes an “action function including [a] previously downloaded unique identifier[]” in that—since the client ID (e.g., unique identifier) of the matched user has already been logged (i.e., previously downloaded), Ex-1007, ¶¶151-52—the receiving device has no need to re-request such identifiers from the server. This understanding is consistent with the inventor’s explanation, during prosecution, that “an ‘action function’ can be used to reduce the frequency of re-requests to the server, for example, by not submitting a subsequent request to the server for identifiers that have already been passed (for a period of time).” Ex-1011 (Proctor Decl.), ¶134. Ex-1002, ¶¶141-144.

- b. **Claim 5: The mobile wireless device of claim 1, wherein the one or more processors further execute the instructions to perform operations including determining, based upon at least a portion of the identifier related information, that at least one beacon transmitter is a broadcast device having a predetermined location.**

Ribaudo's device 12a determines, based on preset match data ("identifier related information"), that at least one beacon transmitter (e.g., mobile device 12b) is a broadcast device having a predetermined location:

a user may tag particular locations based on hardware signatures such as *network identifiers* (e.g., MAC addresses) associated with one or more networks at the location. ... [T]agged information for a particular location may be pre-populated with a default value of the SSID being broadcast by that location (e.g., "T-MOBILE" or "RADISSON Wireless"). A user may be able to add tags to this default tag that may include more useful information about the location, such as "CES-ConferenceRoom4," "MainStreetCafe," "DFWAirport-Terminal3," This additional tagged information may provide a more relevant descriptor for the location than the default tag assigned based on the SSID.

Ex-1007, ¶117; *see also id.*, ¶212.

Ribaudo further discloses “implied proximity,” which involves “distribut[ing] pre-processed matches to members of a particular group *at a particular location* and/or time”—*e.g.*, “a conference, a cocktail party, a speed-dating event, ... or any other suitable gathering of users that is known or scheduled in advance.” Ex-1007, ¶160. And “match data 26 may be sent to some or all users who are members of a particular group at a particular time or location, when two group members come within proximity of each other at the event, when group members come within proximity of each other and another group member, or in any other suitable manner.” *Id.*, ¶163; Ex-1002, ¶¶145-147.

- c. **Claim 6: The mobile wireless device of claim 1, wherein the identifier related information comprises application software for execution upon the mobile wireless device, and the one or more processors further execute the instructions to perform operations including sending of the unique identifier by the mobile wireless device to at least one server of the one or more servers; and in response to the sending of the unique identifier, downloading the application software.**

Ribaudo’s “identifier related information” comprises application software, which is downloaded in response to sending the unique identifier to at least one server. First, Ribaudo states that “a user may also download and install application 20 on the user’s mobile device,” Ex-1007, ¶81, in which case the “identifier related information” that is received via the first radio comprises application software in addition to match data.

Second, Ribauda teaches a “second user may *enter an identifier of another user* (e.g., the first user) such as an email address, telephone number, name, username, instant messaging screen name, or other suitable information for identifying the first user *into the web site associated with data center 14* (and possibly the proprietor of system 10) to view what the second user shares in common with the first user. ...[O]ne or more plug-ins may be added to existing or newly developed applications (e.g., instant-messaging applications, email applications, telephone applications, or any other suitable applications). For example, if a first user sends a second user an email, instant message, or VoIP call, then the plug-in may display what the first and second users share in common.” Ex-1007, ¶140.⁸ Further, as discussed for Element 1[e], the data center contains a server. Ex-1007, ¶34, Fig. 1. Ex-1002 ¶¶148-150.

⁸ Similarly, during prosecution, the inventor explained the language recited in Claim 6 by referring to the specification’s example of a museum patron whose “device 202 receives an identifier from the museum’s broadcast device 204,” then “passes that identifier ‘for’ the museum device [204] to the server 100,” which “then *passes relevant information back to the user’s device*’. The content passed back can include ‘text, pictures, web pages, and *application software such as games, informative display applications or other content.*’” Ex-1011 (Proctor Decl.), ¶¶104-107 (emphases original).

- d. **Claim 14/19: [The mobile wireless device of claim 1, wherein the instructions further comprise/The method of claim 9, additionally comprising]: sending the unique identifier, using the first radio, to at least one server of the one or more servers, and receiving further information relating to an object or entity associated with being within proximity to the mobile device.**

Ribaudo's mobile device user may send a unique identifier associated with another mobile device and/or user, via the first radio (e.g., cellular or WWAN link) to the server, and thereafter receives *further information* (e.g., sales communications) relating to an entity (e.g., merchant) associated with being within proximity to the mobile device. Specifically, Ribaudo teaches that a "second user may *enter an identifier of another user* (e.g., the first user) such as an email address, telephone number, name, username, instant messaging screen name, or other suitable information for identifying the first user *into the web site associated with data center 14* (and possibly the proprietor of system 10) to view what the second user shares in common with the first user. ... *[S]ales people may use this capability to facilitate sales initiated by emails or other forms of communication*. For example, the email or other communication may increase the chances of a response by allowing the recipient to view what he shares in common with the sales person. Providing this rapport with a prospective client may increase the likelihood of making a sale." Ex-1007, ¶140; *see also id.*, ¶34, Fig. 1 (indicating that data center 14 contains a server 30).

The “*further information*” may be user-targeted advertisements: “[d]ata center 14 may collect and store content generated by users of mobile devices 12. For example, data center 14 may associate the URLs of a user’s web log, photos, podcasts, *personal advertisements, classified advertisements, advertisements*, and other suitable content to the MAC addresses and cell tower IDs that the user encounters.” Ex-1007, ¶215. And “[t]he information gathered for each wireless access point (e.g., attribute information of users who pass by the wireless access point) may enable advertisers to advertise on specific wireless access points (e.g., MAC addresses or cell tower IDs) that have the demographics or the usage that the advertiser is targeting for its ads or other offers.”⁹ Ex-1007, ¶217; Ex-1002 ¶¶151-153.

