

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

**DECLARATION OF SUNDEEP RANGAN IN SUPPORT OF PETITION
FOR *INTER PARTES* REVIEW OF U.S. PATENT NO. 11,334,918**

TABLE OF CONTENTS

	Page
I. INTRODUCTION	1
II. BACKGROUND AND QUALIFICATIONS	2
III. INFORMATION CONSIDERED	4
IV. RELEVANT LEGAL STANDARDS	5
A. Claim Interpretation	5
B. Perspective of One of Ordinary Skill in the Art.....	5
C. Obviousness.....	6
V. LEVEL OF ORDINARY SKILL IN THE ART	8
VI. SUMMARY OF MY OPINIONS	10
VII. TECHNOLOGICAL BACKGROUND	11
A. Using Beacon Transmissions to Make Proximity Determinations Was Known	11
B. The Use of MAC Addresses, Unique Identifiers, and Beacon Service Identifiers to Identify Devices and Networks Was Known	16
C. Including Identifiers in Beacon Transmissions Was Known.....	29
D. Periodic Transmission of a Beacon Signal Was Known.....	37
E. Storing Information at Servers and Mobile Devices Communicating with Servers to Obtain Stored Information Was Known	40
F. Filtering Beacon Transmissions by Comparing Stored Information to Transmitted Information to Determine Matches Was Known	46
G. Taking Action if a Match is Determined Between the Stored Information and the Transmitted Information Was Known.....	50
H. Using Protocols Such as Bluetooth and Cellular for Communications Between Mobile Devices and Servers Was Known	55
I. Using A Processor and Memory with Instructions to Execute Functions on Mobile Devices Was Known.....	60

TABLE OF CONTENTS
(continued)

	Page
VIII. THE '918 PATENT AND ITS FILE HISTORY	64
IX. CLAIM CONSTRUCTION	68
X. OVERVIEW OF THE APPLIED PRIOR ART REFERENCES	69
A. Ribaudó (Ex-1007)	69
B. Watanabe (Ex-1005, Ex-1006).....	71
C. Behrens (Ex-1008)	74
D. Mgrdechian (Ex-1010)	76
XI. DETAILED EXPLANATION OF THE UNPATENTABILITY GROUNDS	78
A. Ground 1: Claims 1, 4-6, 9, 14, 16-20, 22, and 24-30 are obvious over Ribaudó.	78
1. Independent Claim 1	78
a. Element 1[pre]: A mobile wireless device comprising:	78
b. Element 1[a]: a first radio;.....	79
c. Element 1[b]: a second radio;.....	80
d. Element 1[c]: one or more processors;.....	81
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:	83
f. Element 1[e]: receiving, using the first radio, identifier related information associated with a proximity beacon service, from one or more servers;	86

TABLE OF CONTENTS

(continued)

Page

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);	89
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:	98
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.....	100
2.	Independent Claim 9	104
a.	Element 9[pre]: A method for facilitating the use of proximity beacons, the method executing within a mobile device, and the method comprising:	104
b.	Element 9[a]: communicating between the mobile device and one or more servers and receiving, at the mobile device, identifier related information, using a first radio;	105

TABLE OF CONTENTS

(continued)

Page

c.	Element 9[b]: receiving, at the mobile device using a second radio, a plurality of short range transmissions, including a plurality of proximity beacon transmissions from one or more beacon transmitter devices associated with a proximity beacon service, each of the proximity beacon transmissions including a respective MAC address, a respective unique identifier (UID), and a Proximity Beacon Service Identifier (PBSI);	105
d.	Element 9[c]: a) determining that a particular short range transmission of the plurality of short range transmissions includes a MAC address, b) determining that the Proximity Beacon Service Identifier (PBSI) is present, and c) determining that the PBSI indicates the particular short range transmission is a proximity beacon transmission associated with the proximity beacon service; and when the three determining steps a) b) and c) are each true, then	105
e.	Element 9[d]: d) determining that an entity or object associated with the proximity beacon service is within proximity to the mobile device, by utilizing the identifier related information and the unique identifier	106
3.	Dependent Claims 4-6, 14, 16-20, 22, and 24-30	106
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.	106

TABLE OF CONTENTS
(continued)

	Page
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.	108
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.....	110
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.....	111
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.....	113

TABLE OF CONTENTS
(continued)

	Page
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.	116
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.	117
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.....	118
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.	119
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.....	120
k. Claim 26:	121

TABLE OF CONTENTS

(continued)

	Page
1. 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.....	125
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.....	125
n. Claim 30:	126
B. Ground 2: Claims 1, 4-6, 9, 14, 16-20, 22, and 24-30 are obvious over Ribaudó in view of Watanabe.....	129
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.	130
2. Independent Claim 1	134
a. Element 1[f]: ... each of the proximity beacon transmissions including ... a Proximity Beacon Service Identifier (PBSI);:	134
b. Element 1[g]:	135
3. Independent Claim 9	136
4. Dependent Claims 4-6, 14, 16-20, 22, and 24-30	137
a. Claim 5:	137
C. Grounds 3 and 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).....	138
1. A POSITA would have been motivated to combine	

TABLE OF CONTENTS

(continued)

	Page
Ribaudo's teachings, or Ribaudo-Watanabe's teachings, with Behrens' teachings and would have had a reasonable expectation of success.....	138
2. Dependent Claims 2-3, 7-8, 10-13, 15, and 31	142
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.	142
b. Claim 3:	144
c. Claim 7:	148
d. Claim 8:	149
e. Claim 10:	150
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.	151
g. Claim 12:	152
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.	153
i. Claim 31:	154
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).....	155
1. Claim 23: The method of claim 22, wherein the application is a multiuser game.....	155

TABLE OF CONTENTS
(continued)

	Page
XII. CONCLUSION.....	158

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

1. My name is Sundeep Rangan. I am presently a professor in the Department of Electrical and Computer Engineering at New York University, Brooklyn, New York. My residence is in Jersey City, New Jersey, and my place of business is in Brooklyn, New York. I am over the age of eighteen, and I am a citizen of the United States.

2. I have been retained to provide this Declaration by Samsung Electronics Co., Ltd. and Samsung Electronics America, Inc. (“Petitioner”) as an independent expert consultant in this inter partes review (“IPR”) proceeding before the United States Patent and Trademark Office (“PTO”).

3. I have been asked by Petitioner Counsel (“Counsel”) to consider whether certain references disclose, teach and/or suggest the features recited in Claims 1-20 and 22-31 of U.S. Patent No. 11,334,918 (“the ’918 Patent”) (Ex-1001), which I understand is currently assigned to Secure Communication Technologies, LLC (“PO”).² My opinions and the bases for my opinions are set forth below.

4. I am being compensated at my ordinary and customary consulting rate for my work, which is \$700 per hour. My compensation is in no way contingent on

² Where appropriate, I refer to exhibits that I understand are attached to the petition for IPR of the ’918 Patent.

the nature of my findings, the presentation of my findings in testimony, or the outcome of this or any other proceeding. I have no other direct financial interest in this proceeding.

II. BACKGROUND AND QUALIFICATIONS

5. I received a B.A.Sc. in Electrical Engineering from the University of Waterloo in Waterloo, Canada in 1992. I then received an M.S. in 1995 and a Ph.D. in 1997, both in Electrical Engineering, from the University of California at Berkeley, California. My doctoral thesis was entitled, “Robust Identification and Control of Multimodal Systems with Applications to Semiconductor Manufacturing.”

6. I am currently a tenured professor in the Department of Electrical and Computer Engineering at New York University in Brooklyn, New York. I am also Associate Director of NYU WIRELESS. I have held both positions since 2018 and have been on the faculty at New York University since 2010.

7. Prior to becoming a full professor, I was an Associate Professor of Electrical and Computer Engineering at New York University from 2010 to 2018 and was Director of NYU WIRELESS from 2016 to 2018. At NYU, my focus is in wireless communications, signal processing, and information theory.

8. From 2006 to 2010, I was Senior Director of Engineering at Qualcomm

Technologies in Bridgewater, New Jersey, where I supervised the advanced research and development group responsible for cellular communication products. I also led engineering teams in high performance base station ASICs for both the 3GPP Long-Term Evolution (LTE) and earlier 3GPP2 Universal Mobile Broadband (UMB) systems. I supervised development of PHY and MAC algorithms, ASIC simulation and verification methodologies, and MAC-layer software. I also led feasibility studies, architectural planning, and early development for a 4G femtocell ASIC. The system-on-chip (SoC) was a multimode device supporting 3G and 4G cellular standards, peak rates in excess of 300 Mbps DL and 120 Mbps UL, and contained several processors and DSPs.

9. During 2000 to 2006, I was Director of Flarion Technologies in Bedminster, New Jersey, which was a company I co-founded to commercialize Flash-OFDM, one of the first cellular OFDM data systems and a precursor to later 4G standards including WiMAX and LTE. The company grew to over 150 employees with trials with tier 1 carriers worldwide. Flarion was sold to Qualcomm for \$800 million in 2006.

10. Before that, I was a Member of Technical Staff at Bell Labs, Lucent Technologies from 1998 to 2000 and was a Postdoctoral Research Fellow at the University of Michigan at Ann Arbor, Michigan from 1997 to 1998.

11. I have authored or co-authored dozens of articles in refereed journals

and approximately 100 conference papers. I am also a named inventor on 59 issued U.S. patents. A list of my publications during the last ten years is included in my CV, which is attached as Ex-1003.

12. I have previously offered testimony as an expert witness. A list of my prior engagements for the last four years in which I testified as an expert at trial or by deposition is also included in my CV.

13. Based on my background and experience, as set forth more fully in my CV, I am familiar with the state of the art in the field of wireless communications in the 2008 time frame. I am a technical expert in the fields relating to the '918 Patent and other related fields, and I remain an active researcher in these fields.

14. Based on my professional experience, I believe I am qualified to testify as an expert on matters related to the '918 Patent.

III. INFORMATION CONSIDERED

15. In preparation for my Declaration, I have considered the materials I discuss in my Declaration, including, for example, the '918 Patent, the references cited by the '918 Patent, the prosecution history of the '918 Patent (including the references cited therein), various background articles and materials referenced in my Declaration, and the prior art references I identify in my Declaration. In addition, my opinions are further based on my education, training, experience, and knowledge in the relevant field.

IV. RELEVANT LEGAL STANDARDS

16. I am not an attorney and offer no legal opinions. For the purposes of my Declaration, I have been informed about certain aspects of the law that are relevant to my analysis, as summarized below.

A. Claim Interpretation

17. I have been informed and understand that in an IPR proceeding, claims are to be interpreted according to the Phillips claim construction standard. I understand that under this standard, the meaning of claim terms is considered from the viewpoint of a hypothetical “person of ordinary skill in the art” (“POSITA”) at the time of the alleged invention. I have been informed and understand that claim construction is a matter of law and that the final claim constructions for this proceeding will be determined by the Patent Trial and Appeal Board (“PTAB”).

18. I provide my opinions regarding terms that may require explicit construction to resolve the grounds I present in my Declaration in Section IX.

B. Perspective of One of Ordinary Skill in the Art

19. I have been informed and understand that a patent is to be understood from the perspective of a hypothetical POSITA. Such an individual is considered to possess normal skills and knowledge in a particular technical field (as opposed to being a genius). I understand that in considering what the claims of a patent require,

what was known prior to that patent, what a prior art reference discloses, and whether an invention is obvious or not, one must use the perspective of such a POSITA.

C. Obviousness

20. I have been informed and understand that a patent claim is obvious under 35 U.S.C. §103, and therefore invalid, if the claimed subject matter, as a whole, would have been obvious to a POSITA as of the priority date of the patent based on one or more prior art references and/or the knowledge of a POSITA.

21. I understand that an obviousness analysis must consider (1) the scope and content of the prior art, (2) the differences between the claims and the prior art, (3) the level of ordinary skill in the pertinent art, and (4) secondary considerations, if any, of non-obviousness (such as unexpected results, commercial success, long-felt but unmet need, failure of others, copying by others, and skepticism of experts).

22. I understand that a prior art reference may be combined with other references to disclose each element of the invention under 35 U.S.C. §103. I understand that a reference may also be combined with the knowledge of a POSITA, and that this knowledge may be used to combine multiple references. I further understand that a POSITA is presumed to know the relevant prior art. I understand that the obviousness analysis may take into account the inferences and creative steps that a POSITA would employ.

23. In determining whether a prior art reference would have been combined

with other prior art or other information known to a POSITA, I understand that the following principles may be considered:

- a. whether the references to be combined involve non-analogous art;
- b. whether the references to be combined are in different fields of endeavor than the alleged invention in the Patent;
- c. whether the references to be combined are reasonably pertinent to the problems to which the inventions of the Patent are directed;
- d. whether the combination is of familiar elements according to known methods that yields predictable results;
- e. whether a combination involves the substitution of one known element for another that yields predictable results;
- f. whether the combination involves the use of a known technique to improve similar items or methods in the same way that yields predictable results;
- g. whether the combination involves the application of a known technique to a prior art reference that is ready for improvement, to yield predictable results;
- h. whether the combination is “obvious to try”;
- i. whether the combination involves the known work in one field of endeavor prompting variations of it for use in either the same field or a

different one based on design incentives or other market forces, where the variations are predictable to a POSITA;

- j. whether there is some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill in the art to modify the prior art reference or to combine prior art reference teachings to arrive at the claimed invention;
- k. whether the combination requires modifications that render the prior art unsatisfactory for its intended use;
- l. whether the combination requires modifications that change the principle of operation of the reference;
- m. whether the combination is reasonably expected to be a success; and
- n. whether the combination possesses the requisite degree of predictability at the time the invention was made.

24. I understand that in determining whether a combination of prior art references renders a claim obvious, it is helpful to consider whether there is some teaching, suggestion, or motivation to combine the references and a reasonable expectation of success in doing so. I understand, however, that a teaching, suggestion, or motivation to combine is not required.

V. LEVEL OF ORDINARY SKILL IN THE ART

25. I am familiar with the level of ordinary skill in the art with respect to

the '344 Patent around its filing date. Based on my experience working, teaching, and conducting research in the relevant field, and based on my review of the '918 Patent specification, claims, file history, and prior art, I believe one of ordinary skill in the art around the time of the alleged invention of the '918 Patent would have had at least 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.

26. In determining the level of ordinary skill in the art, I considered, for example, the type of problems encountered in the art, prior art solutions to those problems, the rapidity with which innovations are made, the sophistication of the technology, and the educational level of active workers in the field.

27. I met or exceeded the knowledge and experience that a POSITA would have had in 2008. I have extensive experience managing and building engineering teams on large projects in the cellular space during this time period. I have additionally supervised and taught numerous undergraduate and graduate students over my career in wireless communications. In my work as a professor and entrepreneur, I worked with graduate students and others who had the knowledge and experience of a POSITA in 2008, and I am able to render opinions from the

perspective of a POSITA based on that knowledge and experience . My opinions concerning the '918 Patent claims and the prior art are from the perspective of a POSITA, as set forth above.

VI. SUMMARY OF MY OPINIONS

28. As I explain below in detail in my Declaration, it is my opinion that Claims 1-20 and 22-31 of the '918 Patent would have been obvious under 35 U.S.C. §103 on the following grounds:

- **Ground 1:** Claims 1, 4-6, 9, 14, 16-22, and 24-30 are obvious over U.S. Patent Publication No. 2007/0030824 to Ribaudo (“Ribaudo”) (Ex-1007);
- **Ground 2:** Claims 1, 4-6, 9, 14, 16-22, and 24-30 are obvious over Ribaudo in view of JP Patent Publication No. 2005/12973 to Watanabe (“Watanabe”) (Ex-1005, Ex-1006);
- **Ground 3:** Claims 2-3, 7-8, 10-13, 15, and 31 are obvious over Ribaudo in view of PCT Patent Publication No. WO2008/132241 to Behrens (“Behrens”) (Ex-1008);
- **Ground 4:** Claims 2-3, 7-8, 10-13, 15, and 31 are obvious over Ribaudo in view of Watanabe and Behrens;
- **Ground 5:** Claim 23 is obvious over Ribaudo in view of U.S. Patent

Publication No. 2005/0174975 to Mgrdechian (“Mgrdechian”);

- **Ground 6:** Claim 23 is obvious over Ribauda in view of Watanabe and Mgrdechian.

VII. TECHNOLOGICAL BACKGROUND

A. Using Beacon Transmissions to Make Proximity Determinations Was Known

29. Using beacon transmissions to make proximity determinations was known by 2008. Indeed, the periodic transmission of beacons is one of the most basic mechanisms for identifying the presence of wireless transmitters within the coverage of the transmission. For example, methods had been described by 2008 for “receiving, by a mobile first device in proximity with a second device, an identifier wirelessly transmitted by the second device” where “[t]he identifier is associated with a user of the second device” and vice versa. WO2008/076827 to Krikorian (Ex-1009, “Krikorian”) ¶¶4-5, Fig. 2.

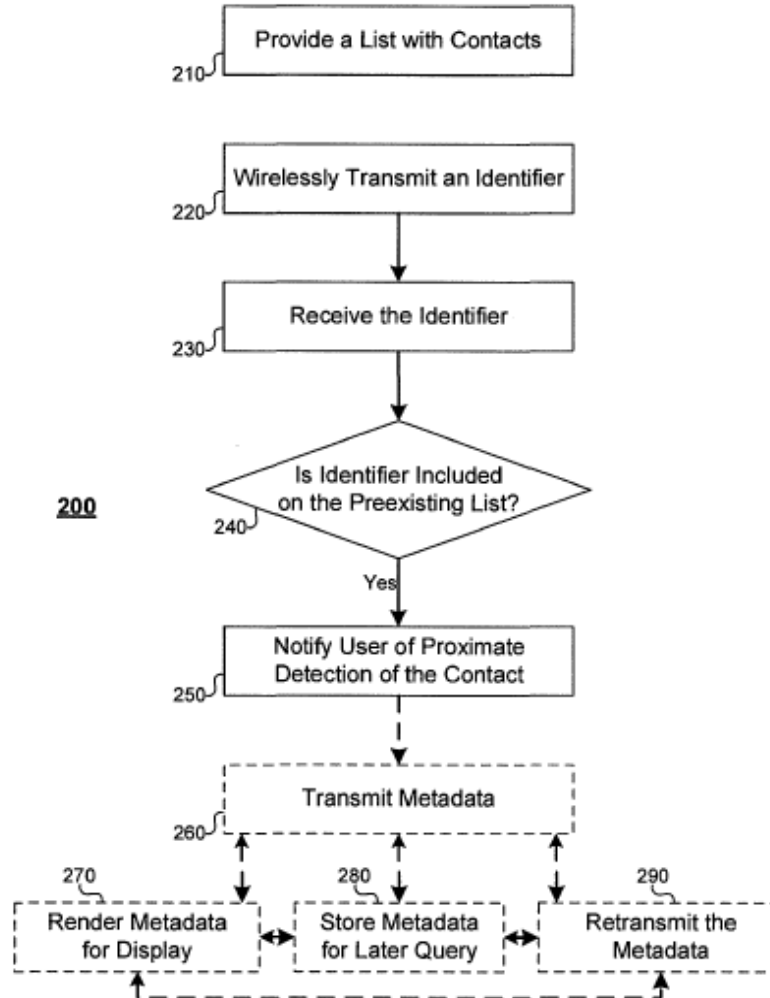


Fig. 2

It was also known that beacon transmissions may be transmitted continuously and/or periodically. Specifically, Krikorian teaches that “[w]ireless transmission by the mobile wireless device 120b of its identifier to the proximity-based wireless network 110b (220) can occur continuously, at specified or periodic times, and/or at times dependent on the remaining battery power left for the mobile wireless device 120b.”

Ex-1009 (Krikorian) ¶25. “For example, a location-based wireless device 130 associated with a public restroom can be programmed to broadcast its identifier every 30 seconds during the hours of operation of the building for which it is located.” Ex-1009 (Krikorian) ¶25. “The mobile wireless device 120a can continuously, at specified or periodic times, upon request, and/or at times dependent on the remaining battery power left for the mobile wireless device 120a, scan for proximate-based transmissions including an identifier.” Ex-1009 (Krikorian) ¶25.