- e. **Claim 16/24: [The mobile wireless device of claim 1, wherein the instructions further comprise/ The method of claim 9, additionally comprising:] controlling further communications between the mobile device and at least one device or server associated with an entity or object in proximity to the mobile device.**

Ribauda teaches “controlling further communications between the mobile device and at least one device or server associated with an entity” in proximity, for

⁹ The ’918 Patent similarly discusses, in connection with using a central server to broker transactions between peers, “customiz[ing] delivered content to include elements such as advertising or other content customized to the recipient based on additional information such as known personal purchasing history, or interests.” Ex-1001, 4:12-28.

example, in advertising. *See, e.g.*, Ex-1007, ¶140 (“[S]ales people may use this capability to facilitate sales initiated by emails or other forms of communication. For example, the email or other communication may increase the chances of a response by allowing the recipient to view what he shares in common with the sales person. Providing this rapport with a prospective client may increase the likelihood of making a sale.”); ¶217 (“[A]dvertisements, 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). ... Data center 14 or another suitable component of system 10 may create a feedback loop similar to a cookie, which may be used to attach a user’s preferences, purchasing patterns, destinations, and other personalized information to suitable wireless access points (e.g., MAC addresses or cell tower IDs).”).

Ribaudo also discloses “controlling further communications” using a “field ID”:

The field ID may be included within a match ID ... to abstract specific data in a user profile 24 so that this specific data can be distributed inside a match ID to other, matched, users without disclosing the data that was input. For example, if data center 14 matched the user of mobile device 12a with the user of mobile device 12b, then when a detection event occurs between mobile devices 12a and 12b (e.g., the

mobile devices 12 detect each other in proximity and recognize that they have been determined to be a match), the field ID may be used to display to the user of mobile device 12b the matched value from the user profile 24a of the user of mobile device 12a.

Ex-1007, ¶47.

Ribaudo further discloses “controlling further communications” based on user preferences (e.g., “blocking”), *see, e.g.*, Ex-1007, ¶¶47, 101, or based on location or time. *See, e.g., id.*, ¶¶117, 160, 163; Ex-1002, ¶¶154-157.

- f. **Claim 17: The method of claim 9, further comprising: receiving, using the first radio, access code information by the mobile device from at least one of the servers; and utilizing the access code information to gain access to the entity or object determined to be in proximity to the mobile device.**

Ribaudo discloses:

Hashing may be used to authenticate a matched user and to prevent the unauthorized alteration of the match ID. Hash values may be generated by data center 14 for the users associated with the match ID ... [A]fter the match IDs are generated, hash values are applied to the match IDs. *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. When a match is detected between users of mobile

devices 12a and 12b for example, a new hash value may be calculated on each of the user's mobile devices 12a and 12b. For example, *mobile device 12a* may calculate a new hash value for the match ID associated with the user of mobile device 12b and *may send this new hash value to mobile device 12b to be compared with the original hash value* that the user of mobile device 12b *received from data center 14 for the user of mobile device 12a*. This may allow a determination to be made with respect to whether the match ID has been altered.

Ex-1007, ¶52.

Thus, the “original hash value” that a mobile device user received from the data center (e.g., server) qualifies as “access code information ... to gain access to the entity” (e.g., a matched user of another mobile device) “determined to be in proximity to the mobile device.” Ex-1002, ¶¶158-160.

- g. Claim 18/28: [The method of claim 9/The mobile wireless device of claim 1], wherein receiving the identifier related information, using the first radio, is performed in response to [the one or more processors executing instructions for:] sending at least the unique identifier to at least one of the one or more servers using the first radio.**

As discussed for Elements 1[a] and 9[a], Ribaudo teaches that a mobile device receives “identifier related information” (e.g., match data) over the “first radio” (e.g., WAN or Internet) from the data center (which includes a server), only after the

device first provides a user profile to the data center (which entails sending a unique identifier to the server using the first radio). Ex-1007, ¶¶24-25, Fig. 1.

Specifically, a mobile device “*submit[s] a user profile* for its associated user *to data center 14* for comparison with user profiles for users of other mobile devices 12. *In response* to such comparison, mobile device 12 may *receive and store match data* generated at data center 14” and “may thereafter communicate with other mobile devices 12 detected in proximity to determine whether their associated users are matches (e.g., have been predetermined to be matches as reflected in the match data stored in mobile device 12). Mobile 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.” Ex-1007, ¶26; Ex-1002, ¶¶161-163.

- h. Claim 20: The method of claim 19, wherein the further information relates to one or more of the following: a loyalty program; a payment service; or a coupon relating to an entity in proximity to the mobile device; or advertising content.**

See Claims 14 and 19 above. As explained for Claim 14, Ribaudo teaches the method of Claim 19 wherein the “further information” relates to advertising content. *See* Ex-1007, ¶¶140, 215, 217. Ex-1002 ¶164.

- i. **Claim 22: The method of claim 19, wherein the further information relates to a nearby user of an application on another device, in common with an application on the mobile device.**

Ribaudo discloses the method of Claim 19, wherein the “*further information*” relates to a nearby user of an application on another device, in common with an application on the mobile device. For example, a “second user may enter an identifier of another user (e.g., the first user) such as an email address, telephone number, name, username, instant messaging screen name, or other suitable information for identifying the first user into the web site associated with data center 14 (and possibly the proprietor of system 10) to view what the second user shares in common with the first user.” Ex-1007, ¶¶140-143; *see also id.*, ¶120; Ex-1002 ¶¶165-166.

- j. **Claim 25: The method of claim 9, wherein the step of determining that an entity or object is within proximity further comprises: comparing the identifier related information with the unique identifier or information derived from the unique identifier.**

As explained for Elements 1[h] and 9[d], Ribaudo teaches “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.” Ex-1007, ¶6. And at “step 108, *mobile device 12a determines whether a match is detected in 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.” *Id.*, ¶85, Fig. 2; Ex-1002 ¶¶167-168.

k. Claim 26:

(1) Element 26[pre]: The method of claim 9, additionally comprising:

See Claim 9 above. Ex-1002 ¶169.

(2) Element 26[a]: sending the unique identifier, using the first radio, to at least one server of the one or more servers, and wherein the one or more servers perform the following steps:

See Claim 14 above. Ex-1002 ¶170.

(3) Element 26[b]: associating an object or entity as being within proximity to the mobile device;

Ribaudó’s data center (which includes a server) associates an entity (*e.g.*, user of another mobile device) as being in proximity to the mobile device (*i.e.*, sender of the unique identifier) by “processing the network identifiers received from the first and second mobile devices to determine whether the first mobile device and the second mobile device are in proximity to one another.” Ex-1007, ¶7.

The data center generates *match data* based on user profiles submitted to the data center (Ex-1007, ¶¶26, 83), and the user profiles may specify a particular city. Ex-1007, ¶99. Such information may likewise enable the server to associate relevant

matches based on proximity (*e.g.*, if two mobile device users reside in the same city). Ribaudó similarly teaches that “system 10 supports connections based on tag information” (Ex-1007, ¶108), which may include location-based tags (Ex-1007, ¶¶117, 212); Ex-1002 ¶¶171-173.

(4) Element 26[c]: storing a user’s purchasing practices or requests from the one or more servers, related to the associated object or entity information as stored proximity user behavior;

Ribaudó’s server stores a user’s purchasing practices or requests from the servers related to the associated entity information as stored proximity user behavior: “[d]ata center 14 may collect and store personality attributes and group attributes of users who encounter certain networks over time,” and “[a]ssigning this attribute information to particular wireless access points may enable the data center 14 ... to direct users of mobile devices to specific locations.” Ex-1007 ¶216. And “[d]ata center 14 or another suitable component of system 10 may create a feedback loop similar to a cookie, which may be used to *attach a user’s preferences*” or “*purchasing patterns*” “to suitable wireless access points.” Ex-1007, ¶217; Ex-1002 ¶¶174-175.

(5) Element 26[d]: retrieving a stored user email address associated with an account associated with the mobile device; and

Ribaudó’s data center generates match data by processing, evaluating, and/or comparing “user profiles 24.” Ex-1007, ¶¶6, 40-41. And a “[u]ser profile 24 may

include a Friends and Acquaintances section ... allow[ing] users to specify their friends acquaintances” by “uploading a list of [their] *email addresses*,” in order “for matches to be determined,” (*id.*, ¶94), thereby storing multiple email addresses associated with respective users of respective mobile devices.

As discussed for Element 26[e] below, the server may subsequently retrieve a stored user email address (*e.g.*, of a prospective customer) associated with an account and mobile device to “facilitate sales initiated by emails.” Ex-1007, ¶140; Ex-1002 ¶¶176-178.

(6) Element 26[e]: sending an email, addressed to the user email address containing customized content based upon the stored proximity user behavior.

As discussed for Elements 26[c]-26[d], Ribaudó’s server stores “proximity user behavior” in the form of “a user’s preferences” or “purchasing patterns,” (Ex-1007, ¶217), as well as email addresses uploaded to a user profile. Ex-1007, ¶¶94, 140.

Further, “*customized content*,” which may be based on such “stored proximity user behavior,” is sent via email from the server to a user. A “plug-in” may be added to an email application to “*display what the first and second users share in common*,” allowing “sales people ... to facilitate sales initiated by emails” that “may increase the chances of a response by allowing the recipient to view what he shares in

common with the sales person.” Ex-1007 ¶140. Ribaudó also discloses that “a first user may be able to introduce second and third users ... even when the first user is not nearby,” in that “[t]he user may be able to *customize an introduction message* to send to each of the users via email.” Ex-1007, ¶119; *see also id.*, ¶157 (“the first user may receive a notification from data center 14 via ... email.”); Ex-1002 ¶¶179-181.

- l. Claim 27: The mobile wireless device of claim 1, wherein the one or more processors further execute the instructions to perform the operations for determining that an entity or object is within proximity by further: comparing the identifier related information with the unique identifier or information derived from the unique identifier.**

See Claim 25 and Elements 1[h] and 9[d] above. Ex-1002 ¶182.

- m. Claim 29: The method of claim 9, wherein the proximity beacon transmissions are received, at the mobile device, without requiring the mobile device to first perform a step of transmitting to the one or more beacon transmitter devices from which the plurality of proximity beacon transmissions are received.**

As discussed for Elements 1[f] and 9[b], Ribaudó’s mobile devices are “beacon transmitters”—they “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). This *beaconed data may be broadcast within any suitable range*, depending on the technology.” Ex-1007, ¶57; *see also id.*, ¶76. Thus, a mobile device is *not required* to first transmit anything

to the transmitting devices, in order to receive the beacon transmissions; Ex-1002 ¶¶183-184.

n. Claim 30:

(1) Element 30[pre]: The mobile wireless device of claim 1 wherein:

See Claim 1, above. Ex-1002 ¶185.

(2) Element 30[a]: the identifier related information comprises a list of contact information, and the one or more processors further execute the instructions to perform operations including:

As discussed for Element 1[e], Ribaudo teaches that mobile devices receive identifier related information (*e.g.*, match data) via first radio (*e.g.*, cellular or WWAN). *E.g.*, Ex-1007, ¶16.

Such match data includes, or considers a “list of contact information.” Ribaudo’s data center generates match data (“identifier related information”) by processing, evaluating, and/or comparing “user profiles 24.” Ex-1007, ¶¶6, 40-41. And a user profile may include a list of contacts for that user: the “[u]ser profile 24 may include a Friends and Acquaintances section ... allow[ing] users to specify their friends acquaintances” by “uploading a list of [their] email addresses,” in order “for matches to be determined.” *Id.*, ¶94; *see also id.*, ¶27.

And the “match ID,” which “may represent the results of data center 14 processing user profiles 24 to generate match data,” may include a “trust score” (Ex-

1007, ¶48), which may be calculated based on “the number of other users that list the user in their contacts lists.” Ex-1007, ¶75; Ex-1002 ¶¶186-188.

- (3) **Element 30[b]: further determining that at least one beacon transmitter device associated with the proximity beacon service is further matched with an entity included within the list of contact information based upon comparing a contact identifier information with at least a portion of the unique identifier, and;**

As discussed for Element 30[a], Ribaudó’s mobile device “submit[s] a user profile for its associated user to data center 14 for comparison with user profiles for users of other mobile devices,” and then “receive[s] and store[s] match data.” Ex-1007, ¶26. A mobile device “may thereafter communicate with other mobile devices ... to determine whether their associated users are matches.” *Id.* As explained for Element 1[f], the mobile device initiating the communication in this scenario is a beacon transmitter device associated with a proximity beacon service.

Ribaudó further teaches that *matching* a beacon transmitter device with an entity (*i.e.*, user of a receiving mobile device) included within the list of contact information, is done based upon *comparing* a contact identifier information with at least a portion of the unique identifier. *First*, as discussed for Element 30[a], the “user profile,” which is used to predetermine matches, may include “***a list of email addresses***” *corresponding to the user’s contacts* (*i.e.*, “friends and acquaintances”). Ex-1007, ¶¶26, 94. *Second*, as discussed for Element 1[h], a mobile device “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.” Ex-1007, ¶85. Accordingly, Ribauda teaches matching a beacon transmitter device with an entity based on comparing a user’s list of email addresses (*i.e.*, “contact identifier information”) with the client ID (*i.e.*, “unique identifier,” or portion thereof). Ex-1002 ¶¶190-192.