30. As another example, US7000001 to Lazaridis et al. (Ex-1027, “Lazaridis”) teaches a bookmark beacon system that determines whether a guest device is in proximity to a user’s wireless device. Specifically, Lazaridis teaches “an exemplary bookmark beacon system 10” that “includes a bookmark beacon 12, a wireless device 14, and a wireless communications network 16 through which the wireless device 14 can access the Internet 18 via a proxy server 20. In addition, the bookmark beacon 12 may be physically coupled with, or in close proximity to, a guest device 22.” Ex-1027 (Lazaridis), 2:3-10. “This transmission may be a continuous transmission, or may be configured to transmit at a periodic interval.” Ex-1027 (Lazaridis), 3:44-46. “When a wireless device user 46 approaches the establishment 42, his or her wireless device 12 receives a bookmark data packet 24 from the bookmark beacon 12. The bookmark data packet 24 may then be used by

the wireless device user 46 to retrieve information relating to the commercial establishment 42.” Ex-1027 (Lazaridis), 3:59-65.

31. Similar methods and systems are also taught by US2009/0239467 to Gulin et al. (Ex-1028, “Gulin”). Specifically, Gulin teaches a “[d]evice, process and program for determining and alerting a user of the existence of nearby acquaintance, including: providing a first electronic communication device having nearfield transmitting and receiving communications capability, a user interface and control circuitry; transmitting from the first communication device an inquiry to determine the presence in the near-field of a compatible second electronic communication device; upon receipt of a positive response to the inquiry, transmitting from the first communication device anonymous user indicia; receiving anonymous user indicia from the second communication device; coordinating the received anonymous user indicia to determine the presence of any matches between the transmitted anonymous user information and the received anonymous user indicia; and providing either a list of matches or an indication of no matches to the user via the user interface.” Ex-1028 (Gulin), Abstract. “Based on the information exchanged, the users can determine whether a relationship between the users exists or might be created.” Ex-1028 (Gulin), Abstract.

32. *See also* US2004/0248569 to Kondou et al. (Ex-1029, “Kondou”) ¶1 (“The present invention relates to a portable terminal having means for connecting

to a wireless public network and short distance wireless communication means. More specifically, the present invention relates to a portable terminal having a function of detecting other person's approach utilizing short distance wireless communication means.”); Ex-1010 (Mgrdechian) ¶73 (“Referring again to FIG. 3A, the process may be A) initiated when an initiating user (e.g., User is interested in obtaining information about another user. For example, as mentioned above, User A may be in the same physical location as User B, and User A may want to meet User B but the conditions are not conducive with a direct communication. Embodiments of the present invention allow a user (e.g., User A) to view information about, and/or send a message to, another user (e.g., User B) if the other user is operating a wireless device in the same area. In one embodiment, an initiating wireless device 310 (i.e., Device A) sends an identification request (i.e., a query or scan) to other wireless devices within range. A plurality of other wireless devices 320 (i.e., Device B) and 380A-380N may receive the request. One or more of the wireless devices 320 and 380A-380N may have wireless device identifications (‘device IDs’) stored internally (e.g., ID 323 in Device B). When an identification request is received, one or more of these devices may access and transmit a device ID back to initiating device 310 in a reply.”); US2006/0287813 to Quigley et al. (Ex-1030, “Quigley”), Abstract (“The device is then able to passively detect and identify beacons within its physical proximity. The identity of the detected beacons is then compared with the

downloaded data to determine their location which is then displayed to the user as their proximate location within the general geographic area.”); US2003/0220114 to Langensteiner et al. (Ex-1033, “Langensteiner”) ¶¶20-21 (“the first beacon device transmits a received identifier to said second beacon; and the second beacon and portable device perform said service interaction when the portable device is within a second broadcast range of the second beacon and when triggered by the second beacon receiving the portable device identifier, with at least one of the first and second broadcast ranges being relatively short”).

B. The Use of MAC Addresses, Unique Identifiers, and Beacon Service Identifiers to Identify Devices and Networks Was Known

33. Using MAC addresses, Bluetooth addresses (such as BD_ADDR), and other unique identifiers to identify devices and networks was known by 2008. Such identifiers are a basic feature of virtually every commercial communication system to distinguish different devices in a network. For example, Krikorian teaches that a “mobile wireless device 110 and/or a location-based wireless device 130 can be identified by a unique and/or a standardized identifier. For example, a unique identifier can be a Bluetooth ID, a MAC address, or other unique identifier. A standardized identifier, for example, can be associated with one or more devices, locations, events and/or labeled spaces. In one example, a standard identifier can be associated with all store and/or office locations of a certain company or

organization.” Ex-1009 (Krikorian) ¶21. Krikorian’s figure 3 “illustrates an exemplary contact list 300 for mobile proximity-based notification. The contact list 300 includes an identifier field 310, a name field 320, a type field 330, a source field 340, and/or another information field 350. The identifier field 310 can include entries of one or more identifiers (e.g., Bluetooth IDs). Each entry in the identifier field 310 can be associated with an entry in the name field 320. The name field 320 can include personal names, location-based names, event names, space names, and/or other names. For example, the identifier ID4 can be associated with all Verizon Service Stores in one or more regions. In another example, identifier ID5 can be associated with Erika’s cell phone, identifier ID6 can be associated with Erika’s blackberry, and identifier ID7 can be associated with Erika’s laptop.” Ex-1009 (Krikorian) ¶23, Fig. 3; *see also* Ex-1029 (Kondou) ¶35 (“A Bluetooth address can be used as the device ID that is exchanged and stored when communication is performed via the wireless public network (for example, when the telephone communication is finished). The Bluetooth address is determined uniquely to each short distance wireless communication device, so there is no wireless communication device having the same Bluetooth address. Therefore, a Bluetooth address and a portable terminal can have a one to-one correspondence.”).

34. These features were also taught by US2005/0130634 to Godfrey (Ex-1031, “Godfrey”). Godfrey teaches that “one or more of the wireless stations 140-

172 may be adapted to identify proximate wireless devices and determine one or more user IDS associated with the user or users of the proximate wireless devices. A user's ID may include, for example, a login ID Supplied by the user to enable the user's use of the wireless station, an email address associated with the user and used by an email client operating on the wireless station, a user ID associated with one or more software programs operating on the wireless station, such as an instant messenger client, and the like.” Ex-1031 (Godfrey) ¶34. Godfrey also teaches that “[t]he poll response frames 404 and 406 may include, for example, data representing the MAC address of the proximate wireless station sending the poll response frame, an indicator of the type of wireless station (e.g., PDA, notebook computer, cell phone, etc.), one or more user IDs associated with the wireless station, and the like.” Ex-1031 (US2005/0130634) ¶54. And “rather than transmitting a poll response frame in response to a poll frame 402, the wireless stations 202,222, and 224 may be adapted to periodically transmit a beacon frame, similar to the poll response frames 404 and 406, identifying the MAC address, type, user ID, etc., of the wireless station transmitting the beacon frame.” Ex-1031 (Godfrey) ¶55.

35. See also Wayne Jansen et al., Proximity Beacons and Mobile Device Authentication NISTIR 7200 (June 2005) (Ex-1032, “Jansen”), 23 (“Beacon Table[:] The handler maintains a table of prospective beacons to carry out its function. The table contains the information about all Bluetooth devices in the

vicinity of the mobile device. The table has the following fields: MAC Address, Last Seen, Last Contact, and Status. An example of such a table is shown below.”), 24 (“The handler populates the table by performing a Bluetooth inquiry process every 50 seconds. The inquiry discovers Bluetooth devices in the vicinity and returns a list of their MAC Addresses. The handler looks up each MAC Address received during the inquiry process to see if it already exists in the beacon table. If the address does not exist, it is entered into the table. For every MAC Address received during the inquiry process, the handler updates the corresponding Last Seen entry in the handler table.”); Ex-1033 (Langensteiner) ¶38 (“the system suitably correlates the mobiles Bluetooth device ID’s with their wide area addresses (phone nos.), for example by pre-registration”); US2008/0261526 to Suresh (Ex-1034, “Suresh”) ¶¶39 (“Device printer (216) identifies the make and model of the device communicating with the system by the radio id and/or BDADDR of the device which would allow access point to fine tune the mode and format communication with the device.”), 58 (“FIGS.5A and 5B illustrate the flow of the method for identifying and reaching new and existing customers to sign up to loyalty program, where mobile devices of customers have short range connectivity like Bluetooth and have capability to send SMS messages. The method comprising the steps of a customer having short range connectivity activated on his mobile device (501); the access node recognizing the mobile device which has short range connectivity activated (502) and the access

node sending the mobile device a request for connectivity (503). Once the customer accepts the connectivity request (504), the mobile device is requested by the access node to send an SMS with a short range ID over the AT channel (506). The short range ID is a unique combination of the customers' phone number along with the Bluetooth ID of the mobile device. The customer also has an option to send his name and email ID over short range connectivity to the access node (505)."); Ex-1028 (Gulin) ¶69 ("In one aspect of the invention, a mobile telephone initiates a search for electronic equipment having a predetermined modality and within communication range of the mobile telephone. This may include a cellular telephone carrier's system. Electronic equipment capable of responding to the request (e.g., another near-field user's electronic equipment such as a second mobile telephone) transmit information through a local interface adapter. Such information may include, for example, an inquiry including information such as a unique identifier and, optionally, additional unique identifiers of friends known to the inquiring user. The unique identifier may be any unique characteristic, item or feature that may be assigned to a contact, and the unique identifier is anonymous in that while it is unique to any individual person, it does not actually identify that person, except to others who know the individual person and have that person's anonymous unique identifier associated with the person's actual identity. Herein, the unique identifier is referred to as the person's anonymous identity, or ANON_ID. The ANON_ID could, for

example, be a unique identifier such as a telephone number, a session initiation protocol (SIP) address, or an encrypted name of the person, or a 128-bit unique identification number encrypting, e.g., a name. In any case, the ANON_ID is unique to the individual person, so that each individual using the system of the present invention is uniquely identified by the ANON_ID. Each individual user of the system of the present invention has stored in the user's electronic equipment a list of ANON IDs and an associated list of additional variously detailed information about the actual person associated with a given ANON_ID."); Ex-1010 (Mgrdechian) ¶¶50 ("The preferred embodiment of the present invention would also include (e.g., as part of the server) a web-based user interface for registration and profile management. Information provided by users through this interface would include, but not be limited to the Bluetooth ID of their mobile device, their name, address, billing information (if applicable), username, profile information, photo, preferences and names of friends."), 91 ("In one embodiment, the wireless device IDs 813 and 823 are unique identifications. If a unique ID is stored in the wireless device, a local application may be included for retrieving the unique ID. One example unique ID is shown in system 800, wherein the unique identifications are Bluetooth IDs (e.g., IDs 813 and 823). In other embodiments, the unique ID may be an RFID or another equivalent identification for uniquely identifying the wireless device. Another example of a unique identification is a unique identification number

assigned to a communication device by the device manufacturer. A device manufacturer, in coordination with the other device manufacturers, may have policies for assigning such unique IDs such that each communication device is provided with a unique ID in the manufacturing process. In some applications, unique IDs, once assigned, are often never changed or reused. A unique ID can then be used to uniquely identify a given device with a common communication network shared by all communication devices.”).

36. It was also known that a plurality of MAC addresses could be used to identify a single device and/or network. For example, US2009/0059878 to Tamura (Ex-1035, “Tamura”) teaches that “one MAC 100 is physically provided but operable as a plurality of virtual media access controllers (hereinafter referred to as ‘virtual MACs’). FIG. 4 shows an example to provide four virtual MACs, i.e., ‘virtual MAC1,’ ‘virtualMAC2,’ ‘virtualMAC3,’ and ‘virtualMACz.’ The virtual MAC1, MAC2 and MAC3 are used for normal wireless communication such as data communication with the terminal. The virtual MACZ operates during an exchange of security information for a negotiation of security information in a register mode to register an additional terminal to the wireless LAN. The MAC 100 is operable on the CPU 50 to processes data for the virtual MAC1, MAC2, MAC3 and MACZ in a time sharing manner to allow the virtual MAC1, MAC2, MAC3 and MACz to operate substantially in parallel. The virtual MAC1, MAC2 and MAC3 are operable

to perform encrypted communication using encryption schemes respectively selected thereto (e.g., different encryption schemes can be selected). As a matter of course, all the virtual MAC1 to MACZ are provided within the housing 40.” Ex-1035 (Tamura) ¶47, Fig. 4. Moreover, Tamura teaches that “AP 10 is operable as a plurality of virtual sub-access points (hereinafter referred to as ‘sub-Aps’) that apparently independently operable after the software for implementing MAC is installed on the AP 10. Specifically, in the present embodiment, a plurality of subAPs are virtually multiplexed to the AP 10 to perform actual communication with terminals 20, 22 and 24. The sub-API, sub-AP2 and sub-AP3 can perform encryption communication with encryption schemes independently selected for the respective sub-API, sub-AP2 and sub-AP3.” Ex-1035 (Tamura) ¶48.

37. Using beacon service identifiers to identify devices, networks, and/or services was also known by 2008. For example, both service set identifiers (SSIDs) and basic service set identifiers (BSSIDs) were known to be used to identify devices, networks, and/or services was also known by 2008—either of which would have been considered a beacon service identifier by a POSITA. Tamura teaches that “an SSID (Service Set ID) is assigned to each of the sub-APs as a identifier unique thereto. The terminal 20, 22 and 24 can identify each of the sub-Aps distinguishably based on the SSIDs received from the respective sub-APs. For each of the normal sub-APs 1 to 3, the type of an encryption scheme (represented by ‘Sec Type’ in FIG.

4) and a value of an encryption key (represented by ‘Sec Key’ in FIG. 4) adopted by the normal sub-APs 1 to 3 and SSID are associated with one another. Likewise, for each terminal, the SSID of a sub-AP used by each of the terminals 20, 22 and 24, the type of an encryption scheme adopted by each of the terminals 20, 22 and 24, and the value of an encryption key adopted by each of the terminals are associated with one another.” Ex-1035 (Tamura) ¶53. Specifically, Tamura teaches that “the target terminal 20 obtains an SSID of the accessible normal sub-AP. This process is performed in conformance with communication specifications specified in the standard IEEE 802.11. Accordingly, the specific beacon includes an SSID of the normal sub-AP. Upon receipt of a specific beacon transmitted from the normal sub-AP, the target terminal 20 can obtain the SSID of the currently-accessible normal sub-AP. The target terminal 20 compares the obtained SSID of the normal sub-AP with the previously received security information. As a result of the comparison, the target terminal 20 specifies the encryption scheme adopted by the normal sub-AP for establishing communication (encryption and decryption) with the target terminal 20 and the value of an encryption key are specified.” Ex-1035 (Tamura) ¶140. Moreover, Tamura teaches that “MAC 100 serves as an example of the one physical MAC. The respective virtual MACs 1, 2, and 3 serve as examples of the virtual MACs, and SSIDs of the respective virtual MACs 1, 2, and 3 serve as examples of identifiers.” Ex-1035 (Tamura) ¶173.

38. See also Sorte et al., *Service publishing to support an efficient network selection in an 802.11 multi-access environment* (Jan. 2006) (Ex-1039, “Sorte”) 4 (“A VAP is a physical AP in which a number of logical entities, named VAP profiles, exist. Each VAP profile appears to be an independent, physical AP and emulates the operation of a physical AP at the MAC layer (it represents an instantiation of a complete 802.11 MAC including BSSID, SSID, and capability set). One of the main advantages of this architecture is that a WISP can differentiate the offered services within the same physical AP. In principle, a number of WISPs can also share the same physical device. Thus, a VAP device is quite suitable for the deployment of a multi-service WLAN. In addition, VAP technology enables VLANs to be extended to the wireless segment of the network. In our lab we make use of a Colubris MSC3200 with VAP technology which supports up to 16 concurrent SSID/BSSIDs.”), 5 (“Service publishing: beacon-based. Service-related information is included within the SSID IE, as explained at the end of this subsection. SLP-based. We group services by means of the SLP scope mechanism on the basis of the different wireless network accesses (i.e., SSIDs). This means that each service is associated with one or more SSIDs, and we also have the differentiation of the service publishing at the SLP level. In other words, the query to the SLP server from an MT indicates the SSID of the AP the MT is currently attached to. Thus, the SLP server replies with the information of the services belonging to the scope with which

the SSID is associated.”); US8411662 to Saund et al. (Ex-1036, “Saund”), 1:63-2:9 (“The present invention relates to providing new capabilities for the IEEE 802.11 beacon. In 802.11, data frames carry information from higher layers. However, management and control frames must be provided that support data transfer. The beacon frame is a type of management frame. wireless local network requires these management frames for stations to establish and maintain communications. A typical beacon frame is about fifty bytes long. It contains a common frame header and cyclic redundancy checking field, including others. The beacon also contains a service set identifier (SSID). The SSID identifies a specific wireless local area network. Before associating with said network, a wireless device must have the same SSID as the access point.”), 2:25-30 (“The IEEE 802.11 beacon is able to transmit a 32-character network identifier. This network identifier is only intended to carry the name of the network. Actual capabilities of the network are carried in other IE’s. The invention system comprises additional uses for the SSID to include reliable and secure capability encoding.”), 2:45-63 (“The IEEE 802.11 beacon SSID is adapted to serve as a capabilities encoding channel. For example, encoded capabilities and preferences are incorporated into the SSID to determine: Group membership: such as invited members of a conference or game playing group. User preferences: Device capabilities: System location: Game state: Such as a point of play in a computer game. Encryption and security preferences: Application Software state. Such as

viewing a specific file. The following are further examples of the invention system incorporating the use of SSID transmission of information: Encoding of information where the information is encrypted. Encoding of information: Such as where information is integrity protected (checksum, secure hash, keyed hash, digital signature).”), 3:9-12 (“After obtaining encoded SSID, device may use central server to assist in decoding. Central server may return additional identity or location information.”); US2008/0045181 to Suzuki (Ex-1037, “Suzuki”) ¶¶46 (“The wireless-communication-setting-data-retention unit 125 is configured to retain setting data used for performing wireless communications. For example, a service-set identifier (SSID), security-setting data, the MAC address of the bridge terminal 120, and so forth are retained, as the setting data. Here, the SSID is an identifier used for identifying the wireless ad-hoc network 290. For example, an arbitrary character string input by a user is used, as the SSID. Further, a code, an identifier, and so forth used for a robust security network (RSN) can be retained, as the security-setting data.”), 50 (“For example, an SSID used to identify the wireless ad-hoc network 290, security setting data including a code, an identifier, and so forth that are used for the RSN, the MAC address of the wireless terminal 200, the current identification-server metric of the wireless terminal 200, and so forth are retained, as the setting data.”), 55 (“The terminal identifier 611 of each of the neighboring terminals may be the MAC address of the wireless terminal corresponding to the neighboring terminal.”),

57 (“The transmission-destination-terminal identifier 621 and the relay terminal 622 may be the MAC address of the corresponding wireless terminal, for example. Further, the authentication-server metric 623 may be the number of hops of a path leading to the bridge terminal 120 and/or a value including the wireless-communication quality of each of links of the path.”); WO2006/028640 to Briancon et al. (Ex-1038, “Briancon”) ¶7 (“Figure 2 is an illustration of an access point (AP) 14 running multiple 802.11 type wireless networks. The access point 14 and the wireless transmit/receive units (WTRUs) 161, 162, 16s, 164 (16) in the AP's effective operating area form a basic service set (BSS) 18. As illustrated, the BSS 18 has an associated BSS identification 1 (BSSID 1) code of ‘AA:AA:AA:AA:AA:AA’. The AP 14 is also supporting four (4) virtual wireless local area networks (V-WLANs) 12, V-WLAN 1121 (faculty and administrators), V-WLAN 2 122 (students), V-WLAN 3 123 (facilities and security) and V-WLAN 4 124 (guests and visitors). Each V-WLAN 12 has an associated extension service set (ESS) linking the AP's portion of the V-WLAN 12, such as by layer 2, to other APs' portions of the VWLAN 12. Each ESS has an associated ID, ESSID 1, ESSID 2, ESSID 3 and ESSID 4. The presentation of each of the multiple V-WLANs to the WTRUs 16 by the AP 14 can be referred to as a virtual AP (V AP). The use of V APs reduces the number of physical APs 14 that are needed to implement multiple networks and allows for reduced interference and collisions.”).