- (4) **Element 30[c]: the mobile wireless device, upon determining there is a match, allowing further communications with the detected beacon transmitter device associated with the entity included within the list of contact information, wherein the further communications utilize the first radio.**

Ribauda teaches that, upon receiving match data generated at the data center, a “[m]obile device 12”—*i.e.*, beacon transmitter device—“may thereafter communicate with other mobile devices 12 detected in proximity.” Ex-1007, ¶26. As discussed for Element 30[a] above, the beacon transmitter device is associated with an entity (*i.e.*, user) who is included within the “list of contact information” that is used to generate match data. *See* Element 30[a], above.

Then, “[m]obile device 12 may notify its user if such a match is detected in proximity, *allowing the user to initiate an interaction*” (Ex-1007, ¶26)—*i.e.*, allowing further communications with the detected beacon transmitter device. And

the user-initiated interactions may utilize the first radio (i.e., cellular or WWAN). Specifically, the mobile devices “may use the TCP/IP protocol to create a messaging connection between mobile devices 12a and 12b. Other messaging mechanisms,” including “cellular telephone ... may also be used.” Ex-1007, ¶79; *see also id.*, ¶76 (listing GSM and CDMA as “other suitable wireless platforms” for communication among mobile devices); Ex-1002 ¶¶193-195.

B. Ground 2: Claims 1, 4-6, 9, 14, 16-20, 22, and 24-30 are obvious over Ribaudó in view of Watanabe.

Ground 2 is identical to Ground 1, except that for the claimed “Proximity Beacon Service Identifier (PBSI),” and all limitations associated with that feature, it incorporates Watanabe’s teaching of including a “service code 202” in a proximity beacon transmission. *See* Ex-1006, ¶¶14-15, Fig. 2; Ex-1002 ¶196.

1. A POSITA would have been motivated to combine Ribaudó’s teachings with Watanabe’s teachings and would have had a reasonable expectation of success.

A POSITA would have been motivated to combine the teachings of Ribaudó and Watanabe with a reasonable expectation of success because each relates to detecting nearby wireless devices and establishing communications. Ex-1006, Abstract; Ex-1007, Abstract, ¶18; Ex-1002 ¶¶197-203.

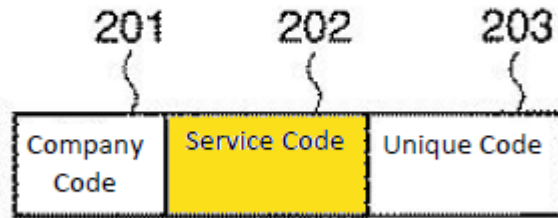
Ribaudó’s “mobile device detects the presence of the other user’s mobile device, receives an identifier associated with the detected other user, and compares the received identifier with the pre-processed match data stored on the user’s mobile

device to determine whether the other user is one of the user's predetermined matches." Ex-1007 ¶6. These devices "may *beacon* data such as the client ID of the user associated with mobile device 12" (Ex-1007, ¶57) and an SSID of 'proprietor_name.net'...." *Id.*, ¶123. Additionally, "[t]he unique MAC address of mobile device 12a may be beacons when the BLUETOOTH interface of mobile device 12a is active." *Id.*, ¶157.

As discussed for Element 1[g] in Ground 1, a POSITA would have understood that Ribaud's "SSID of 'proprietor_name.net'" qualifies as a PBSI, because users may recognize and associate a given proprietor (*e.g.*, online dating platform) with a service (*e.g.*, providing dating matches to users within a given area). *See, e.g.*, Ex-1007, ¶¶97-104, 123. Regardless, it nonetheless would have been obvious to include a PBSI in Ribaud's beacon transmissions, based on Watanabe's teachings.

Watanabe's wireless communication system includes access points and client terminals, where "each access point 11 has a power induction transmitter 112 that continuously or intermittently (cyclically) generates an induction *beacon*" that includes "a company code 201 indicating the service provider," a "*service code 202 indicating the type of service* that can be provided via that access point," and "a unique code 203 unique to that ... transmitter." Ex-1006, ¶¶14-15, Fig. 2.

[FIG. 2]



A POSITA would have been motivated to include, in Ribaudó's beacon, a "service code[]" indicating the type of service that can be provided" by the transmitting device, as taught by Watanabe. Ribaudó's "mobile devices 12 may be used as reference beacons in system 10 in a substantially similar manner to the manner in which network access points ... are used." Ex-1007, ¶77. And "although MAC addresses and SSIDs are primarily described, [the] invention contemplates use of any other suitable identifiers ... according to particular needs." *Id.*, ¶76. Further, Watanabe discloses that its service code is one of a "plurality of fields" in a beacon's transmitter identification information, whose "field structure ... is a common structure used when utilizing various types of internet services." Ex-1006, ¶15; Ex-1002 ¶201. Moreover, Watanabe teaches that incorporating a service code in transmitter identification information is beneficial, in that "[b]y configuring the service content to be provided" by the transmitting device, "services can be selectively provided according to the location of the access point and the bandwidth

required, and cost increases can [thereby] be avoided.” Ex-1006, ¶16.

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) in its beacon transmission, to help identify and facilitate communication with other devices relevant to a given service, while preserving bandwidth and other costs, in Ribaudó’s ad hoc network. Ex-1002 ¶202.

A POSITA would have had a reasonable expectation of success in applying Watanabe’s teachings to Ribaudó. Ex-1002 ¶203. 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. Ex-1006, ¶¶46-55; Ex-1007, ¶¶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.

2. Independent Claim 1

See Elements 1[pre], 1[a]-1[e], and 1[h] in Ground 1 above, explaining that Ribaudó teaches these limitations. *See supra* Section XII.A.1; Ex-1002 ¶204.

a. Element 1[f]: ... each of the proximity beacon transmissions including ... a Proximity Beacon Service Identifier (PBSI);:

Watanabe discloses mobile devices (*e.g.*, access points) that transmit induction beacons containing a plurality of fields, including a “*service code 202*” indicating the type of service that can be provided” via that device. *See* Ex-1006, ¶15. Accordingly, the combination of Ribaudó in view of Watanabe (“Ribaudó-Watanabe”) teaches Element 1[f], where the claimed “MAC address,” “unique identifier” and “PBSI” are as follows.

Claim Element	Ribaudó-Watanabe
“MAC address”	Ribaudó’s MAC address of transmitting device
“Unique identifier”	Ribaudó’s client ID and potentially other suitable information for uniquely identifying a user
“PBSI”	Watanabe’s service code

Ex-1002 ¶¶205-207.

b. Element 1[g]:

In the Ribaudó-Watanabe combination, the “network identifiers” would additionally include Watanabe’s “service code.” *See* Ex-1006, ¶15. Accordingly, Ribaudó-Watanabe teaches determining that the beacon transmissions include a MAC address and a PBSI as reflected below.

Claim Element	Ribaudó-Watanabe
“MAC address”	Ribaudó’s MAC address of transmitting device
“PBSI”	Watanabe’s service code

Further, the PBSI of Ribaudo-Watanabe would indicate that the particular short range transmission is a proximity beacon transmission associated with the proximity beacon service, because Watanabe teaches that its “service code ... *indicat[es] the type of service that can be provided.*” Ex-1006, ¶15. Ex-1002, ¶¶208-210.

3. Independent Claim 9

The following limitations of Claim 9 are taught by either: (1) Ribaudo, as shown in the corresponding limitations in for Claim 1 in Ground 1; (2) Ribaudo-Watanabe, as shown in the corresponding limitations for Claim 1 in Ground 2. Ex-1002 ¶211.

Element 9[pre]	Ground 1, Elements 1[pre], 1[c], 1[d], and 1[e]
Element 9[a]	Ground 1, Elements 1[a] and [e]
Element 9[b]	Ground 1, Element 1[b] Ground 2, Element 1[f]
Element 9[c]	Ground 2, Element 1[g]
Element 9[d]	Ground 1, Element 1[h]

4. Dependent Claims 4-6, 14, 16-20, 22, and 24-30

Ribaudo-Watanabe teaches dependent Claims 4, 6, 14, 16-22, and 24-30 for the same reasons discussed for these corresponding claims in Ground 1 above. *See supra* Sections XII.A.3.a and XII.A.3.c-.n; Ex-1002 ¶212.

a. Claim 5:

As discussed in Ground 1, Ribaudo teaches the added limitation of Claim 5.

See supra Section XII.A3.b.

Watanabe also teaches this limitation. Watanabe teaches that “when the client terminal 14 has entered into an area 812” (i.e., a predetermined location) “that is covered by the access point 11-2” (i.e., a beacon transmitter device), it “receives the induction beacon 802 and is started up, and compares the transmitter identification information ‘C2:S2:U2,’ included therein, to the identification information ‘C2:S2’ for filtering” which “has been set in advance” (i.e., identifier related information). Ex-1006, ¶¶52, 50. Watanabe thus teaches determining based on the identifier related information that the beacon transmitter is associated with access point 11-2 covered by area 812, which a POSITA would have understood corresponds to a predetermined location. Ex-1002 ¶214.

Accordingly, Ribaudo-Watanabe teaches dependent Claim 5. Ex-1002 ¶¶213-215.

C. Grounds 3 and 4: Claims 2-3, 7-8, 10-13, 15, and 31 are obvious over Ribaudo in view of Behrens (Ground 3), or Ribaudo in view of Watanabe and Behrens (Ground 4).

- 1. A POSITA would have been motivated to combine Ribaudo’s teachings, or Ribaudo-Watanabe’s teachings, with Behrens’ teachings and would have had a reasonable expectation of success.**

A POSITA would have been motivated to combine the teachings of Ribaudo or Ribaudo-Watanabe with Behrens and would have had a reasonable expectation of success in doing so because each relates to detecting nearby wireless devices and establishing communications. Ex-1007, Abstract, ¶18; Ex-1006, Abstract; Ex-1008, 1:6-9. *See supra* Sections XII.A.1, XII.B.1; Ex-1002 ¶216.

As explained for Grounds 1 and 2 above, Ribaudo, alone or in combination with Watanabe, teaches a mobile device receiving a plurality of proximity beacon transmissions, each including a MAC address, unique identifier, and Proximity Beacon Service Identifier (“PBSI”). Ex-1002 ¶217.

Behrens teaches electronic devices that “continuously/repeatedly transmit” and scan for “unique identifiers (UID) via non-directed wireless radio frequency transmission.” Ex-1008, 11:1-5. According to Behrens, a UID “may consist of or include a [WLAN] MAC (media access control) address, Bluetooth Device Address (i.e., BD_ADDR), or other unique or quasi-unique identifier.” Ex-1008, 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.” Ex-1008, 22:24-28. Moreover, “[e]ven in the event that the device has a UIDs, the software may allow use of a different UID.” Ex-1008, 22:28-29. Behrens teaches that “this may be beneficial to the user” because it “may even allow a user to have ***multiple or changing UIDs*** and, therefore, different online identities,” which “may also be linked to a single user account,” where the user could manage them. Ex-1008, 23:1-5. Behrens cites “MAC addresses” as a type of UID. Ex-1008, 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. Ex-1002 ¶218.

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,” Ex-1007, ¶68, and that “[t]he client ID may be used to shield the true identity of the user, for privacy purposes for example,” or, “[a]lternatively, the client ID may simply be the user ID of the user, which in certain embodiments may reveal the true identity of the user,” *id.*, ¶46. Ribaudo also teaches “***time-slicing*** to join and bounce between several networks.” *Id.*, ¶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.*, ¶72. Ribaudo thus explains that for certain periods of a time a

device may have an ID associated with one identity and functionality, and during another period of time, the same device may have a different ID associated with a different functionality. *See id.*

Thus, a POSITA would have been motivated to implement, in Ribaudo or Ribaudo-Watanabe, Behrens' teaching that *multiple unique identifiers* (which include MAC addresses) may be associated with the same transmitting device, allowing the user to access different servers or online services, which may each require different unique identifiers, using a single mobile device. A POSITA would have been further motivated to implement Behrens' teachings using Ribaudo's time-slicing technique to economically distribute bandwidth resources. Ex-1002 ¶220. As Behrens explains, employing multiple identifiers would provide the user benefit of having "different online identities" so that the user may "create a new online identity for an event or party he attends or has attended." Ex-1008, 23:2-4. In Ribaudo-Behrens and Ribaudo-Watanabe-Behrens, the "second unique identifier" would be associated with the same entity/object (*i.e.*, the same mobile device user) as the "first unique identifier," and the multiple unique identifiers would be received via Bluetooth or WLAN (*i.e.*, Wi-Fi) from the same transmitting device, as taught by Behrens.