C. Including Identifiers in Beacon Transmissions Was Known

39. Including identifiers in beacon transmissions was known by 2008. For example, Krikorian teaches a method that “includes receiving, by a mobile first device in proximity with a second device, an identifier wirelessly transmitted by the second device. The identifier is associated with a user of the second device.” Ex-1009 (Krikorian), Abstract, ¶4. “The method includes wirelessly transmitting, by a first device, an identifier associated with a user of the first device.” Ex-1009 (Krikorian) ¶5. “The identifier can be a unique ID. The identifier can be a standardized ID.” Ex-1009 (Krikorian) ¶8. “Mobile proximity-based notification includes providing a list of contacts to the mobile wireless device 120a (210), wirelessly transmitting to the proximity-based wireless network 110b an identifier by the mobile wireless device 120b (220), receiving the identifier by the mobile wireless device 120a (230), determining whether the identifier is included on the preexisting list (240), and/or notifying a user of the mobile wireless device 120a of proximate detection of a contact (250). Mobile proximity-based notification can further include transmitting metadata and/or other information between the mobile wireless devices 120a and 120b (260), rendering the metadata for display (270), storing the metadata for later query (280), and/or retransmitting the metadata (290).” Ex-1009 (Krikorian) ¶22.

40. This is also taught by Lazaridis. Lazaridis teaches “[a] bookmark

beacon system comprises a computer network, a wireless network configured to enable a wireless device to access the computer network, and a bookmark beacon that transmits a bookmark data packet to the wireless device. The bookmark data packet includes a resource address that enables the wireless device to retrieve information stored on the computer network.” Ex-1027 (Lazaridis), Abstract. Lazaridis further teaches “a system and method for a bookmark beacon that enables communication with any device having access to a computer network, such as the Internet.” Ex-1027 (Lazaridis), 1:16-20. “The bookmark data packet 24 transmitted by the bookmark beacon 12 preferably includes a resource address, such as an IP address or a Uniform Resource Locator (URL), that 40 enables the wireless device 14 to locate a network server 26 and website 28 over the Internet 18. Alternatively, the resource address may enable a network connection directly to the guest device 22. The data packet 24 may also include a limited amount of text describing the purpose of the bookmark beacon 12.” Ex-1027 (Lazaridis), 2:37-45. Moreover, Lazaridis teaches “one or more printers coupled to the computer network, wherein each printer has a unique printer address on the computer network; a bookmark beacon associated with each printer that transmits a bookmark data packet identifying the unique printer address of the associated printer, wherein the bookmark data packet can be received by the plurality of wireless devices; and a message server having a unique location on the computer network that transmits and

receives electronic messages to and from the plurality of wireless devices over the computer network and wireless network, and that is also configured to (a) receive one of the unique printer addresses from one of the wireless devices, and (b) transmit an electronic message identified by the one wireless device over the computer network to the printer associated with the one unique printer address.” Ex-1027 (Lazaridis), 7:65-8:14.

41. This feature is also taught by Mgrdechian. Mgrdechian teaches that “[i]n one embodiment, the method further comprises, on the first wireless device, transmitting a wireless identification request. In another embodiment, the method further comprises transmitting the information associated with the at least one wireless device identification from the remote computer system to the first wireless device. In another embodiment, the method further comprises receiving the information associated with the at least one wireless device identification.” Ex-1010 (Mgrdechian) ¶13. “In another embodiment, the one or more wireless device identifications are unique identifications. In yet another embodiment, the unique identifications include a Bluetooth identification or an RFID.” Ex-1010 (Mgrdechian) ¶14. Mgrdechian further teaches that “a communication process is initiated by a user (the ‘Sender’ or ‘User A’, using ‘Device A’) interested in viewing the profile of another user (the ‘Recipient’ or ‘User B’, using ‘Device B’), identifying any mutual friends they may have in common or in sending a message

to them. To begin this process, Device A broadcasts a wireless inquiry to neighboring devices, including Device B, requesting that they provide their unique identification numbers to Device A. Upon receipt of this inquiry, each device, including Device B, broadcasts its unique ID back to Device A. The inquiry by Device A can be made in any number of ways including a directional electromagnetic or ultrasonic beam sent from Device A in the direction of Device B which queries an RFID tag or similar device, or through an omni-directional method or wireless protocol (such as any Bluetooth or any 802.11 standard) in which all devices within a given distance are queried.” Ex-1010 (Mgrdechian) ¶26. “In one embodiment, response to the inquiry for an ID may be done via the same wireless protocol as the inquiry. In one embodiment, the response to the inquiry for an ID may be done or via a different wireless protocol as the inquiry. In addition, embodiments of the devices can include cases where the ID’s are static, dynamic or pseudo-random.” Ex-1010 (Mgrdechian) ¶27. “Upon receipt of the unique ID of Device B (and of any other devices that respond to the inquiry for their ID), Device A may upload these IDs to a central service which may include a website, a database and one or many servers. The system will then match the IDs provided by Device A with those of registered users and download the images of the users associated with the IDs back to Device A.” Ex-1010 (Mgrdechian) ¶28. “In another embodiment, a device may continuously or intermittently broadcast its ID and/or other information without

having received an inquiry.” Ex-1010 (Mgrdechian) ¶42.

42. This feature is also taught by Suzuki. Suzuki teaches that in Figure 6 “the format of a beacon frame generated by the Institute of Electrical and Electronics Engineers (IEEE) 802.11 standard. A beacon frame 520 is used to transmit beacon information of a MAC sub layer. The beacon frame 520 includes a MAC header 521, a frame body 530, and a frame check sequence (FCS) 529. The MAC header 521 includes data on a frame control 522, a period 523, a reception-destination address 524, a transmission source address 525, a basic-service-set identifier (BSSID) 526, and a sequence control 527.” Ex-1037 (Suzuki) ¶59, Fig. 6. “The BSSID 526 is provided to retain data on a basic-service-set identifier (BSSID) defined by the IEEE 802.11 standard. In the ad-hoc mode, the MAC address of the first wireless terminal started on a network to which the wireless terminal belongs is used.” Ex-1037 (Suzuki) ¶63. “The beacon frame 520 includes data on a time stamp 531, a beacon period 532, function information 533, an SSID 534, corresponding speed 535, an RSN 538, and so forth, as the frame body 530.” Ex-1037 (Suzuki) ¶66. “The function information 533 shows various types of information relating to a point-coordination function (PCF), data encryption, and so forth. The function information 533 includes information about network-operation mode indicating whether a wireless terminal which transmits data is a basic-service set (BSS) under the control of an access point used in infrastructure mode, or an independent basic-service set (IBSS) used in the

ad-hoc mode.” Ex-1037 (Suzuki) ¶68. “The SSID 534 shows a service-set identifier used to identify the wireless ad-hoc network 290. The corresponding speed 535 shows the list of supported wireless-transfer rates. The RSN 538 is a field provided to retain information including a code, an identifier, and so forth that are used for the RSN.” Ex-1037 (Suzuki) ¶69. Suzuki further teaches that “FIG. 7 shows example data items included in an RSN field according to an embodiment of the present invention. The RSN 538 of the beacon frame 520 retains security-setting data including a code, an identifier, and so forth that are used to make a network robust.” Ex-1037 (Suzuki) ¶70, Fig. 7. Moreover, “FIG. 9 shows the format of a probe-response frame 570 generated by the IEEE 802.11 standard. The probe response frame 570 is used by a wireless terminal to which the probe-request frame 550 had been transmitted, so as to respond to the probe-request frame 550.” Ex-1037 (Suzuki) ¶77, Fig. 9. “The probe-response frame 570 is used to transmit a probe response generated in the MAC sub layer and includes data on a MAC header 571, a frame body 580, and an FCS 579. Here, the MAC header 571 and the FCS 579 have the same configurations as those of the MAC header 521 and the FCS 529 of the beacon frame 520 shown in FIG. 6. However, a subtype 5722 shows the probe response.” Ex-1037 (Suzuki) ¶78. “Further, the frame body 580 corresponds to the payload of the probe-request frame 570 and is used to transfer data existing in the MAC sub layer. The frame body 580 includes data on a time stamp 581, a beacon

period 582, function information 583, an SSID 584, corresponding speed 585, RSN 588, and so forth, and has the same configuration as that of the beacon frame 520 shown in FIG. 6.” Ex-1037 (Suzuki) ¶79. Additionally, it teaches that “[e]ach of FIGS. 10 and 11 shows example processing procedures performed by the wireless terminal 200 according to an embodiment of the present invention. Upon receiving the beacon frames 520 and/or the probe-response frames 570 transmitted from different wireless-communication devices, the wireless terminal 200 selects an unauthenticated neighboring terminal having network parameters agreeing with those of the wireless terminal 200, at step S911. The term ‘network parameters’ denotes an SSID, network-operation mode, security-setting data, and so forth. Namely, the wireless terminal 200 compares network parameters included in the SSID 534, the function information 533, and the RSN 538 of the beacon frame 520 and/or the SSID 584, the function information 583, and the RSN 588 of the probe-response frame 570 to the wireless-communication-setting data retained in the wireless-communication-setting-data-retention unit 205. Further, the wireless terminal 200 can determine whether or not the neighboring terminal is authenticated by referring to the authentication state 612 corresponding to the terminal identifier 611 shown on the neighboring-terminal list 610 based on the transmission-source address 525 of the beacon frame 520 and/or the transmission-source address 575 of the probe-response frame 570.” Ex-1037 (Suzuki) ¶83, Figs. 10-11.

43. See also US6928263 to Blake et al. (Ex-1040, “Blake”), 2:39-46 (“The system may comprise just one or a plurality of second beacon devices, each arranged to receive identifiers from the first beacon, and there is suitably a secure data channel linking the first to the or each second beacon device for the transmission of received identifiers. The second beacon device may maintain and periodically update a list of identifiers for portable devices with which a service interaction is being performed.”); Ex-1033 (Langensteiner) ¶14 (“The system may comprise a plurality of second beacon devices, each arranged to receive identifiers from the first beacon.”); Ex-1030 (Quigley) ¶¶15-16 (“c) the mobile location indicating device passively detecting one or more beacons within the proximity of the mobile location indicating device, and determining the unique identifier(s) of said one or more detected beacons; d) the mobile location indicating device comparing the determined unique identifier(s) with the downloaded data, thereby determining respective location data of said one or more detected beacons”); Ex-1039 (Sorte), 1 (“-In a multi-access and multi-service 802.11 environment, the problem of providing users with useful service-related information to support a correct, rapid network selection is expected to become a very important issue. In this paper, we propose a feasible, short-term 802.11-tailored solution for service publishing. To achieve a working solution compliant with existing equipment, our suggestion is to publish service information encoded within the SSID Information Element within beacon frames.

... - As is well known, APs periodically broadcast (every 100 ms) management frames (beacons), which include a number of pieces of information within fixed-length mandatory frame body components (Fixed Fields, FFs), together with variable-length mandatory and optional frame body components (Information Elements, IEs). This mechanism provides a means for MTs to discover not only APs but also certain service capabilities. An IE consists of three fields: the ID of the IE, the length of the body, the body. The SSID (Service Set IDentity) is an IE (with ID=0) containing the name of the network, the maximum length of which is 32 octets (i.e., 32 ASCII characters). ... To achieve a working solution compliant with existing equipment, our suggestion is to publish service information encoded within the SSID, where the network name is correctly separated from the other set of information.”), 2 (“Service-related information is published within the SSID.”).

D. Periodic Transmission of a Beacon Signal Was Known

44. Transmitting a beacon signal periodically was known by 2008. For example, the IEEE 2005 Bluetooth specification (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-1026) defines a “*beacon train*” as “A pattern of reserved slots within a basic or adapted piconet physical channel. Transmissions starting in these slots are used to resynchronize parked devices.” Ex-1026 (Bluetooth Specification), Fig. 72. The Bluetooth

specification further explains that: “The beacon train consists of one beacon slot or a train of equidistant beacon slots that is **transmitted periodically** with a constant time interval. The beacon train is illustrated in Figure 72. A train of N_B ($N_B \geq 1$) beacon slots is defined with an interval of T_B slots. The beacon slots in the train are separated by Δ_B . The start of the first beacon slot is referred to as the beacon instant and serves as the beacon timing reference. The beacon parameters N_B and T_B are chosen so that there are sufficient beacon slots for a parked slave to synchronize to during a certain time window in an error-prone environment.” Ex-1026 (Bluetooth Specification) at 131-32.

45. The Bluetooth specification further explains that “The beacon train serves four purposes: a) Transmitting master-to-slave packets that the parked slaves can use for resynchronization b) Carrying messages to the parked slaves to change the beacon parameters c) Carrying general broadcast messages to the parked slaves d) Unparking one or more parked slaves.” Ex-1026 (Bluetooth Specification) at 132.

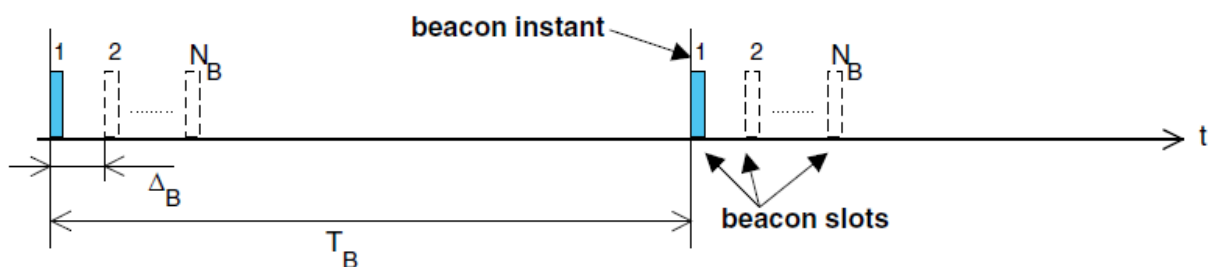


Figure 72—General beacon train format

Ex-1026 (Bluetooth Specification), Fig. 72.

46. As another example, the IEEE 2007 Wi-Fi Specification (IEEE Standard 802.11, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications) (Ex-1025, “Wi-Fi Specification”), explains that: “In an infrastructure BSS, ... The AP shall **periodically transmit** special frames called **Beacon frames** that contain a copy of its TSF timer to synchronize the TSF timers of other STAs in a BSS. A receiving STA shall always accept the timing information in Beacon frames sent from the AP servicing its BSS. ... Beacon frames shall be generated for transmission by the AP once every dot11BeaconPeriod TUs.” Ex-1025 (Wi-Fi Specification) at 419. Figure 11-1 below shows beacon transmissions included within a Beacon frame. Note, here “TSF” refers to the timing synchronization function in the Wi-Fi specification.

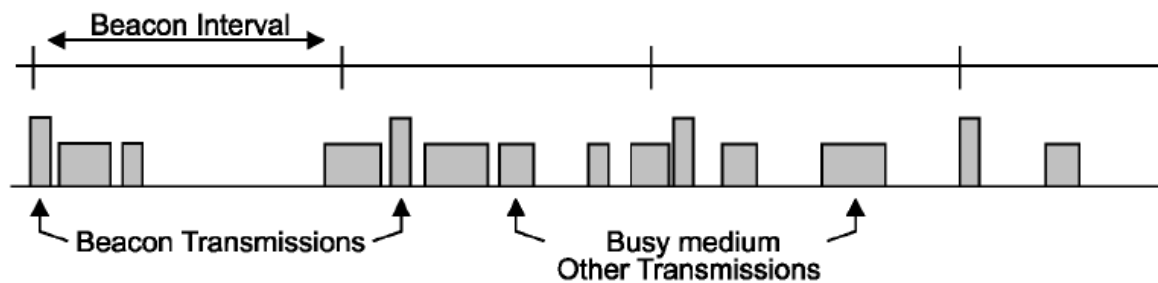


Figure 11-1—Beacon transmission on a busy network

Ex-1025 (Wi-Fi Specification) at 420.

47. Details regarding the “Beacon frame format” are provided in Table 7-8 of the specification. Ex-1025 (Wi-Fi Specification) at 80-81.

E. Storing Information at Servers and Mobile Devices Communicating with Servers to Obtain Stored Information Was Known

48. Storing information at servers and mobile devices communicating with servers to obtain stored information was known by 2008. For example, Krikorian teaches “transmitting metadata between the mobile first device and the second device. Transmitting the metadata can be in response to a request from the first or second device. In one embodiment, the method can further include rendering the metadata for display to the user of the mobile first device or the user of the second device. In another embodiment, the method can further include storing the metadata for local querying at a later time. In yet another embodiment, the method can further include transmitting the metadata to a third device when the third device is in proximity with the first or second device.” Ex-1009 (Krikorian) ¶9. Furthermore, Krikorian teaches that “[p]roviding a list of contacts to the mobile wireless device 120a (210) includes locally storing the list in memory on the mobile wireless device 120a. ... In another example, providing the list can include receiving the list, or a portion thereof to be added to a preexisting list on the mobile wireless device 120a, from a remote server or from a proximate wireless device 120 or 130. Access to the remote server can be via a cellular or broadband wireless network used by the mobile wireless device 120a. Providing the list by a remote server can occur at specified and/or at periodic times, or by request. one example, the remote server can be

associated with the email system used by the user of the mobile wireless device 120a and send contacts included in the user's address book (e.g., all contacts in the user's Outlook account, or Gmail account). In another example, the remote server can be associated with a social networking site used by the user of the mobile wireless device 120a. Social networking sites can include MySpace, Facebook, Linkedin, any online dating service, and/or any other social networking services. The social networking server, for example, can send contacts included in the user's contact list (e.g., all friends, friends of friends, and/or date matches, etc.). In yet further examples, the remote server can be associated with other services that the user of the mobile wireless device 120a has an account with (e.g., flickr, HeyLetsGo).” Ex-1009 (Krikorian) ¶24.

49. This is also taught by Lazaridis. Lazaridis teaches that “[o]perationally, the bookmark beacon 12 transmits a bookmark data packet 24 to the wireless device 14, including information that is used by the wireless device 14 to access a network server 26 having a website 28 associated with the guest device 22. Through an Internet connection, the wireless device 14 may, for example, communicate with the guest device 22, retrieve information relating to the guest device 22, or interact with applications associated with the guest device 22. Alternatively, if the guest device 22 has a network connection, the bookmark data packet 24 may provide the wireless device 14 with the information necessary to directly access the guest device 22 (such

as an IP address for the guest device 22).” Ex-1027 (Lazaridis), 2:11-23. “[B]ookmark beacon 12 could be used independently to communicate information, such as an advertisement, to a nearby wireless device 14.” Ex-1027 (Lazaridis), 2:34-36. Moreover, “the web server 46 and web pages 48 are preferably accessed by the wireless device 14 through a wireless network 16 that is linked to the Internet 18 by a proxy server 20. Once the web pages 48 are accessed by the proxy server 20, information relating to the commercial establishment 42 is collected, and the information is delivered to the wireless device 14 in step 3. The information delivered from the web pages could include, for example, advertisements, sales, or any other information relating to the commercial establishment.” Ex-1027 (Lazaridis), 4:10-20, Fig. 1. Lazaridis further teaches “an exemplary method 50 for retrieving information on a wireless device relating to a guest device having a bookmark beacon. The method begins at step 52 when a wireless device comes within proximity of a bookmark beacon. In step 54 the bookmark beacon transmits a bookmark data packet that is received by the wireless device. Once the bookmark data packet is received, the wireless device stores the bookmark data packet to enable a wireless device user to retrieve the information necessary to communicate with the guest device (step 56). If the wireless device user chooses to interact with (or receive information concerning) the guest device (step 58), then the mobile device contacts a web site identified by the bookmark data packet (step 60). In step 62, the web site

preferably determines the relevant information regarding the guest device such as protocols and drivers that the user requires, and then downloads that information to the user's mobile device. The information downloaded to the wireless device may preferably be in a variety of forms such as simple text, graphics and text, applets, forms, etc. Then, in step 64, the wireless device or wireless device user may act on the downloaded information as described herein.” Ex-1027 (Lazaridis), 5:66-6:20, Fig. 4.

50. This feature is also taught by Mgrdechian. Mgrdechian teaches “a communication method comprising receiving in a first wireless device one or more wireless device identifications associated with one or more other wireless devices, transmitting at least one of the one or more wireless device identifications from the first wireless device to a remote computer system, and receiving information associated with the one or more wireless device identifications from the remote computer system in the first wireless device.” Ex-1010 (Mgrdechian) ¶18. “In yet another embodiment, the present invention includes a computer system coupled to a network, the computer system including software for performing a method comprising storing a plurality of wireless device identifications, storing information for a plurality of users, associating the wireless device identifications with the information, receiving one or more wireless device identifications from a wireless device, accessing the information associated with the one or more wireless device

identifications, and transmitting the information associated with the one or more wireless device identifications to the wireless device.” Ex-1010 (Mgrdechian) ¶20. “In one embodiment, the wireless device identifications and information are stored in a database accessible over the Internet.” Ex-1010 (Mgrdechian) ¶21. Moreover, Mgrdechian teaches an example where “the device IDs may be received by the remote computer system and used by a web application 361 and a database 370 to access information associated with each device ID, such as Device B (i.e., User B). In one embodiment, when computer system 360 receives a device ID, web application 361 may generate a database query using the device IDs received from wireless device 310. Database 370 retrieves information associated with each device ID in the query, and then formats the information to send to the initiating device 310. In one embodiment, device IDs may be included as fields (e.g., indexes) in database tables that are associated with other information in the database, for example. The association may be implemented using a variety of techniques such as associated fields in a relational database or as links or references between objects, for example. The information in database 370 may have been set up previously by a user accessing a web address for computer system 360 (e.g., using the web application 361) or a related website or using a related web application such as an Internet browser. Database 370 may be a single database, distributed database or other data storage systems that can use device IDs to access information associated with device IDs.

The associated information may be updated automatically or manually by a user who accesses the information through computer system 360 (e.g., over the Internet or wirelessly). After the associated information has been retrieved, computer system 360 may then transmit the information back to the initiating device for use by the initiating user.” Ex-1010 (Mgrdechian) ¶75.

51. See also Ex-1039 (Sorte), 2 (“802.21 aims to standardize the format of ISEs and classifies them into three categories: 1. General Network Information (GNI): it gives a general overview of the network (e.g., network ID, location, network operator). 2. Link Layer Information (LLI): it includes the information related to link layer (e.g., channel, frequency, PHY types, data rates, security, QoS). 3. Higher Layer Information (HLI): it provides information relevant to higher layer services/applications that are supported by the access (e.g., IP configuration, Virtual Private Network, types of applications), pricing, service discovery protocols), roaming partners and so forth. This set of information may be retrieved by the MT by means of MIH message exchange from an information server in the network.”); Ex-1028 (Gulin) ¶¶70 (“By receiving the unique identifier associated with the newly contacted electronic equipment, the user of the mobile telephone may search an associated database, such as an electronic phonebook application, having stored unique identifying information associated with each user's ANON_ID to identify contact information associated with the ANON_ID and to the real person.”), 72 (“In

this embodiment, the central server may be used to create and store unique ANON_IDs, so that every user has his or her own unique ANON_ID across the network. This embodiment would thus facilitate making a given user's ANON_ID more widely known and to allow for association of specific information or individual status that may be of further interest to other users."); Ex-1029 (Kondou) ¶10 ("In addition, a server according to the present invention is placed on a network that a portable terminal can access via a wireless public network. The server stores and manages at least one of a device ID of an object of approach detection that the portable terminal can download, a profile of a user thereof, communication establishment information in short distance wireless communication, a communication history and a decode key for encrypted communication history.").

F. Filtering Beacon Transmissions by Comparing Stored Information to Transmitted Information to Determine Matches Was Known

52. Filtering beacon transmissions by comparing stored information at the mobile device to information transmitted in a beacon transmission to determine whether a match is present was known by 2008. For example, Godfrey teaches that "a filtering process may be performed to determine whether the user should be notified of a proximate station user. The filtering process may include, for example, comparing the user ID with a list of associate user IDS or applying one or more notification filter rules that govern the notification process." Ex-1031 (Godfrey) ¶35.

53. This is also taught by Krikorian. Krikorian teaches “determining, using an application running on the mobile first device, whether the identifier is included on a preexisting list stored on the mobile first device.” Ex-1009 (Krikorian) ¶4. “The method also includes receiving, by a mobile second device in proximity with the first device, the identifier, and determining, using an application running on the mobile second device, whether the identifier is included on a preexisting list stored on the mobile second device.” Ex-1009 (Krikorian) ¶5. Moreover, Krikorian teaches “[d]etermining whether a received identifier is included on the preexisting list (240) is performed by an application running on the mobile wireless device 120a. The application can further determine whether the associated contact, if any, is with a person, a location, a space, and/or an event. For example, if the identifier received is ID6, then the application can determine that ID6 is included on the list 300 and that ID6 is associated with Erika. If the received identifier does match an identifier on the preexisting list, the application can generate a notification message based on one or more associated fields of the identifier in the preexisting list. For example, the message can state that ‘Your friend Erika is nearby’ and include Erika’s picture. The mobile wireless device 120a can include default notification message generating instructions based on a type of the contact, a source of the contact, or other type of information characterizing the contact. In some embodiments, one or more specific contacts can include specific message notification settings in the other information

field 350. For example, the Verizon Store can include instructions to direct the phone to play a distinctive tune to indicate to the user that a store is nearby. The application can further determine if the matched contact includes any instructions that should be locally executed. For example, if the received identifier was ID1, then the other information field 350 for Brian can include instructions to connect to a Match.com server to download existing or updated profile information for Brian. In another example, if the received identifier was ID9, then the ‘Ring Silencer’ contact can include instructions in the other information field 350 to direct the application to turn off the ringer of the mobile wireless device 120a until the device leaves the proximity-based wireless network 110b or another condition(s) is met (e.g., after an elapsed amount of time).” Ex-1009 (Krikorian) ¶26.

54. See also Ex-1032 (Jansen 2005), 8 (“The beacon enrollment phase – During this phase, the (client) PDA tries to authenticate the beacon for the first time. It consists of the following steps: • The PDA tries to identify and connect to a personal beacon. Note that in the case of the Bluetooth variant, the beacon’s identity is already known and could be used to connect to the beacon directly. However, the PDA inquires for all Bluetooth devices available and tries to connect only to devices of class ‘Access Point.’ If no such device exists, this phase fails. The enrollment phase also fails if such devices exist, but no connection can be successfully made to any of them. • The PDA starts the high-level protocol with the connected device,

whereby it requests and receives the user certificate. If the certificate transfer fails, or the certificate does not verify, the PDA closes the connection and restarts the previous step with another device as the prospective token. • The PDA tries to authenticate the prospective token through a challenge-response protocol, based on the certificate information. If the authentication exchange fails, the PDA retries the above steps with another device. If the authentication succeeds, the PDA concludes that the prospective token is the intended personal beacon, saves the certificate (i.e., as a flag attesting that enrollment completed successfully) and the communications address of the token (e.g., a MAC Address for Bluetooth) for subsequent use in the authentication phase, and closes the connection.”); Ex-1031 (Godfrey) ¶11 (“In accordance with a further aspect of this invention a method is provided for establishing a direct wireless link between a first wireless device and at least one proximate wireless device. The method includes identifying a second wireless device within a predetermined proximity of the first wireless device; determining an identity associated with a user of the second wireless device; comparing the identity associated with the user of the second wireless device with a set of one or more predetermined identities, and notifying a user of the first wireless device that the user of a proximity of the user of the Second wireless device based on the comparison of the identity with the set of one or more predetermined identities.”).

G. Taking Action if a Match is Determined Between the Stored Information and the Transmitted Information Was Known

55. Taking some sort of action if a match is determined to be present between stored information at the mobile device and information transmitted in a beacon transmission was known by 2008. For example, Krikorian teaches “notifying a user of the mobile first device, if the identifier is included on the preexisting list, that the user associated with the identifier is in proximity to the mobile first device.” Ex-1009 (Krikorian) Abstract, ¶4. “The method also includes notifying a user of the mobile second device, if the identifier is included on the preexisting list, that the user associated with the identifier is in proximity to the mobile second device.” Ex-1009 (Krikorian) ¶5. Krikorian further teaches “[n]otifying a user of the mobile wireless device 120a of proximate detection of a contact (250) can include using a graphical user interface to deliver a visual notification message, using a speaker to deliver an audio notification message, vibrating the mobile wireless device 120a, and/or any other notification method.” Ex-1009 (Krikorian) ¶27. “Transmitting metadata and/or other information between the mobile wireless devices 120a and 120b (260) can be initiated by the application based on a proximity detection that matched a contact on the list, by an instruction from the user of the wireless device 120a, and/or can be in response to a query or request by another mobile wireless device 120. For example, the user of the wireless device 120a can include instructions in the other information

field 350, associated with John, to transmit metadata to John's mobile wireless device 120b indicating that the user is nearby. In another example, after receiving a notification message indicating that Brian is nearby, the user of the mobile wireless device 120a can manually instruct a message to be sent to Brian including a picture and a short message. Metadata can be encoded in a human readable name of a mobile wireless device 120. Other information can include, for example, advertisements for a store, text or IM messages, or other real-time communications. In one embodiment, the user of mobile wireless device 120a can elect to receive advertisements/special offers when he or she comes within proximity of a Verizon Store. In this case, the mobile wireless device 120a can transmit a message to the location-based wireless device 130, based on an instruction in the other information field 350, and the location-based wireless device 130 at the Verizon Store can send advertisement messages in response. Elective advertisements advantageously allow passive, unobtrusive advertisements to consumers.” Ex-1009 (Krikorian) ¶28.

56. This is also taught by Lazaridis. Lazaridis teaches that “[i]n other exemplary embodiments of the bookmark beacon system 10, the bookmark beacon 12 may be associated with, for example, a cash register in a restaurant, a facsimile machine, a printer, a secure door, or even a tree.” Ex-1027 (Lazaridis), 4:21-24. For example, Lazaridis teaches a cash register example: “At a restaurant, a mobile device user orders a meal (order A) and sits at table B. A waiter enters order A into a cash

register with a web browser interface. The order and amounts owing are managed and maintained securely stored on a web page that is reserved for orders relating to table B. The wireless device user then completes his or her meal and initiates communication with a bookmark beacon, attached to table B, that provides the mobile device with a bookmark data packet identifying the web page associated with table B. The mobile device then accesses the web page as described above. Upon receiving the preferably secure web page, the user may, for example, be able to review his or her order, confirm the order and complete payment for such transaction. The bookmark data packet utilized in this exemplary embodiment may comprise the following information.” Ex-1027 (Lazaridis), 4:31-53; *see also id.* 4:54-5:7 (Facsimile example), 5:8-28 (Printer example), 5:29-51 (Secure door example), 5:52-65 (Tree example).

57. *See also* Ex-1039 (Sorte), 4 (“Our objective is to set up a network configuration able to publish and provide a multi-service 802.11b access environment. ... We offer a number of different services: Internet access; video service; TDS service; printing service.”), 7-8 (“The process evolves as illustrated in Fig. 6. The user begins to attach to an AP. If the process is successful (i.e., the user is authenticated and receives the IP address, if needed), the user can immediately verify whether the service (e.g., Internet access) is available. If more refined service information is needed to enjoy the service (e.g., the TDS service), the user may issue

a query using a service discovery protocol, for instance SLP. Finally, if the user is unable to receive the service, he disconnects from the current access and attempts to attach to another access. The process ends when either the user finds the desired service or the accesses to monitor are exhausted and the service is unavailable.”), 8 (“One means of identifying the APs providing the service is beacon-based service publishing. In this case, the user can enjoy the service immediately after completing the process of connection to the network for certain services (e.g., Internet access).”); Ex-1040 (Blake), 7:43-49 (“The beacons 102-108 are controlled by a beacon infrastructure server (BIS) 110, with one or more terminals 112, 114, 116, 118 being connected to the server 110. The terminals 112-118 enable service providers, i.e., the users of beacons 102-108, to author or edit allocated service slots in the form of added data piggy backed on inquiry facilitation signals transmitted by beacons 102-108.”); Ex-1010 (Mgrdechian) ¶¶34 (“Once the information regarding the identity of User A, the unique ID of Device B and the selection of which message to send (including either their user-profile or a customized message) has been received by the server, message delivery may be contingent on a number of pre-set conditions including whether User B has an interest in receiving messages from someone with the profile of User A, the form of the message, the number of messages User B is willing to receive in a given day and other preferences designed to filter unwanted, repetitive, overwhelming or otherwise undesirable messages (i.e. spam) to avoid

annoying, harassing or overloading the Recipient.”), 35 (“In the event that the server determines that the message or sender does not meet the preset conditions to be sent to the Recipient, the message will be discarded.”), 36 (“In the event that the server determines that the message or Sender does meet the preset conditions to be sent to the Recipient, the Recipient will receive or be notified of the message which may then be delivered to, or retrieved by the Recipient in any of a number of ways including logging on to the server, or through any other means as technically feasible including via cell phones, PDA’s or email. The recipient can choose to be notified immediately upon receipt of such a message, on a periodic basis or through a manual inquiry at the time of their choosing.”), 41 (“In another embodiment of the present invention, Device A automatically queries other devices for their IDs, receives one or many responses to its request and communicates this information to the server, which then compares the profiles associated with the IDs to the pre-defined preferences of User A. If any of the profiles match these preferences, an alert is sent to User A to indicate the presence of a person-of-interest. In a variation of this embodiment, User A can be a business or other organization (such as an advertiser) which may take some additional action based on the presence of a person with a specific profile. For example, a business or advertiser may retrieve profiles and forward information or advertisements to such user's accounts. Users of the service may opt to receive and optionally filter such information or advertisements based on

predefined criteria (i.e., restaurant ads only).”).

H. Using Protocols Such as Bluetooth and Cellular for Communications Between Mobile Devices and Servers Was Known

58. Using protocols such as Bluetooth and cellular for communications between mobile devices and servers was known by 2008. For example, Mgrdechian teaches embodiments “where: 1) Device A communicates with the server via a cable, cradle or other physical connection to a PC or other electronic apparatus which can relay ID or other information to the server; or 2) through any form of wireless connection such as Bluetooth Wi-Fi or 802.11 which could relay the ID and messaging information either directly or through some intermediary (such as a cellular network or PC) to the server. An additional alternate embodiment includes the case where Device A displays the IDs to User A at some later time when User A can log-on or access the server and manually enter the information.” Ex-1010 (Mgrdechian) ¶33. Moreover, Mgrdechian teaches embodiments which “allow users of wireless devices to interact using a local wireless protocol when the wireless devices are within range of each other. Such devices may be coupled together over an ad hoc or peer-to-peer wireless network, for example. ... For example, wireless technologies that may be used as a local wireless protocol include Bluetooth, an 802.11 protocol, Zigbee or equivalent wireless technology for establishing a peer-to-peer or ad hoc network or detecting the presence of other wireless devices and

exchanging device IDs. ... However, protocols such as Bluetooth, 802.11 or Zigbee are particularly well-suited for applications where the other wireless devices are operating in close physical proximity of each other. Moreover, those skilled in the art will understand that the range R of any device is not exact, but rather, signal strengths decrease as the distance between wireless devices increases making connectivity more difficult.” Ex-1010 (Mgrdechian) ¶72.

59. This is also taught by Lazaridis. Lazaridis teaches that “[c]ommunication between a wireless device and traditionally non-wireless equipment, such as printers, facsimile machines, ATMs, etc., currently requires the equipment to be specially manufactured with wireless capabilities, such as a Bluetooth® interface. Bluetooth® is a de facto standard, as well as a specification for small-form factor, low-cost, short-range radio links between wireless devices.” Ex-1027 (Lazaridis), 1:26-32. Moreover, Lazaridis teaches that “[u]pon receiving the bookmark data packet 24, the mobile device user is preferably given the option to then access the server 26 and website 28 or the guest device 22 identified by the resource address. Communication with the Internet is preferably achieved through an existing wireless network 16 and proxy server 20. Communication across the wireless network connection 16 may be facilitated on the wireless device 14 using any known software that is capable of interfacing the wireless device 14 with the proxy server 20. The proxy server 20 is then used as a gateway that allows the

wireless device 22 to indirectly communicate with the website 28 or guest device 22 over the network connection. The proxy server 20 preferably communicates with the target website 28 through a Hypertext Transfer Protocol (HTTP) fetch and cache component.” Ex-1027 (Lazaridis), 2:55-3:5.

60. *See also* Ex-1028 (Gulin) ¶¶2 (“Electronic equipment, such as, for example, mobile communication devices, mobile telephones, personal digital assistants, etc. are typically equipped to communicate with mobile or cellular telephone communication networks. Such electronic equipment is increasingly being equipped with adapters to support advanced communications in a variety of media other than or in addition to such mobile telephone networks. Such advanced communication media may include, for example, Ethernet, Bluetooth, 802.11, wireless local area networks (WLANs), WiFi, WiMax and the like, in addition to a mobile telephone network. These advanced media are referred to herein as ‘near field’ (or ‘near-field’) communications media. It is noted that in a cellular telephone network, the near-field communication may include communication with another mobile telephone user, in which case the near-field connection is between the mobile telephone and the cell tower through which it connects to the mobile telephone network.”), 72 (“In one embodiment, there is a central server or network through which connections and communications are made. In this embodiment, the user would make a connection, for example, through a mobile telephone network, or in

another embodiment, through a Wi-Fi network in an institution such as a university.”), 84 (“the local interface adapter 50 may be wired and/or wireless and may support communications utilizing any communication protocol (e.g., Ethernet, Bluetooth, 802.11, WLAN, WiFi, WiMax, Infrared, etc.), 86 (“The following discussion will focus on communications between the first mobile telephone 10 and the second mobile telephone 10’ using Bluetooth compatible protocols. However, one of ordinary skill in the art will readily appreciate that other communication protocols and/or specifications may also be implemented in accordance with the present invention (e.g., 802.11 compliant standards (e.g. 802.11(a), 802.11(b), 802.11(g), etc.), WiFi, WiMax, infrared, Ultra Wideband, near-field communications, radio frequency identification, Ethernet, etc.).”); Ex-1040 (Blake), 5:20-24 (“the telephone network 48 also provides the link from the telephone 10 to a wide-area network (WAN) server 52 and, via the WAN 54 (which may be the internet), to one or more remote service providers 56 providing a source of data for the telephone 10”), 7:53-59 (“Having filled out the template with, for example, a description of the service and other information for the data to be carried via the beacon broadcast, the template is returned to server 110, preferably via a secure link using, e.g., Secure HTTP(S-HTTP) or Secure Sockets Layer (SSL). SSL creates a secure link between a client and a server, over which any amount of data can be sent securely.”); Ex-1033 (Langensteiner) ¶13 (“The service interaction between the

portable device and Second beacon may be carried out via a different communications mechanism (for example RF or IR), and/or according to a different communications protocol (e.g. Bluetooth, 802.11, HomeRF, Zigbee), to the exchange of inquiry message and identifier between the portable device and first beacon.”); Ex-1009 (Krikorian) ¶¶3 (“Advertisers typically use Bluetooth to broadcast advertisements to all Bluetooth receivers within the range of a transmission device. Social networks typically use Bluetooth to detect wireless devices and then query a centralized server that determine if a connection exists between the devices' owners' and links the two devices for communication.”), 8 (“Receiving the identifier can include using Bluetooth and/or wireless USB. ... The first and second devices can communicate with each other using Bluetooth and/or wireless USB”), 19 (“Information transmission and reception over a proximity-based wireless network 110 can be based on one or more wireless communication protocols. Wireless communication protocols can include, for example, Bluetooth, wireless USB, and/or other local area wireless communication protocols. Bluetooth and wireless USB advantageously allow use of proximity-based networks 110 in any location, including indoors, in underground subways/tunnels, remote locations, and other locations where GPS and cellular network signals fail to reach. Class 1, 2, and 3 Bluetooth devices can respectively transmit information to devices within, and up to, about 100 meters, about 10 meters, and about 1 meter. Wireless USB devices can

transmit information to devices within and up to about 10 meters.”).

I. Using A Processor and Memory with Instructions to Execute Functions on Mobile Devices Was Known

61. Using a processor and memory with instructions to execute functions on the mobile device was known by 2008. For example, Krikorian teaches “a computer program product” that “is tangibly embodied in an information carrier and includes instructions being operable to cause a data processing apparatus to receive, by a mobile first device in proximity with a second device, an identifier wirelessly transmitted by the second device. The identifier is associated with a user of the second device. The instructions are also operable to cause the data processing apparatus to determine, using an application running on the mobile first device, whether the identifier is included on a preexisting list stored on the mobile first device. The instructions are also operable to cause the data processing apparatus to notify a user of the mobile first device, if the identifier is included on the preexisting list, that the user associated with the identifier is in proximity to the mobile first device.” Ex-1009 (Krikorian) ¶6. Moreover, Krikorian teaches that its described techniques “can be implemented in digital electronic circuitry, or in computer hardware, firmware, software, or in combinations of them. The implementation can be as a computer program product, i.e., a computer program tangibly embodied in an information carrier, e.g., in a machine-readable storage device or in a propagated

signal, for execution by, or to control the operation of, data processing apparatus, e.g., a programmable processor, a computer, or multiple computers. A computer program can be written in any form of programming language, including compiled or interpreted languages, and the computer program can be deployed in any form, including as a stand-alone program or as a subroutine, element, or other unit suitable for use in a computing environment. A computer program can be deployed to be executed on one computer or on multiple computers at one site.” Ex-1009 (Krikorian) ¶¶30-31 (“Method steps can be performed by one or more programmable processors executing a computer program to perform functions of the invention by operating on input data and generating output.”). Additionally, Krikorian teaches that “[p]rocessors suitable for the execution of a computer program include, by way of example, both general and special purpose microprocessors, and any one or more processors of any kind of digital computer. Generally, a processor receives instructions and data from a read-only memory or a random access memory or both. The essential elements of a computer are a processor for executing instructions and one or more memory devices for storing instructions and/or data. Generally, a computer also includes, or is operatively coupled to receive data from or transfer data to, or both, one or more mass storage devices for storing data, e.g., magnetic, magneto-optical disks, or optical disks. Data transmission and instructions can also occur over a communications network. Information carriers suitable for embodying

computer program instructions and data include all forms of non-volatile memory, including by way of example semiconductor memory devices, e.g., EPROM, EEPROM, and flash memory devices; magnetic disks, e.g., internal hard disks or removable disks; magneto-optical disks; and CD, DVD, HDDVD, and Blu-ray disks. The processor and the memory can be supplemented by, or incorporated in special purpose logic circuitry.” Ex-1009 (Krikorian) ¶32.