A POSITA would have had a reasonable expectation of success in combining Ribaudo or Ribaudo-Watanabe with Behrens. Ex-1002 ¶221. 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. *E.g.*, Ex-1006, ¶¶46-55; Ex-1007, ¶¶6-7; Ex-1008, Abstract, 6:1-30, 19:5-14. And, as discussed above, Ribauda 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. Ex-1007, ¶¶45, 68. A POSITA would thus have understood that applying Behrens’ teachings to the Ribauda and Ribauda-Watanabe systems would have yielded predictable results. Ex-1002 ¶¶216-221.

2. Dependent Claims 2-3, 7-8, 10-13, 15, and 31

- a. Claim 2: The mobile wireless device of claim 1, wherein the MAC address is a randomly generated 48 bit number matching a format of a Bluetooth BD_ADDR.**

As discussed for Element 1[f], Ribauda discloses that “[t]he *unique MAC address* of mobile device 12a *may be beacons* when the BLUETOOTH interface of mobile device 12a is active.” Ex-1007, ¶157. A POSITA would have understood that the MAC address for a Bluetooth-enabled device “is a unique *48-bit Bluetooth device address (BD_ADDR)*.” Ex-1021 at 232; Ex-1002 ¶223. Behrens acknowledges this, teaching that “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.” Ex-1008, 11:21-26; *see also id.*, 19:12-14 (“In the case

of Bluetooth, various address parts and lengths (*e.g.*, 48-bit BD_ADDR, 24-bit LAP, etc.) ... may be used.”).

While Ribaudó and Behrens are silent as to whether the MAC addresses of their respective Bluetooth-enabled devices are *randomly-generated*, it would have been obvious to use a randomly-generated MAC address for a transmitting device in the Ribaudó-Behrens and Ribaudó-Watanabe-Behrens systems. *First*, it was well-known in the art that a Bluetooth MAC address may configured to be either a static, public address, or else a randomly-generated address that changes periodically, as a privacy-enhancing option. Ex-1002 ¶224; Ex-1042. *Second*, Ribaudó itself teaches that “substantial privacy” may be an important consideration for its wireless system. Ex-1007, ¶226. Accordingly, a POSITA would have been motivated to use a randomly-generated MAC address in order to advance Ribaudó’s objective of enhancing privacy for the user of the transmitting device. Further, a POSITA would have had a reasonable expectation of successfully implementing a randomly-generated MAC address, as it was a well-known approach, and was one of just two options for configuring a MAC address for a Bluetooth device. Ex-1002 ¶¶222-224.

b. Claim 3:

- (1) Element 3[pre]: The mobile device of claim 1, wherein the one or more processors further execute the instructions to perform operations including:**

See Claim 1 for Grounds 1 or 2 above. Ex-1002 ¶225.

- (2) **Element 3[a]: receiving, by the second radio, a first proximity beacon transmission including a first MAC address and a first unique identifier at a first time; and**

See Element 1[f] for Grounds 1 or 2 above. As explained for Element 3[b] below, in the Ribaudó-Behrens and Ribaudó-Watanabe-Behrens combinations, the first MAC address and unique identifier would be transmitted and received at first time. Ex-1002 ¶226.

- (3) **Element 3[b]: receiving, by the second radio, a second proximity beacon transmission including a second MAC address and a second unique identifier at a second time, the second MAC address being different from the first MAC address and the second unique identifier being different from the first unique identifier; and**

Ribaudó-Behrens and Ribaudó-Watanabe-Behrens teach Element 3[b].

First, as discussed for Element 1[f] in Ground 1 above, Ribaudó’s teaching of “***beacon[ing]*** data,” Ex-1007, ¶191, entails a *plurality* of short-range transmissions—i.e., regular, periodic transmissions of data (including identifiers) in order to facilitate device discovery. See Ex-1002, ¶228; Ex-1007, ¶148. Watanabe corroborates this. See Ex-1006, ¶46 (explaining that the “transmitter 112 of an access point 11 applies transmitter identification information to the beacon (S501), to ***send it*** continuously or ***periodically*** (S502).”).

Second, as discussed in Section XII.C.1, Ribaudó and/or Behrens discloses that *multiple unique identifiers* can be assigned to a given transmitting device, Ex-

1007, ¶68 (disclosing “one or more client IDs”); Ex-1008, 22:28-29, 23:1-5 (disclosing “**multiple or changing UIDs**”); *see also id.*, 19:8-14 (MAC addresses are UIDs). This beneficially enhances privacy, by allowing “different online identities,” and/or the ability to “shield” or “reveal” one’s identity depending on context. Ex-1007, ¶46; Ex-1008, 23:1-5.

Third, as further discussed in Section XII.C.1, Ribaudo discloses that mobile devices (which include beacon transmitters) can use time-slicing to distribute bandwidth resources economically, such that—for certain periods of time a device may have an ID associated with one identity and functionality, and during other periods of time, the same device may have a different ID associated with a different functionality. Ex-1007, ¶72.

Accordingly, the Ribaudo-Behrens and Ribaudo-Watanabe-Behrens systems teach the following scenario, in which the same beaconing device (e.g., mobile devices 12b, 12c, etc.) transmits, at two different time slices, two different MAC address, and two different unique identifiers, but transmits the same PBSI (e.g., SSID or the system proprietor, or Watanabe’s service code) indicating the type of service that remains associated with that transmitter at both times. Ex-1002 ¶231.

Time Slice	Beacon transmitter transmits:
TS1	(MA1 + UID1 + PBSI)
TS2	(MA2 + UID2 + PBSI)

Specifically, (1) during a first time slice (*e.g.*, TS1), the transmitter beacons a first MAC address (MA1), a first unique identifier (UID1), and a PBSI; and (2) at a second time slice (TS2), the same transmitter beacons a second, updated MAC address (MA2), along with second unique identifier UID2 and the same PBSI. In that scenario, a receiving mobile device would, at time slice TS2, “receiv[e] by [its] second radio (*i.e.*, Wi-Fi or Bluetooth), a second proximity beacon transmission including a second MAC address and a second unique identifier at a second time, the second MAC address being different from the first MAC address and the second unique identifier being different from the first unique identifier.” Ex-1002 ¶¶227-232.