62. This is also taught by Gulin. Gulin shows in Figure 2 below, a mobile telephone having a processing device component and a memory component. Ex-1028 (Gulin), Fig. 2.

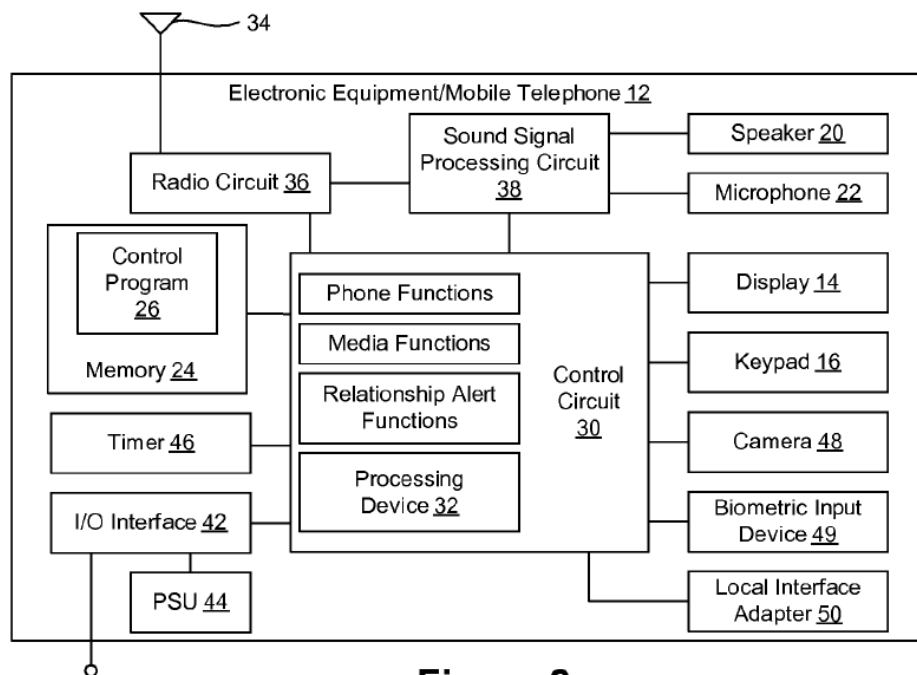


Figure 2

Moreover, Gulin teaches “a process for establishing communication between first and second electronic communication devices and determining whether a

relationship exists between users of the first and second devices, the first and second devices each including compatible near-field communications capability, a memory, a processor, a user interface and being programmed to maintain information relating first and second anonymous user information with secure detailed user information for a plurality of known individual persons.” Ex-1028 (Gulin) ¶29. Furthermore, “[r]eferring to FIG. 2, a functional block diagram of the mobile telephone 10 is illustrated. The mobile telephone 10 includes a primary control circuit 30 that is configured to carry out overall control of the functions and operations of the mobile telephone 10. The control circuit 30 may include a processing device 32, such as a CPU, microcontroller or microprocessor. The processing device 32 executes code stored in memory (not shown) within the control circuit 30 and/or in a separate memory, such as memory 24, in order to carry out operation of the mobile telephone 10 and perform all of the functionality disclosed herein. As illustrated in FIG. 2, the control circuit may include functionality to control the main device functions, such as those of the mobile telephone 10, to control additional device functions such as media functions, and the relationship alerter functions in accordance with embodiments of the present invention. It will be apparent to a person having ordinary skill in the art of computer programming, and specifically in application programming for mobile telephones or other electronic devices, how to program an electronic device such as the mobile telephone 10 to operate and carry out logical

functions associated with the programming described herein.” Ex-1028 (Gulin) ¶79.
“The memory 24 may be any suitable memory device. For example, the memory 24 may be, for example, random access memory, read only memory, a buffer, a flash memory, a hard drive, a removable media, a volatile memory and/or a non-volatile memory or a combination of any of the foregoing. In order to carry out the various functions described herein, the memory 24 may include one or more computer applications (or sub-applications), including a control program 26 programmed to achieve the functionality described herein.” Ex-1028 (Gulin) ¶80.

63. See also Ex-1029 (Kondou) ¶¶23 (“In addition, the control portions 13 exchange device IDs with each other when a history of communication with the other party exists in the communication history memory portions 141 of both sides, and store an approach log including a device ID of the other party with which device IDs were exchanged and a time when the exchange was performed in an approach history memory portion 142 of the memory portion 14.”), 29 (“Bluetooth is used for storing a device ID, a user profile, connection management information (such as a link key) or others in the memory portion 14 (the approach history memory portion 142) between the two portable terminals 1.”).

VIII. THE ’918 PATENT AND ITS FILE HISTORY

64. The ’918 Patent relates to techniques for mobile wireless devices (e.g., cellular phones) in proximity with one another to exchange information “utilizing

both a short range and long range wireless capability.” Ex-1001, 2:66-3:3. The ’918 Patent concedes that 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 combining these two wireless capabilities, allowing 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.

65. As shown in Figure 1 below,³ “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.

³ Throughout, emphasis and annotations are added unless otherwise specified.

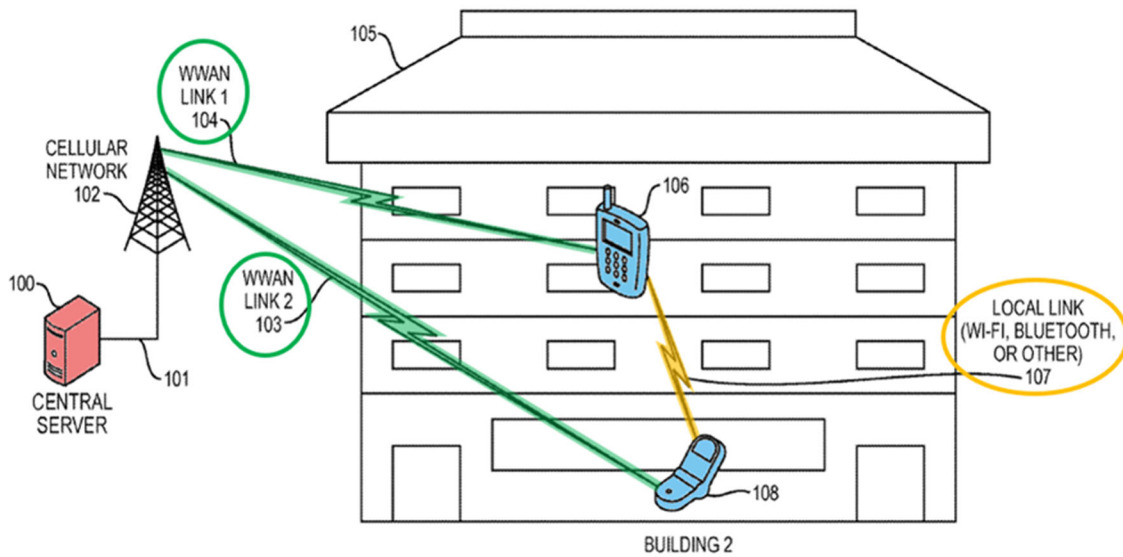


Figure 1

66. One example of the short-range wireless capability, shown in Figure 6 below, is an “independent basic service set or IBSS,” involving an “ad-hoc network” of wireless devices that “transmit identifiers called *beacons*.” See ’918 Patent, 10:31-44. The ’918 Patent further explains, as shown in Figure 6 below, the 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).

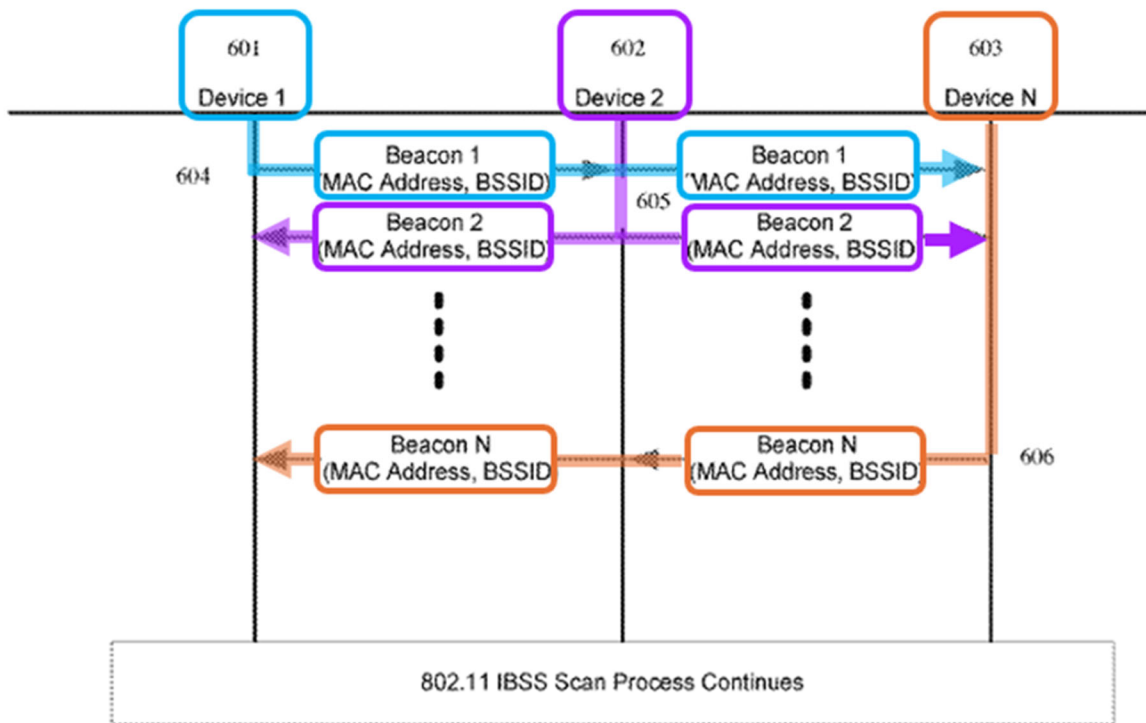


Figure 6 - 802.11 IBSS Beacon Process

67. 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. The '918 Patent also claims priority to provisional application Nos. 61/095,359 and 61/095,001, filed on September 8, 2008 and September 9, 2008, respectively.

68. The '918 Patent issued following a lengthy prosecution that included a series of Examiner rejections and Applicant claim amendments. The Examiner's Notice of Allowance indicated that "the closest prior art of record, Sundar (US 2003/0134650)" disclosed most features of the independent claim, but failed to disclose: (1) "each of the proximity beacon transmissions including a MAC address

and unique identifier”; (2) “determining if a particular short range transmission of the plurality of short range transmissions includes a MAC address”; and (3) “utilizing the unique identifier.” *See* Ex-1004 at 2237-2238 (December 2, 2021 Notice of Allowance at 2-3).

69. Also during prosecution, in response to written description rejections, inventor James Proctor, Jr. submitted a declaration (Ex-1011), asserting, among other things, that: (a) Figure 1 demonstrates that wireless devices 106 and 108 each include two radios (one for each communication link); and (b) the claimed requirement of “beacon transmissions” comprising a “PBSI,” “MAC address,” and “unique identifier” is supported by the specification’s discussion of the “IBSS beacon process” in connection with Figure 6 (*i.e.*, ’918 Patent at 10:31-11:6)—where, in one embodiment, “‘PBSI’ is the BSSID field of the beacon,” and in another embodiment, “‘PBSI’ is the SSID.” *See* Ex-1004 at 1546-1548, 1555-1556 (Proctor Decl., ¶¶73-84, 120-124); Ex-1011.

70. This Petition presents arguments not considered during prosecution. *See* Ex-1004. The prior art combinations in this Petition were not before the PTO during prosecution. Ex-1004.

IX. CLAIM CONSTRUCTION

71. For purposes of my Declaration, I do not believe that any term requires

explicit construction to resolve the issues I present in my Declaration.

X. OVERVIEW OF THE APPLIED PRIOR ART REFERENCES

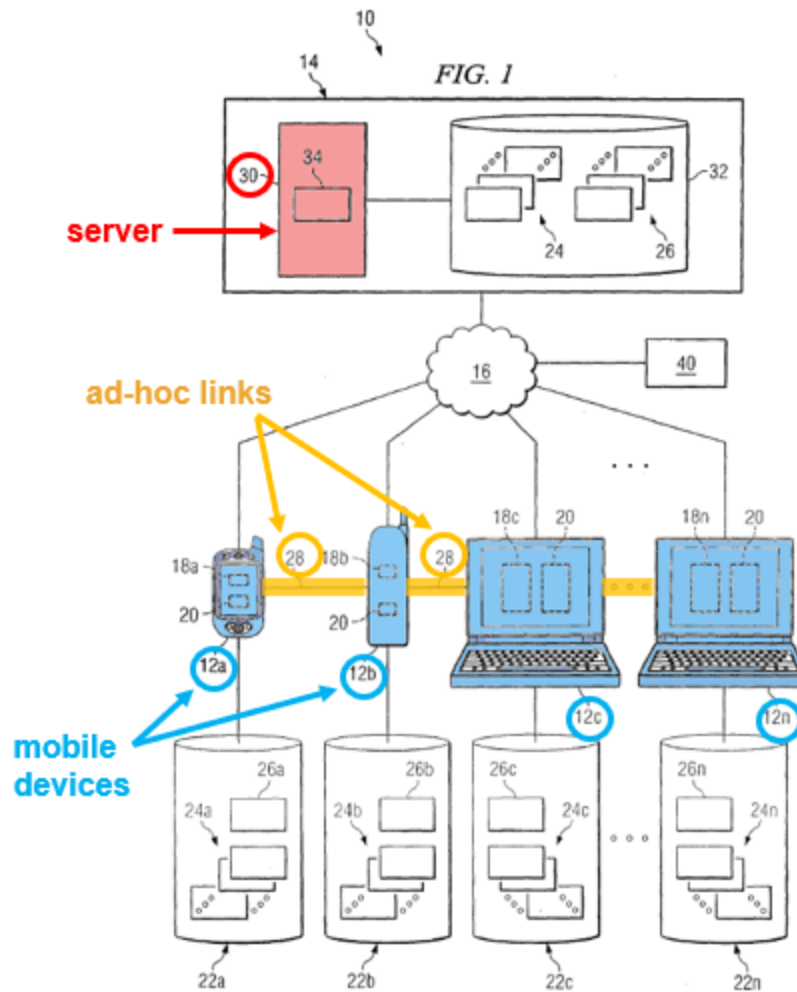
A. Ribaudó (Ex-1007)

72. Ribaudó (U.S. Patent Publication No. 2007/0030824), titled “System and Method for Providing Communication Services to Mobile Device Users Incorporating Proximity Determination,” was published on February 8, 2007. I understand from Counsel that Ribaudó is §102(b) prior art to the ’918 Patent.

73. Ribaudó teaches “a system and method for providing communication services to mobile device users incorporating proximity determination” in order 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.

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

34, 66, Fig. 1.



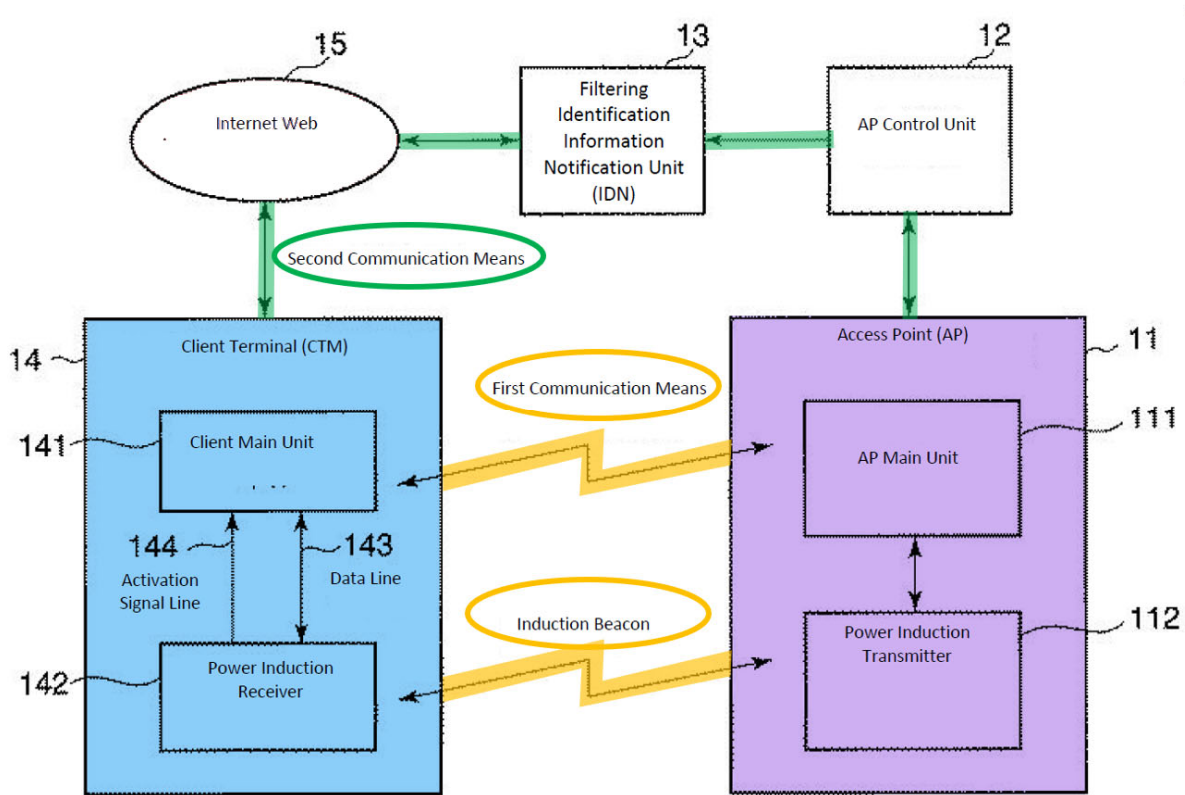
75. As Ribaudo explains, “a user (e.g., of mobile device 12a) may be associated with one or more client IDs, which may identify the user publicly,” which “may be the unique MAC address[es] of the Wi-Fi NIC of the user’s mobile device[s] 12.” Ex-1007 ¶68. In operation, the mobile device “may beacon data 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.

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

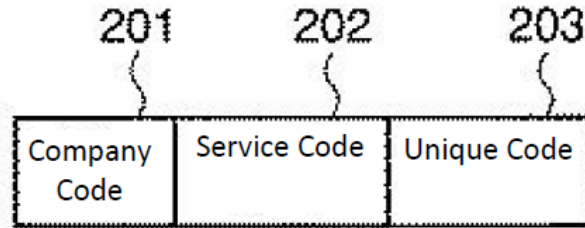
76. Watanabe (JP Patent Publication No. 2005/12973), titled “Wireless Communication System” was published on January 13, 2005. I understand from Counsel that Watanabe is §102(b) prior art to the ’918 Patent. Citations to Watanabe in my Declaration are to the certified English translation of Ex-1005, which I understand is attached to the Petition as Ex-1006.

77. Watanabe teaches a wireless communication system that “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.



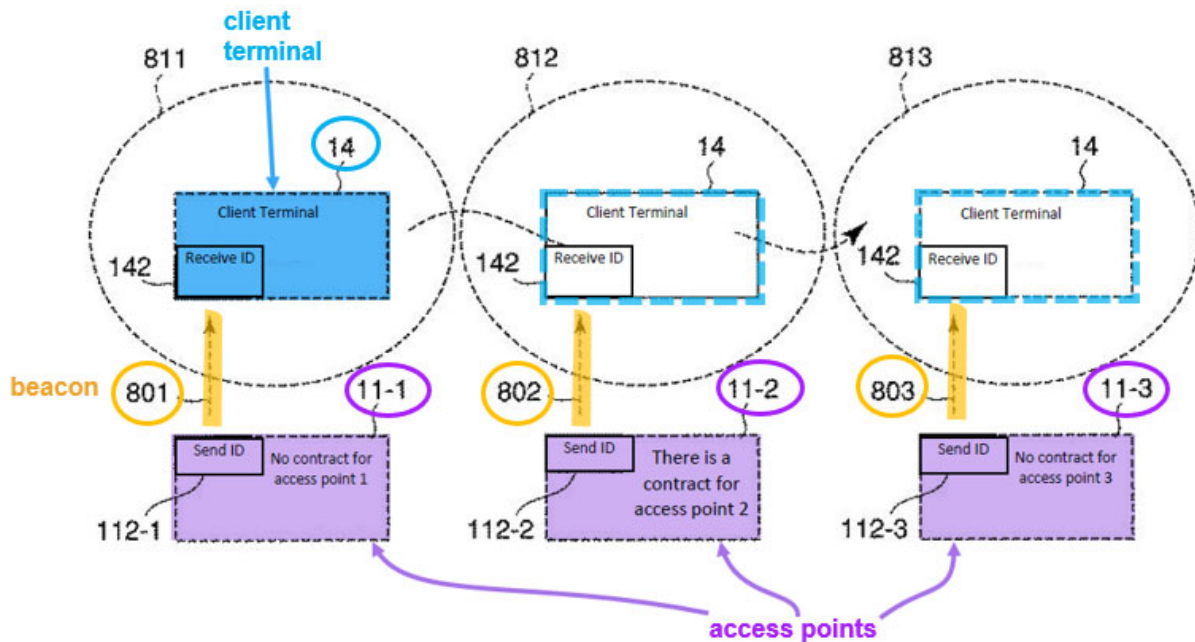
78. As Watanabe explains, “each access point 11... generates an induction *beacon* (power supply signal) that uses the first communication means to supply power” and report “transmitter identification information.” Ex-1006 ¶¶14, 49. Transmitter identification information includes: a “company code 201 indicating the service provider,” a “service code 202 indicating the type of service that can be provided via that access point,” and “a unique code 203 unique to that power induction transmitter.” *Id.*, ¶15, Fig. 2.

[FIG. 2]



79. “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.

80. Watanabe’s wireless system is illustrated in Figure 8 (below), where a trio of “of 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.



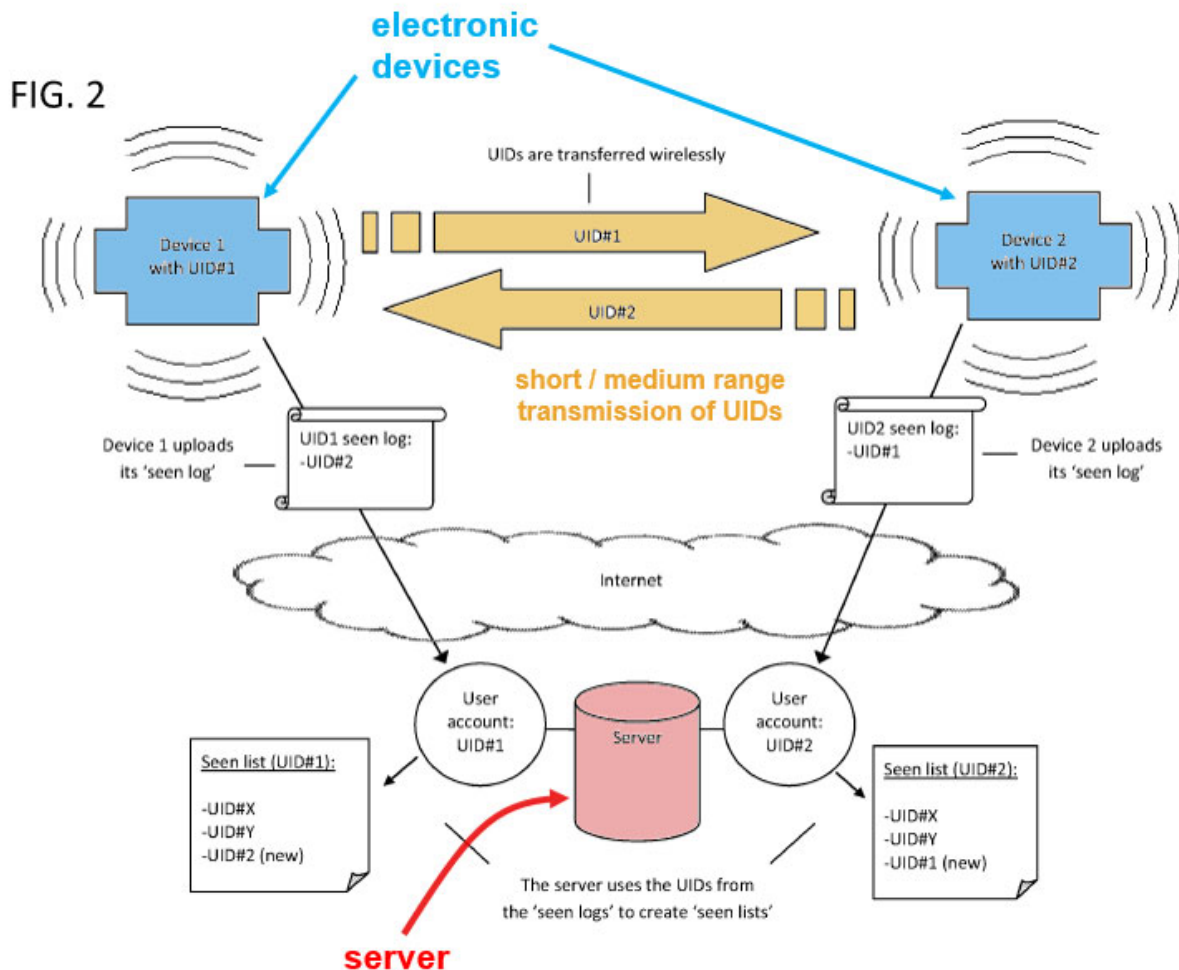
C. Behrens (Ex-1008)

81. Behrens (PCT Patent Publication No. WO2008/132241), titled “Device and Method for Establishing Social Networks Through the Use of Wireless Technology,” was filed as a PCT application on April 30, 2008 designating the United States, and published in English on November 6, 2008. I understand from Counsel that Behrens is §102(e) prior art to the ’918 Patent.

82. Behrens teaches portable electronic devices (e.g., mobile phones) that “continuously/repeatedly transmit” and scan for “unique identifiers (UID) via non-directed wireless radio frequency transmission” in order 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. Specifically, the UID “may consist of or include

a MAC (media access control) address, Bluetooth Device Address (i.e., BD_ADDR), or other unique or quasi-unique identifier.” Ex-1008, 11:21-26. Behrens also teaches that 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.

83. Figure 2 below, a schematic diagram of Behrens’ method, 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.



D. Mgrdechian (Ex-1010)

84. Mgrdechian (U.S. Patent Publication No. 2005/0174975), titled “System and Method for Wireless Communication Between Previously Known and Unknown Users,” was published on August 11, 2005. I understand from Counsel that Mgrdechian is §102(b) prior art to the ’918 Patent.

85. 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 wireless device exchanges information with a remote server a via Internet, Ex-1010, ¶92, and where the wireless devices communicate with each other via Bluetooth or Wi-Fi link, based on “unique identifications” or “unique IDs” that are stored in a remote database. Ex-1010, ¶¶21, 91, 92; *see also id.*, Fig. 8 (annotated).

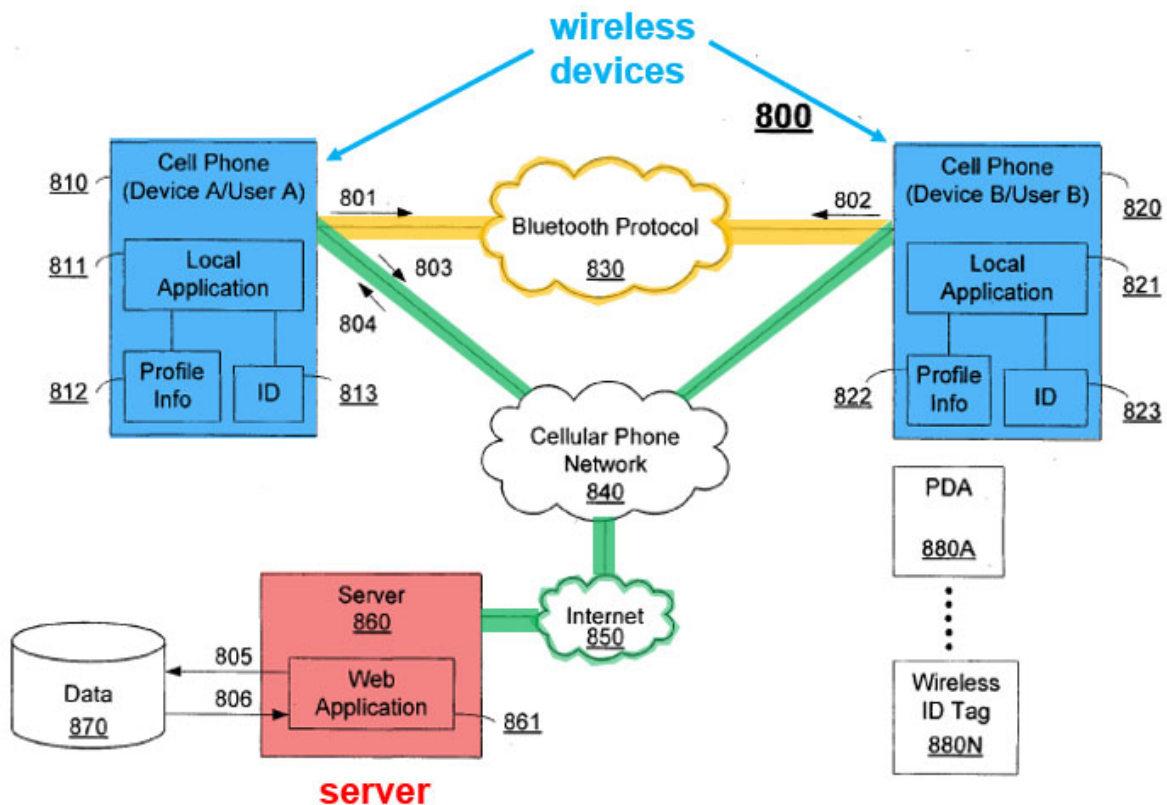


Fig. 8

86. As one example, Mgrdechian explains that its invention can be applied to “gaming applications operating on mobile devices.” Ex-1010, ¶86.

XI. 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.

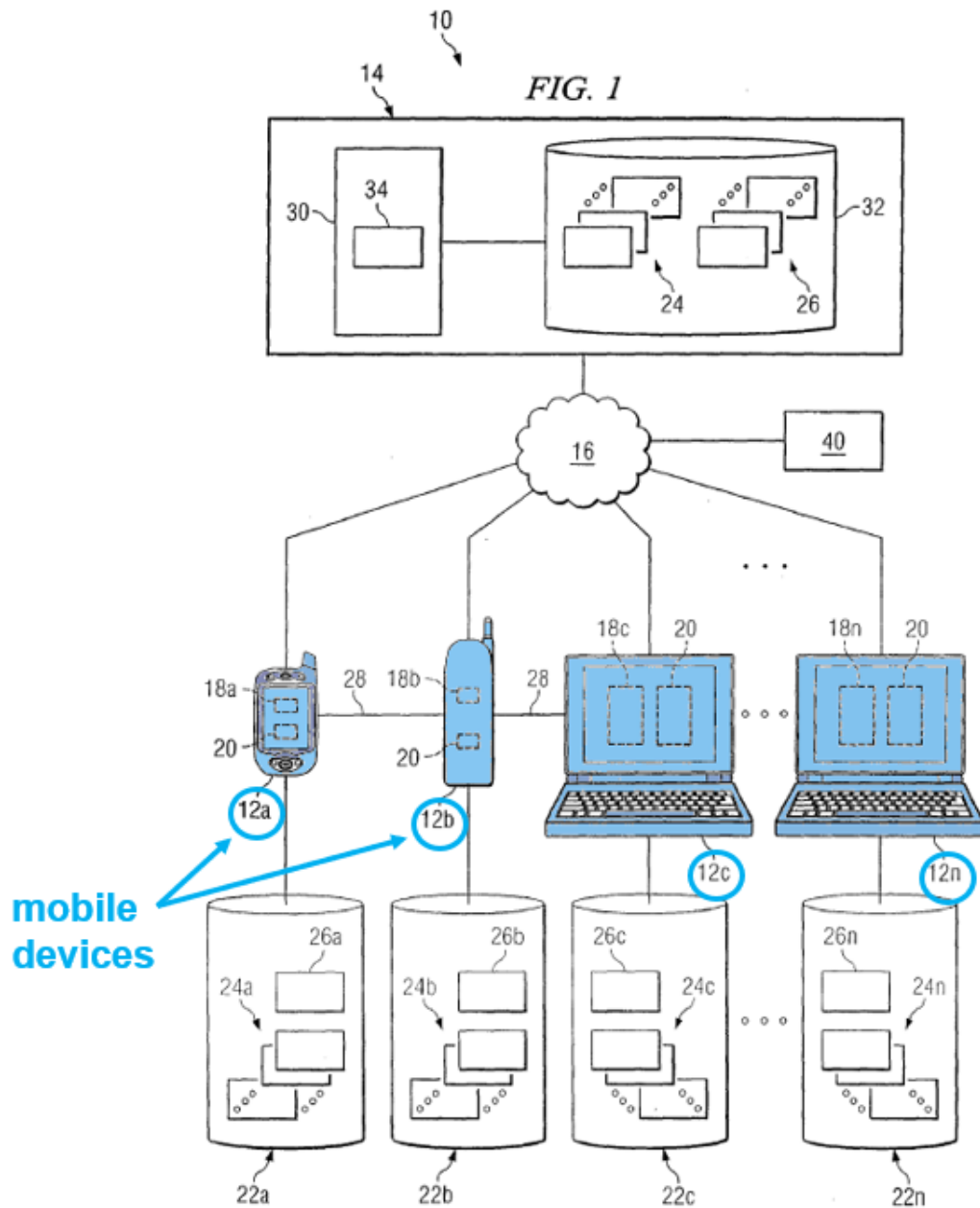
1. Independent Claim 1

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

87. In my opinion, Ribaudó teaches⁴ the preamble, to the extent it is limiting.

88. Ribaudó's wireless system, shown in Figure 1 below, 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. To focus my analysis, mobile device "12a" is the recited mobile wireless device.

⁴ I understand from Counsel that the term "teaches" includes both express teachings and those fairly suggested to a person of ordinary skill in the art.



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

89. In my opinion, Ribaud teaches Element 1[a].

90. Ribaud explains that “[m]obile devices 12 may each include any

suitable combination of hardware, software, and firmware to provide the functionality described herein,” and that “[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. Ribaudo further teaches that “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.**” Ex-1007, ¶¶24-25. Ribaudo’s system may also “employ a **cellular** connection ... to download from data center 14.” Ex-1007, ¶204. If mobile 12a is the recited wireless mobile device, then adapter 18a’s cellular/WWAN radio is the recited first radio. I note that my analysis is consistent with the inventor’s statements during prosecution. *See* Ex-1011 (Proctor Decl.), ¶¶73-89 (explaining how the ’918 specification discloses “first” and “second radio[s]”).⁵

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

91. In my opinion, Ribaudo teaches Element 1[b].

⁵ Moreover, as I discussed in the Technological Background section, by 2008, it was known that cellular protocols can facilitate communication between a mobile device and a server. *See* Section VII.H (citing Ex-1010 (Mgrdechian) ¶¶33, ¶72; Ex-1027 (Lazaridis), 1:26-32, 2:55-3:5; Ex-1028 (Gulin) ¶¶2, 72, 86; Ex-1040 (Blake), 5:20-24, 7:53-59; Ex-1033 (Langensteiner) ¶13; Ex-1009 (Krikorian) ¶¶3, 8, 19.).

92. Similar to element 1[a], Ribaudo further explains that “[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.

93. If mobile 12a is the recited wireless mobile device, then adapter 18a’s Wi-Fi (or Bluetooth) radio is the recited second radio. I again note that my analysis is consistent with the inventor’s statements during prosecution. *See* Ex-1011 (Proctor Decl.), ¶¶73-89 (explaining how the ’918 specification discloses “first” and “second radio[s]”).⁶

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

94. In my opinion, Ribaudo teaches Element 1[c].

95. For example, Ribaudo discloses that mobile devices 12 “each include any suitable *combination of hardware, software, and firmware* to provide the

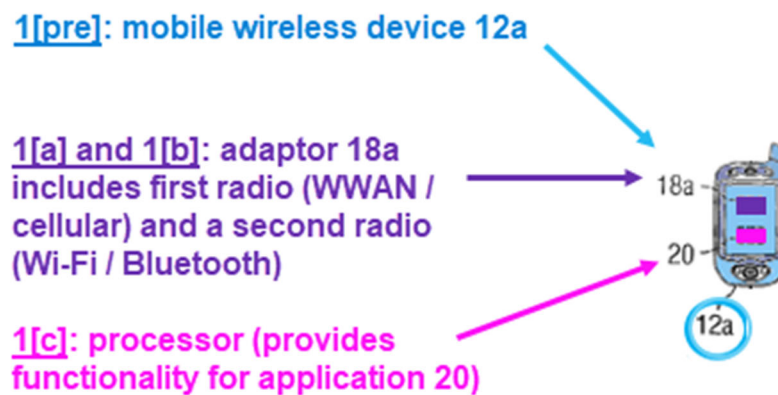
⁶ Moreover, as I discussed in the Technological Background section, by 2008, it was known that Bluetooth can be used to facilitate communication between mobile devices. *See* Section VII.H (citing Ex-1010 (Mgrdechian) ¶¶33, ¶72; Ex-1027 (Lazaridis), 1:26-32, 2:55-3:5; Ex-1028 (Gulin) ¶¶2, 72, 86; Ex-1040 (Blake), 5:20-24, 7:53-59; Ex-1033 (Langensteiner) ¶13; Ex-1009 (Krikorian) ¶¶3, 8, 19.).

functionality described” including “one or more applications 20” to “facilitate communication with other mobile devices 12 (e.g., mobile devices 12b through 12n) and between mobile device 12 and data center 14.” Ex-1007, ¶19. Ribaudó further discloses, in connection with Figure 2, that “the 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.” Ex-1007, ¶84.