(4) Element 3[c]: associating the first and second unique identifier with a single beacon transmitter device.

See Element 3[b] above. As explained in Section XII.C.1, Behrens teaches that a unique identifier ‘uniquely *identifies* a device.’ Ex-1008, 19:8-10; *see also* Ex-1007, ¶68 (explaining that the one or more client IDs “may identify the user publicly”). Accordingly, in the scenario described for Element 3[b] above, the receiving device (*e.g.*, mobile device 12a) associates the first and second unique identifier with the same beacon transmitter device (*e.g.*, 12b, 12c, etc.). Ex-1002 ¶233.

c. Claim 7:

- (1) Element 7[pre]: The mobile wireless device of claim 3, wherein**

See Claim 3 above. Ex-1002 ¶234.

- (2) Element 7[a]: the identifier related information comprises a list of contact information, and the one or more processors further execute the instructions to perform operations including:**

See Element 30[a] above. Ex-1002 ¶235.

- (3) Element 7[b]: further determining that at least one beacon transmitter device associated with the proximity beacon service is further matched with an entity included within the list of contact information based upon comparing a contact identifier information with at least a portion of the unique identifier, and**

See Element 30[b] above. Ex-1002 ¶236.

- (4) Element 7[c]: the mobile wireless device, upon determining there is a match, allowing further communications with the detected beacon transmitter device associated with the entity included within the list of contact information, wherein the further communications utilize the first radio.**

See Element 30[c] above. Ex-1002 ¶237.

d. Claim 8:

- (1) Element 8[pre]: The mobile wireless device of claim 1 wherein the one or more processors further execute the instructions to perform operations including:**

See Element 3[pre] above. Ex-1002 ¶238.

- (2) Element 8[a]: receiving, via a second radio, the plurality of proximity beacon transmissions further includes receiving a first unique identifier at a first time that is different from a second unique identifier received at a second time; and**

See Element 3[b] above. Ex-1002 ¶239.

- (3) Element 8[b]: associating the first and second unique identifier with a single beacon transmitter device.**

See Element 3[c] above. Ex-1002 ¶240.

e. Claim 10:

- (1) Element 10[pre]: The method of claim 9,**

See Claim 9 above. Ex-1002 ¶241.

- (2) Element 10[a]: wherein a first one of the plurality of proximity beacon transmissions received at a first time includes a first unique identifier, and**

See Elements 1[f] and 3[a] above. Ex-1002 ¶242.

- (3) **Element 10[b] wherein a second one of the plurality of proximity beacon transmissions received at a second time includes a second unique identifier being different from the first unique identifier; and**

See Element 3[b] above. In the scenario described in Element 3[b] above, at time slice TS2, a receiving mobile device (*e.g.*, 12a) receives “a second one of a plurality of proximity beacon transmissions” that “includes second unique identifier” (*e.g.*, UID2) “being different from the first unique identifier” (*e.g.*, UID1) which had been sent at time slice TS1 as part of the first one of a plurality of proximity beacon transmissions, as indicated below. Ex-1002 ¶243.

Time Slice	Beacon transmitter transmits:
TS1	(MA1 + UID1 + PBSI)
<u>TS2</u>	(MA2 + <u>UID2</u> + PBSI)

- (4) **Element 10[c]: associating both the first unique identifier and the second unique identifier with a particular entity or object in proximity to the mobile device.**

See Element 3[c] above. The recited “particular entity” corresponds to the same particular user of the transmitting device (*e.g.*, 12b, 12c, etc.) in the scenario described in Element 3[c], and “associating” the unique identifiers with that user may or may not entail disclosing the user’s true identity. *See* Ex-1007, ¶46; Ex-1008, 23:1-5. Ex-1002 ¶244.

- f. **Claim 11: The mobile wireless device of claim 9 wherein the MAC address is selected from a group consisting of (a) a randomly generated 48 bit number matching a format of a MAC address and (b) a Bluetooth BD_ADDR.**

See Claim 2 above. Ribaud-Behrens and Ribaud-Watanabe-Behrens teach Claim 11, whether the MAC address of the Bluetooth-enabled transmitting device is a “randomly generated 48 bit number matching the format of a MAC address,” or is instead a standard Bluetooth BD_ADDR. Ex-1002 ¶245.

- g. **Claim 12:**

- (1) **Element 12[pre]: The method of claim 9**

See Claim 9 above. Ex-1002 ¶246.

- (2) **Element 12[a]: wherein a first one of the plurality of proximity beacon transmissions is received at a first time and includes a first unique identifier and first MAC address, and the Proximity Beacon Service (PBSI); and**

See Elements 1[f] and 3[a] above. Ex-1002 ¶247.

- (3) **Element 12[b]: where a second one of the plurality of proximity beacon transmissions received at a second time includes a second unique identifier different from the first unique identifier and second MAC address different from the first MAC address, and the Proximity Beacon Service Identifier; and**

See Elements 1[f] in Grounds 1 or 2, and Element 3[b] above. As discussed for Element 3[b] above, each of the plurality of transmissions from the transmitting device would include the same “PBSI”—whether the SSID of the proprietor, as

disclosed by Ribaudo (Ex-1007, ¶123), or the added service code per Watanabe’s teachings (Ex-1006, ¶15), to indicate a particular service that remains associated with that device during both time slices, as shown below. Ex-1011 (Proctor Decl.), ¶124, Ex-8, n.5 (emphases original). Ex-1002 ¶248.

Time Slice	Beacon transmitter transmits:
TS1	(MA1 + UID1 + PBSI)
<u>TS2</u>	(<u>MA2</u> + <u>UID2</u> + <u>PBSI</u>)

- (4) **Element 12[c]: associating both the first unique identifier and the second unique identifier with the same entity or object in proximity to the mobile device.**

See Element 10[c] above. Ex-1002 ¶249.

- h. Claim 13/15: The [method of claim 9, / mobile wireless device of claim 1, wherein the instructions] further compris[ing / e]: preventing the sending of the unique identifier, using the first radio, to the one or more servers, based upon previous detections of the respective unique identifier associated with the proximity beacon transmission.**

Ribaudo-Behrens and Ribaudo-Watanabe-Behrens disclose Claims 13 and 15.