96. 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 installed on the device. Virtually all embedded communication devices, both at the time of '918 Patent and today, use a combination of hardware, software, and firmware. The firmware is the component of the software that directly interfaces with the hardware. For example, Yeong, J. H., et al., *802.11 a MAC layer: firmware/hardware co-design*, FOURTH INTERNATIONAL CONFERENCE ON INFORMATION, COMMUNICATIONS AND SIGNAL PROCESSING, 2003 (Ex-1041, “Yeong”), describes a typical design. Here, the modem PHY functions are implemented in an ASIC (hardware). The host software interfaces to the

hardware via firmware running on an embedded ARM processor.⁷

97. I have annotated below, the mobile device 12a of Figure 1 to indicate limitations 1[pre]-1[c]:



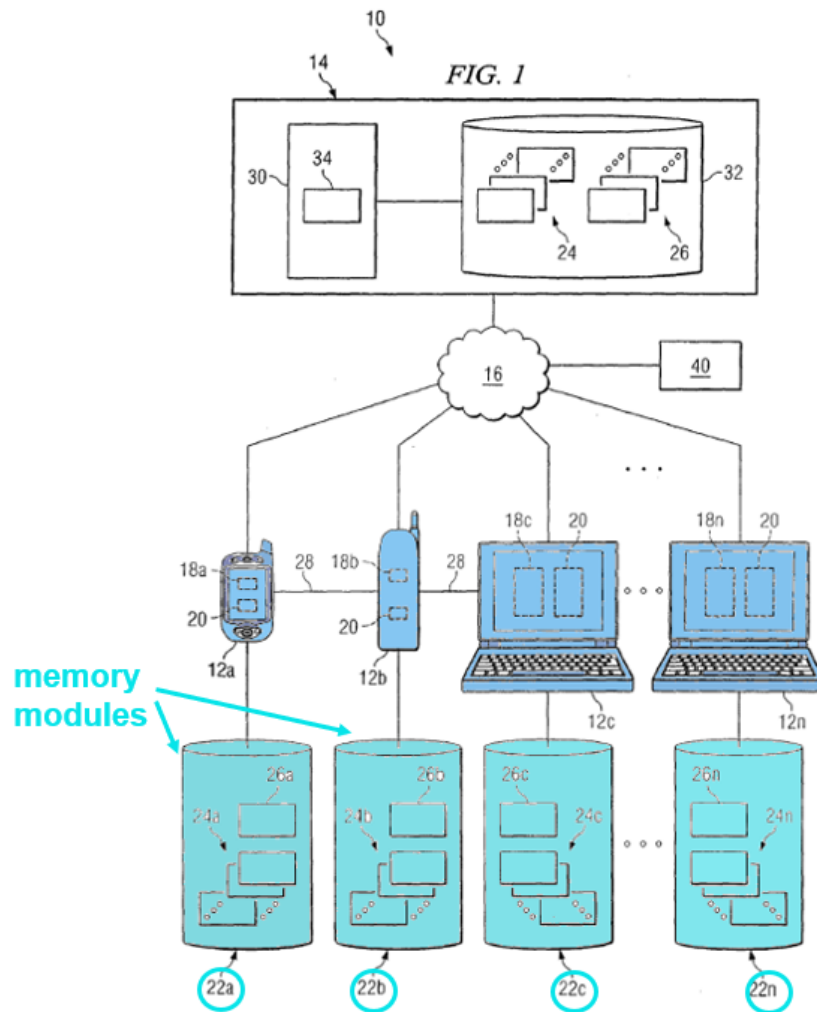
- e. **Element 1[d]: one or more memory devices coupled to the one or more processors, the one or more memory devices storing a set of instructions that when executed by the one or more processors cause the one or more processors to perform operations including:**

98. In my opinion, Ribaud teaches Element 1[d].

99. Ribaud explains that its “[m]obile devices 12 may each have an

⁷ Moreover, as I explained in the Technological Background section, using a processor and memory with instructions to execute functions on mobile devices was known by 2008. *See, e.g.*, Section VII.I (citing Ex-1009 (Krikorian) ¶¶6, 30-32; Ex-1028 (Gulin), ¶¶29, 79-80, Fig. 2; Ex-1029 (Kondou) ¶¶23, 29.).

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.

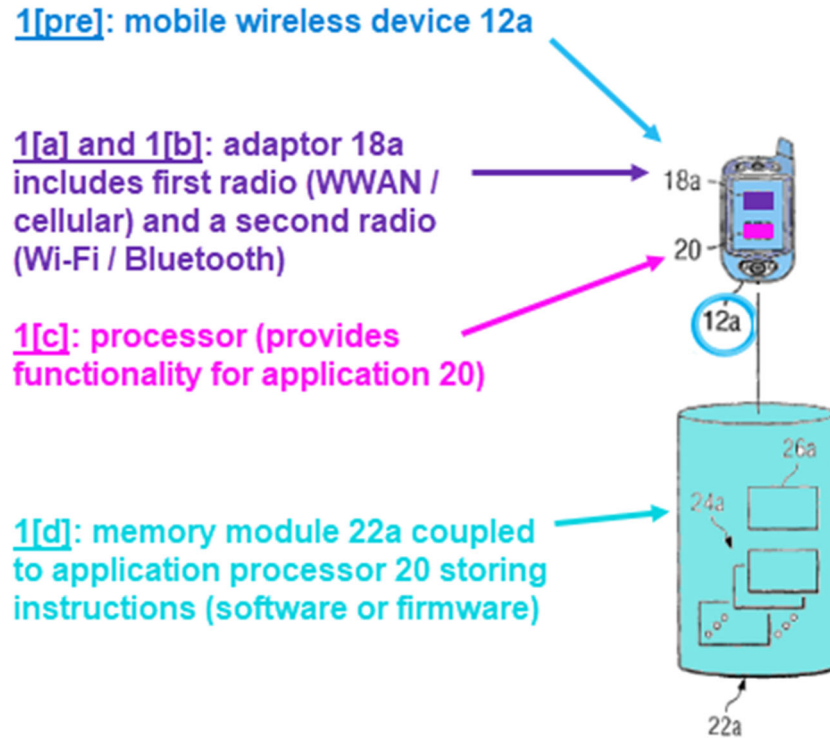


100. Specifically, “[m]emory module 22 may store various data associated with the user of mobile device 12,” including “one or more user profiles 24 for the user of mobile device 12[,] ... match data 26 downloaded from data center 14 and identifying one or more predetermined matches for the user[, and]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

101. Along with data, the memory module 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).

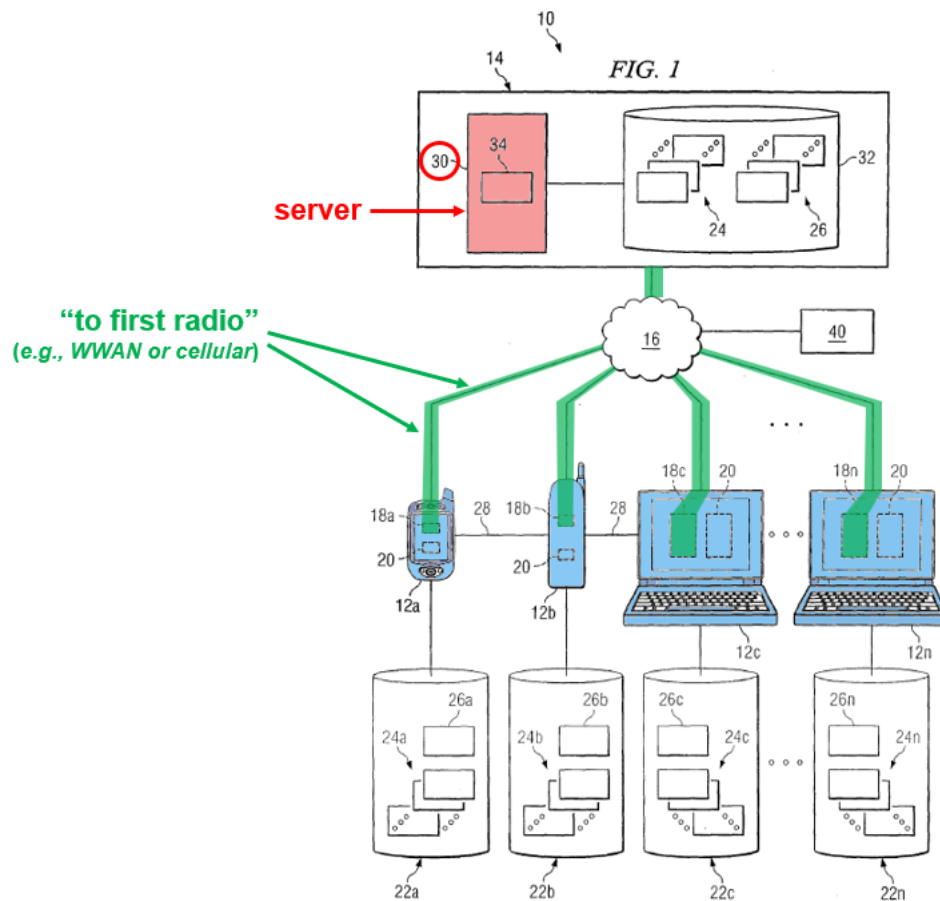
102. Accordingly, as I have depicted below, a POSITA would have recognized that the mobile device 12a includes a memory module 22 that is coupled to one or more processors (for running application 20), and that stores a set of software instructions that when executed by the processors, cause the processors to perform the communication services operations described further below. Moreover, as I explained in the Technological Background section, using a processor and memory with instructions to execute functions on mobile devices was known by 2008. *See, e.g.*, Section VII.I (citing Ex-1009 (Krikorian) ¶¶6, 30-32; Ex-1028 (Gulin), ¶¶29, 79-80, Fig. 2; Ex-1029 (Kondou) ¶¶23, 29.).



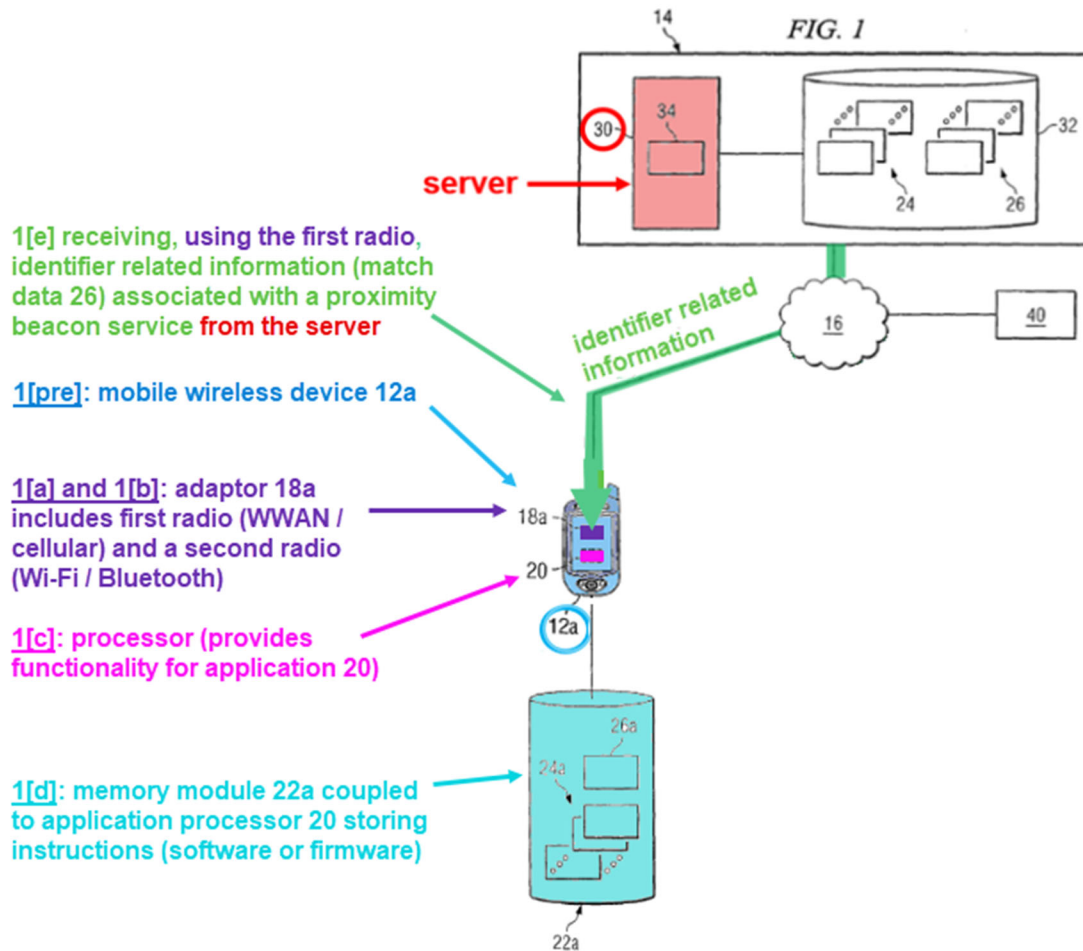
- f. **Element 1[e]: receiving, using the first radio, identifier related information associated with a proximity beacon service, from one or more servers;**

103. In my opinion, Ribaudo teaches Element 1[e].

104. Ribaudo discloses that its “[d]ata center 14 includes a server system 30” (red) as shown in Figure 1. Ex-1007, ¶34, Fig. 1.



105. 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 I have 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.



106. 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 beaconsed data may be broadcast

within any suitable range, depending on the technology being employed.” Ex-1007, ¶57; *see also* ¶123 (“In ad-hoc mode, in certain embodiments, application 20 may beacon an SSID of ‘proprietor_name.net’ (e.g., where ‘proprietor_name’ corresponds to the name of a proprietor of system 10).”); *see also id.*, ¶¶157, 173 (further describing beaconing by mobile devices 12).

107. 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.

- 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);**

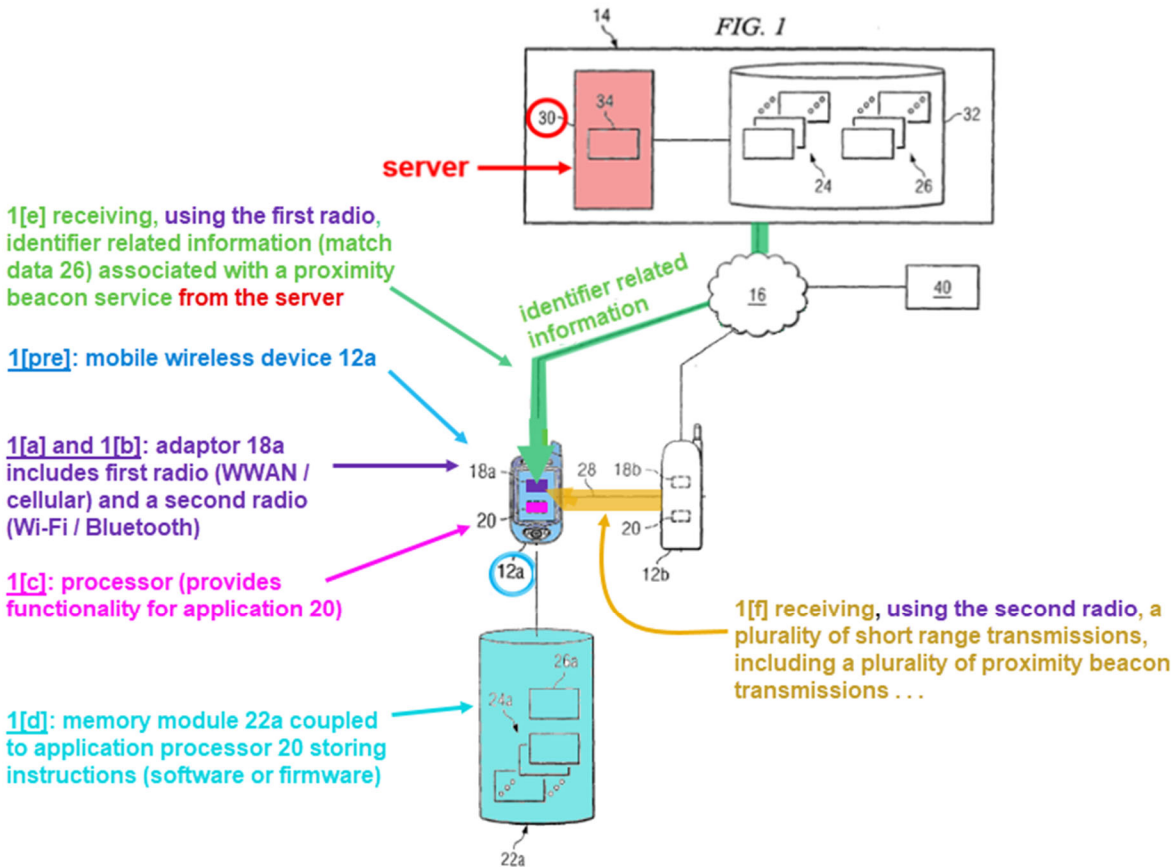
108. In my opinion, Ribauda teaches Element 1[f][1].

109. Ribauda discloses that its mobile devices receive proximity beacon

transmissions from other mobile devices that are located within a detection range. For example, Ribaudó 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).” Ex-1007, ¶57. Accordingly, as depicted below, if 12a is the recited wireless mobile device then 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. Moreover, using beacon transmissions to make proximity determinations was known to a POSITA by 2008. *See, e.g.*, Section VII.A (citing Ex-1009 (Krikorian) ¶¶4-5, 25, Fig. 2; Ex-1027 (Lazaridis), 2:3-10, 3:44-46, 3:59-65; Ex-1028 (Gulin), Abstract; Ex-1029 (Kondou) ¶1; Ex-1010 (Mgrdechian) ¶73; Ex-1030 (Quigley), Abstract; Ex-1033 (Langensteiner) ¶¶20-21).

110. Ribaudó further discloses that 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. I have illustrated this below, based on Ribaudó's Figure 1.



111. 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.”); *see also id.*, ¶¶123, 157, 173 (further describing beaconing by mobile devices 12). The proximity beacon transmissions, based on Wi-Fi or Bluetooth, are “short range,” when compared to

cellular/WWAN transmissions.

112. Finally, there are a plurality of such short-range, proximity beacon transmissions. A POSITA would have understood Ribaudo’s explanation that “[m]obile devices 12 may **beacon** data that can be used to identify them,” Ex-1007, ¶191, along with Ribaudo’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. This is because Wi-Fi and Bluetooth beacons are well-known to POSITAs as periodic signals (sent a plurality of times).

113. As shown in the Wi-Fi Specification, Figure 11-1 (below) shows beacon transmissions being sent periodically, once every “Beacon interval.”

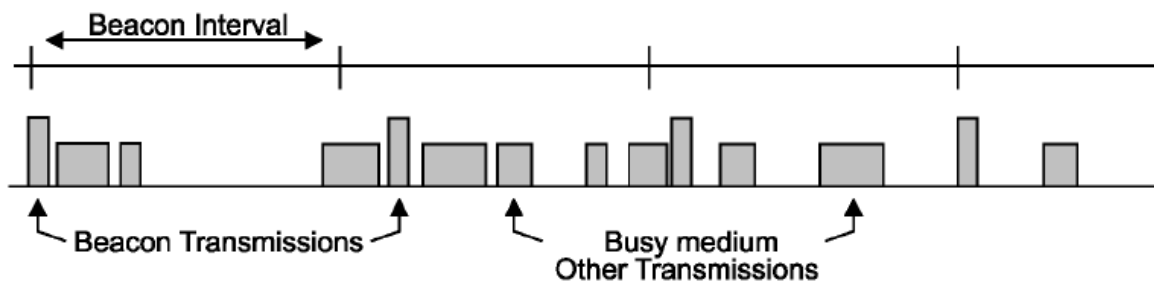


Figure 11-1—Beacon transmission on a busy network

Ex-1025 (“Wi-Fi Specification”) at 420; *see also* Section VII.D, *supra*.

114. The Bluetooth specification similarly explains that “The **beacon train**

consists of one beacon slot or a train of equidistant beacon slots that is **transmitted periodically** with a constant time interval.” Ex-1026 (Bluetooth Specification) at 131-32. The Bluetooth specification further explains that “The beacon train serves four purposes: a) Transmitting master-to-slave packets that the parked slaves can use for resynchronization b) Carrying messages to the parked slaves to change the beacon parameters c) Carrying general broadcast messages to the parked slaves d) Unparking one or more parked slaves.” Ex-1026 (Bluetooth Specification) at 132.

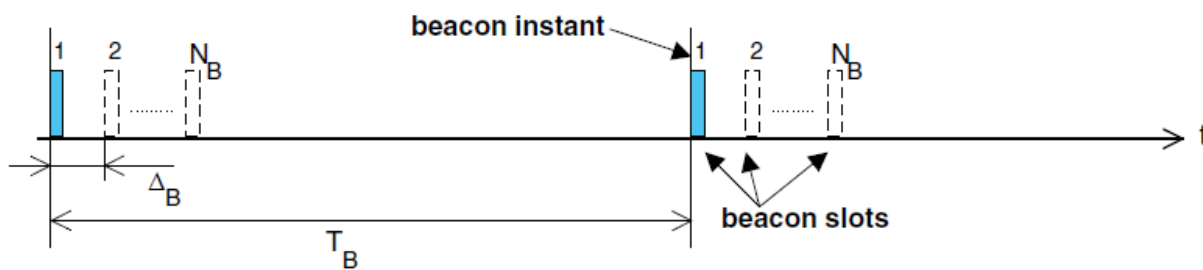


Figure 72—General beacon train format

Ex-1026 (Bluetooth Specification), Fig. 72.

115. More generally, a “beacon”—by definition—entails continuous or periodic transmissions of data (including identifiers) in order to facilitate device discovery. Ex-1024 (Wikipedia, “Radio beacons”) (“Radio beacons transmit a continuous or periodic radio signal with limited information (for example, its identification or location) on a specified radio frequency.”); Ex-1022 (‘beacon channel,’ ‘beaconing’); Ex-1023 (‘beaconing’); *see also* Section VII.D, explaining that, by 2008, it was known by POSITAs to periodically transmit a beacon signal.