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.” Ex-1008, 20:10-15. Behrens also teaches that “blacklists containing specific UIDs may be used to eliminate these

UIDs from being associated with others.” Ex-1008, 26:1-2. For example “blacklists may be UID specific, whereby a user may instruct the server and/or his device to ignore certain UIDs.” Ex-1008, 26:2-3. It would have been obvious to a POSITA to instead instruct the wireless device not to send specific UIDs rather than send them and have them ignored because it would achieve the same result but reduce use of transmission bandwidth and power. Moreover, it would have been obvious that the specific unique identifier selected for blocking would have been one previously detected because such prior detection would have provided the reason for blocking it. Ex-1002 ¶¶250-251.

i. Claim 31:

- (1) Element 31[pre]: The mobile wireless device of claim 3 wherein the one or more processors further execute the instructions to perform operations including:**

See Element 3[pre]. Ex-1002 ¶252.

- (2) Element 31[a]: receiving, via a second radio, the plurality of proximity beacon transmissions further includes receiving a first unique identifier at a first time that is different from a second unique identifier received at a second time; and**

See Element 3[b]. Ex-1002 ¶253.

(3) Element 31[b]: associating the first and second unique identifier with a single beacon transmitter device.

See Element 3[c] above. Ex-1002 ¶254.

D. Grounds 5 and 6: Claim 23 is obvious over Ribaudo in view of Mgrdechian (Ground 5), or Ribaudo in view of Watanabe and Mgrdechian (Ground 6).

1. Claim 23: The method of claim 22, wherein the application is a multiuser game.

Ribaudo in view of Mgrdechian (Ribaudo-Mgrdechian), or Ribaudo in view of Watanabe and Mgrdechian (“Ribaudo-Watanabe-Mgrdechian”), teach Claim 23. As explained for Claim 22 in Grounds 1 and 2 above, Ribaudo alone or in view of Watanabe teaches that a mobile device sends a unique identifier to the server, and subsequently receives “further information” relating to a nearby user of an application on another device, in common with an application on the mobile device. See Ex-1007, ¶¶120, 140 (discussing applications shared between the first and second users of respective mobile devices).

Ribaudo aims to “allow[] mobile device users with one or more commonalities or other reasons for interacting to detect each other when they are or have been proximity” (Ex-1007, ¶6), and mentions that its “[m]obile devices 12 may include ... *game consoles*.” *Id.*, ¶18. It would have been obvious that the nearby user’s “application,” for which “further information” is received by the mobile device, is a multiuser game. Mgrdechian demonstrates this.

Like Ribaudó and Watanabe, Mgrdechian discloses a “wireless communication system ... that provides an exchange of information between wireless devices” whose users are “previously unknown” to each other, Ex-1010, ¶¶2-3, where each device exchanges information with a remote server via Internet, Ex-1010, ¶92, and where the devices communicate with each other via Bluetooth or Wi-Fi, based on “unique identifications” or “unique IDs” stored in a remote database. Ex-1010, ¶¶21, 91-92; *see also id.*, Fig. 8.

Mgrdechian’s invention can be applied to ***“gaming applications operating on mobile devices”***:

One player may decide to initiate or play a game with another based on the other user’s profile. For example, the system may automatically enable a gaming application when other devices are detected within their vicinity, and the information associated with the local devices may indicate that the users of such devices are players of a particular game, have specific skill levels or may present some other challenge. The system may automatically notify the user of that person’s presence so that a gaming scenario can begin.

Ex-1010, ¶86.

Accordingly, it would have been obvious in view of Mgrdechian’s teachings to use the Ribaudó or Ribaudó-Watanabe systems with a “gaming application”

played by multiple nearby users, where “further information” about one device’s user (e.g., playing a particular game, skill level or other challenge) is received by another mobile device. Ex-1002 ¶259. A POSITA would have been motivated to implement Mgrdechian’s “gaming application” scenario in Ribaudó or Ribaudó-Watanabe, as such an application is consistent with Ribaudó’s goal of “allow[ing] mobile device users with one or more commonalities or other reasons for interacting to detect each other when they are or have been proximity,” Ex-1007 ¶6. Further, a POSITA would have had a reasonable expectation of successfully implementing Mgrdechian’s gaming application in Ribaudó or Ribaudó-Watanabe, since all three references aim to detect nearby wireless devices and establish communications over Bluetooth and Internet, and since Ribaudó itself contemplates that gaming applications may be used with its system, teaching that its “mobile devices” may be “game consoles.” Ex-1007, ¶18; Ex-1002 ¶¶255-259.

XIII. CONCLUSION

Petitioner requests IPR institution for Claims 1-20 and 22-31 of the ’918 Patent.

Respectfully Submitted,

/s/ William M. Fink

William M. Fink (Reg. No. 72,332)

CERTIFICATE OF WORD COUNT

Pursuant to 37 C.F.R. §42.24(d), Petitioner certifies that this petition includes 13,980 words, as measured by Microsoft Word, exclusive of the table of contents, mandatory notices under §42.8, certificates of service, word count, and exhibits.

CERTIFICATE OF SERVICE (37 C.F.R. §42.6(e)(1))

The undersigned hereby certifies that the above document was served on May 30, 2025, by filing this document through the Patent Trial and Appeal Board P-TACTS System, as well as delivering a copy via express mail upon the following attorneys of record for the Patent Owner:

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

A courtesy copy was sent to the below counsel via electronic mail:

Nelson Bumgardner Conroy PC
Timothy E. Grochocinski
C. Austin Ginnings
745 McClintock Drive, Suite 340
Burr Ridge, Illinois 60527
Phone: (708) 675-1974
Email: tim@nelbum.com
Email: austin@nelbum.com

Nelson Bumgardner Conroy PC.
Christopher G. Granaghan
3131 West Seventh Street, Suite 300
Fort Worth, Texas 76107
Phone: (817) 377-9111
Email: chris@nelbum.com

Dated: May 30, 2025

Respectfully submitted,

/s/ William M. Fink

William M. Fink (Reg. No. 72,332)

O'Melveny & Myers LLP

1625 Eye Street, NW

Washington, DC 20006

Telephone: (202) 383-5300

Fax: (202) 383-5414

E-Mail: tfink@omm.com

Attorney for Petitioner