The Watanabe reference also corroborates this, 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).” Ex-1006, ¶46.

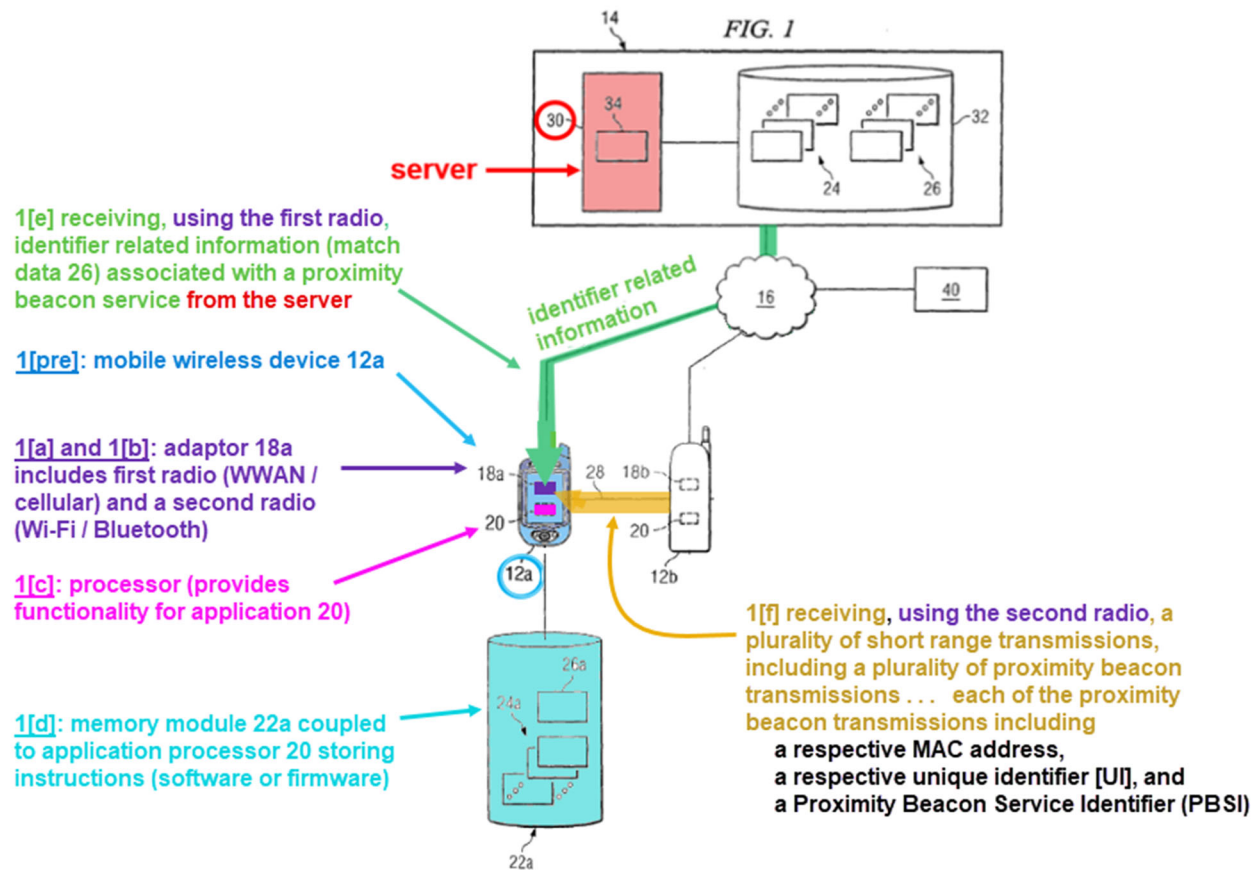
116. This is further confirmed by Ribaud. For example, Ribaud explains that “John’s mobile device 12 detects Steve’s mobile device 12 at a first time” and subsequently “detects Mary’s mobile device 12 at a second time,” Ex-1007, ¶148, which teaches that John’s device *receives a plurality* of short-range, proximity beacon transmissions.

117. Ribaud also teaches Element 1[f][2].⁸ As I have shown in the below chart and annotation, Ribaud 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	Ribaud
---------------	--------

⁸ For context, as I explained in the Technological Background above, by 2008, it was known to use MAC addresses, unique identifiers, and beacon service identifiers to identify devices and networks. *See* Section VII.B (citing Ex-1009 (Krikorian) ¶¶21, 23, Fig. 3; Ex-1029 (Kondou) ¶35; Ex-1031 (Godfrey) ¶¶34, 54, 55; Ex-1032 (Jansen), 23-24; Ex-1033 (Langensteiner) ¶¶38-39, 58; Ex-1028 (Gulin), ¶69; Ex-1010 (Mgrdechian) ¶¶50, 91; Ex-1035 (Tamura), ¶47, Fig. 4; Ex-1035 (Tamura) ¶¶48, 37-38, 53, 140, 173; Ex-1039 (Sorte) 4, 5; Ex-1036 (Saund), 1:63-2:9, 2:25-30, 2:45-63, 3:9-12; Ex-1037 (Suzuki) ¶¶46, 50, 55, 57; Ex-1038 (Briancon), ¶7). It was further known to include identifiers in beacon transmissions. *See* Section VII.C (citing Ex-1026 (Bluetooth Specification), 131-32, Fig. 72; Ex-1025 (Wi-Fi Specification) at 80-81, 419-420.).

“MAC address”	MAC address of transmitting device (12b)
“Unique identifier”	client ID and potentially other suitable information for uniquely identifying a user (12b) ⁹
“PBSI”	SSID of the proprietor of the system (10)



118. **MAC address:** As Ribaudo explains, “[t]he adaptor 18 of a mobile

⁹ As discussed below, Ribaudo contemplates that, in addition to “client ID”, other suitable information can be used to uniquely identify a mobile device user.

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. Ribaudó 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.

119. **Unique identifier:** Ribaudó further teaches that “[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*.”

120. **Proximity Beacon Service Identifier (“PBSI”)**: The term “PBSI” is not an industry term of art, but in the context of the record of the ’918 Patent, its plain and ordinary meaning encompasses the “SSID” of Ribaudó’s system. 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.

121. Ribaudó’s disclosed “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); *see also id.*, ¶¶29, 55, 162, 223, 226 (further discussing providing dating

related services to users within a geographic area).

122. *Second*, as I discussed in Section VIII above, during prosecution, the inventor of the '918 Patent submitted a declaration, in which he explained 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 ("the claimed 'PBSI' is the SSID"); *see also id.*, ¶46 ("the invention claimed in the '410 application uses a certain type of radio transmission, called a proximity beacon, to activate special services when one wireless device is detected near another."); ¶148 ("the purpose of the PBSI is to identify transmissions associated with the proximity beacon service. The PBSI for a given service is shared among multiple wireless devices that use the service."); Ex-8, n.5; Ex-1001, 10:52-59.

- 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:**

123. In my opinion, Ribauda teaches Element 1[g].

124. Ribauda teaches that, in its system, proximity determination requires a mobile device first *determining* if it received certain identifiers from another mobile

device. For example, Ribaudó discloses that “a first user’s mobile device detects the presence of a second user’s mobile device in proximity based on *network identifiers* communicated from the mobile devices of the first and second users,” and that this detection is achieved by “*processing* the [received] network identifiers.” Ex-1007, ¶7; *see also id.*, ¶6, cl. 1. Ribaudó discloses that 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 Ribaudó as teaching that an SSID (*i.e.*, the PBSI identified for Element 1[f] above) may also be a “network identifier,” since Ribaudó explains that “SSIDs ... *represent* one or more network identifiers,” and “provide ‘human readable versions of MAC addresses or other network identifiers.’” Ex-1007, ¶213.

125. As discussed for Element 1[f] above, Ribaudó 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.

126. Ribaudó further teaches that a 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, ¶¶6-7; *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.”). Ribaudó’s teaching of “processing” and subsequently “comparing” network identifiers entails *determining that such identifiers are present* in the beacon transmission.

127. Accordingly, Ribaudó teaches determining that its beacon transmissions include a MAC address and a PBSI.

128. 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. Ribaudó 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, Ribaudó’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.

- 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.**

129. In my opinion, Ribaudó teaches Element 1[h].

130. Ribaudó 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

131. For example, 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).

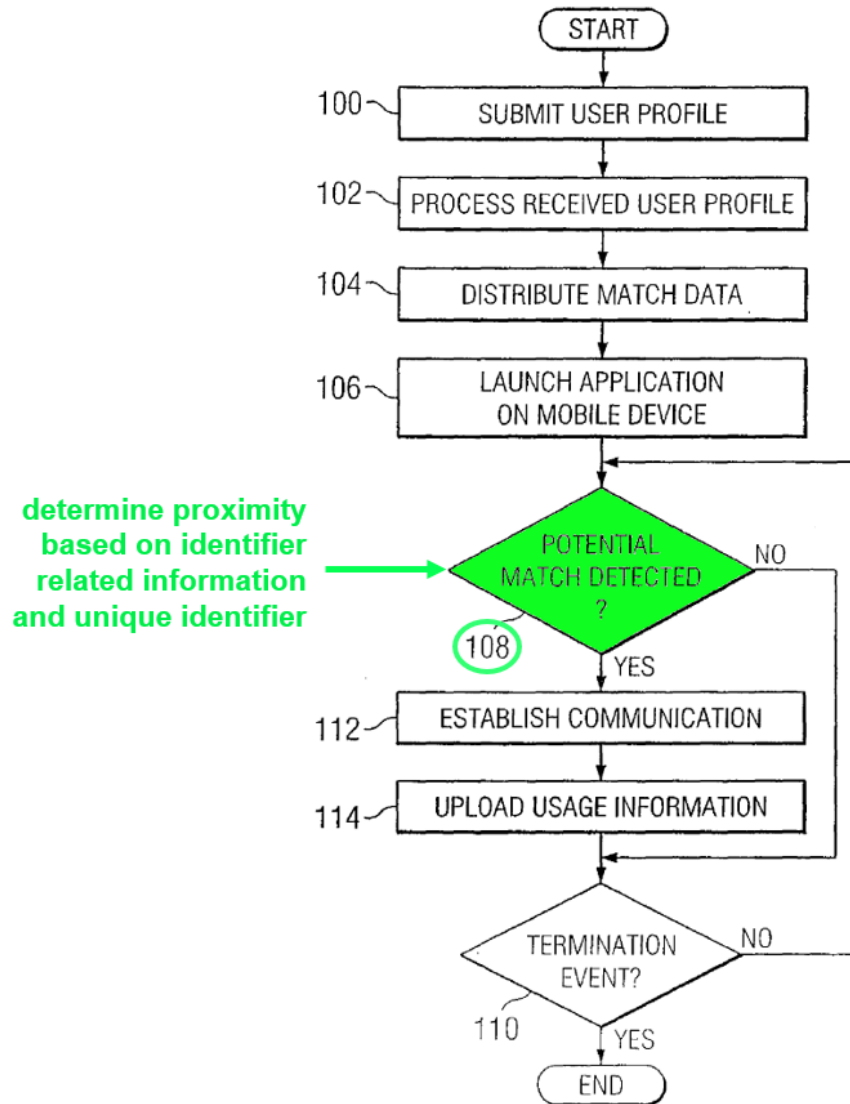
132. In Ribaudo’s Figure 2, “a user of mobile device 12a submits a user profile 24a to data center 14,” which then “pre-processes the information ... to generate match data 26 for the user,” and then “distributes the generated match data to one or more appropriate mobile devices 12.” Ex-1007, ¶¶80-83, 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 beaconsed by other mobile devices 12.

Ex-1007, ¶84.

FIG. 2



133. Finally: “[a]t 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.

134. Further, in Ribaudó’s example where “John’s mobile device 12 detects Steve’s mobile device 12 at a first time” and “detects Mary’s mobile device 12 at a second time,” Ribaudó explains that “[i]f the second time is within a predefined time period from the first time, then it may be assumed that Steve and Mary are in proximity,” and they both receive a notification if they are a match. Ex-1007, ¶148.

135. Accordingly, in Ribaudó’s process, a 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”).

2. Independent Claim 9¹⁰

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

¹⁰ The limitations of claim 9 closely map to the limitations of claim 1, as I have indicated below.

136. In my opinion, Ribaudo teaches Element 9

```
. See Elements 1

```
, 1[c], 1[d], and 1[e] above.
```


```

- b. Element 9[a]: communicating between the mobile device and one or more servers and receiving, at the mobile device, identifier related information, using a first radio;**

137. In my opinion, Ribaudo teaches Element 9[a]. *See* Elements 1[a] (first radio) and 1[e] above.

- c. Element 9[b]: receiving, at the mobile device using a second radio, a plurality of short range transmissions, including a plurality of proximity beacon transmissions from one or more beacon transmitter devices associated with a proximity beacon service, each of the proximity beacon transmissions including a respective MAC address, a respective unique identifier (UID), and a Proximity Beacon Service Identifier (PBSI);**

138. In my opinion, Ribaudo teaches Element 9[b]. *See* Elements 1[b] (second radio) and 1[f] above.

- d. Element 9[c]: a) determining that a particular short range transmission of the plurality of short range transmissions includes a MAC address, b) determining that the Proximity Beacon Service Identifier (PBSI) is present, and c) determining that the PBSI indicates the particular short range transmission is a proximity beacon transmission associated with the proximity beacon service; and when the three determining steps a) b) and c) are each true, then**

139. In my opinion, Ribauda teaches Element 9[c]. *See* Element 1[g] above.

- e. **Element 9[d]: d) determining that an entity or object associated with the proximity beacon service is within proximity to the mobile device, by utilizing the identifier related information and the unique identifier.**

140. In my opinion, Ribauda teaches Element 9[d]. *See* Element 1[h] above.

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.**

141. In my opinion, Ribauda teaches Claim 4.

142. As discussed for Elements 1[f] and 1[h] above, Ribauda 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.

143. Ribauda further teaches that the proximity determination may be made at a later time, based on one or more 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.

144. Finally, the term “action function” is not an industry term of art, but in the context of the record of the ’918 Patent, 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. I note that 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-1004

at 1558 (Proctor Decl. ¶134).

- 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.**

145. In my opinion, Ribauda teaches Claim 5.

146. Ribauda teaches that the receiving mobile 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. For example:

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. ... In certain embodiments, tagged information for a location may be shared with other users who use the location to provide context for the other users' detected matches at the location, and may be used for a variety of other purposes.

Ex-1007, ¶117; *see also id.*, ¶212.

147. Ribaudó further discloses “implied proximity,” which involves “distribut[ing] pre-processed matches to members of a particular group ***at a particular location*** and/or time. The members of the group may be assumed to be close enough for some or all members of the group to detect one another (e.g., within walking distance)”—for example, “a conference, a cocktail party, a speed-dating event, a coffee shop, an airport, a university, a wedding, or any other suitable gathering of users that is known or scheduled in advance.” Ex-1007, ¶0160. Ribaudó further explains that “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.” Ex-1007, ¶163.

- 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.**

148. In my opinion, Ribauda teaches Claim 6.

149. Ribauda teaches that its “identifier related information” comprises application software, which is downloaded in response to sending the unique identifier to at least one server. *First*, Ribauda 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.

150. *Second*, Ribauda 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. ...[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, ¶140.¹¹ Further, as discussed for Element 1[e], the data center contains a server. Ex-1007, ¶34, Fig. 1.

- 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.**

151. In my opinion, Ribauda teaches Claims 14 and 19.

152. For example, Ribauda teaches that a 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)

¹¹ Similarly, I note that 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,” and 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).

associated with being within proximity to the mobile device. Specifically, Ribaud 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).

153. Ribaud also teaches that the “*further information*” may correspond to advertisements targeted to specific users. Specifically, “[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. Ribaud further teaches that “[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.”¹² Ex-1007, ¶217. Moreover, as I explained in the Technological Background section, by 2008, it was known to store information at servers, and to have mobile devices communicating with servers to obtain stored information. *See, e.g.*, Section VII.E (citing, *e.g.*, Ex-1009 (Krikorian) ¶¶9, 24); Ex-1027 (Lazaridis), 2:11-23, 2:34-36, 4:10-20, 5:66-6:20, Figs. 1, 4; Ex-1010 (Mgrdechian) ¶¶18, 20, 21, 75; Ex-1039 (Sorte), 2; Ex-1028 (Gulin) ¶¶70, 72; and Ex-1029 (Kondou) ¶10.

- 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.**

154. In my opinion, Ribaudo teaches Claims 16 and 24.

155. Ribaudo teaches various ways of “controlling further communications

¹² I note that 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.

between the mobile device and at least one device or server associated with an entity” in proximity. For example, Ribauda discloses controlling further communications in the form of advertisements or other sales-related communications. *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).”).

156. Ribauda 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. A field ID for “University,” for example, could be XML6463, and the value entered into that field by the user of mobile device 12 a may be “Harvard.” When a detection event occurs based on the field ID “XML6463” (e.g., the user of mobile device 12a and the user of mobile device 12b are within a predetermined or other suitable proximity and it is determined that both have specified “Harvard” as the value for “University”), “Harvard” may be displayed on mobile device 12b, for example.”).

Ex-1007, ¶47.

157. Ribauda 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.

- 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.**

158. In my opinion, Ribauda teaches Claim 17.

159. Ribauda 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.

160. 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.”

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.

161. In my opinion, Ribaud teaches Claims 18 and 28.

162. As discussed for Elements 1[a] and 9[a], Ribaud 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.

163. 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. Moreover, I explained in the Technological Background section, by 2008, it was known to store information at servers, and to have mobile devices communicating with servers to obtain stored information. *See, e.g.*, Section VII.E (citing, *e.g.*, Ex-1009 (Krikorian) ¶¶9, 24); Ex-1027 (Lazaridis), 2:11-23, 2:34-36, 4:10-20, 5:66-6:20, Figs. 1, 4; Ex-1010 (Mgrdechian) ¶¶18, 20, 21, 75; Ex-1039 (Sorte), 2; Ex-1028 (Gulin) ¶¶70, 72; and Ex-1029 (Kondou) ¶10.

- 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.**

164. In my opinion, Ribaudou teaches Claim 20. For the reason I explained for Claim 14 above, Ribaudou teaches the method of Claim 19 wherein the “further information” relates to advertising content. *See* Claims 14 and 19 above; Ex-1007, ¶¶140, 215, 217.

- 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.**

165. In my opinion, Ribauda teaches Claim 22.

166. Ribauda 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. ... [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, ¶¶140-143; *see also id.*, ¶120 (“In certain embodiments, the present invention allows users of mobile devices 12 who have installed application 20 to distribute copies of application 20 to other users of other mobile devices 12 who have not installed application 20, which may allow the other users to access one or more

features of system 10.”).

- 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.**

167. In my opinion, Ribauda teaches Claim 25.

168. As explained for Elements 1[h] and 9[d] above, in Ribauda’s system, a mobile device determines that an entity (*e.g.*, user of another mobile device) is in proximity, by comparing its preset match data (*i.e.*, “identifier related information”) with the client ID of the other mobile device (*i.e.*, “unique identifier”). *See, e.g.*, Ex-1007, ¶6 (“Subsequently, 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.”), ¶85 (“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.” Ex-1007, Fig. 2.¹³

k. Claim 26:

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

169. In my opinion, Ribauda teaches Element 26[pre]. *See* Claim 9 above.

(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:

170. In my opinion, Ribauda teaches Element 26[a]. *See* Claim 14 above.

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

171. In my opinion, Ribauda teaches Element 26[b].

172. Ribauda teaches that the 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., the sender of the unique identifier). For example, Ribauda teaches “processing the network identifiers received from the first and second mobile devices to determine whether the first mobile device and the second mobile

¹³ Moreover, as I explained in the Technological Background section, filtering beacon transmissions by comparing stored information to transmitted information to determine matches was known to a POSITA by 2008. *See, e.g.*, Section VII.F (citing Ex-1031 (Godfrey) ¶¶11, 35; Ex-1009 (Krikorian) ¶¶4-5, 26; Ex-1032 (Jansen), 8).

device are in proximity to one another.” Ex-1007, ¶7.

173. In addition, Ribauda teaches that the data center generates *match data* based on user profiles submitted to the data center (Ex-1007, ¶¶26, 83), and that the user profiles may specify a particular city (Ex-1007, ¶99). Accordingly, 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). Ribauda similarly teaches that “system 10 supports connections based on tag information” (Ex-1007, ¶108), which may include location-based tags (Ex-1007, ¶¶117, 212).

(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;

174. In my opinion, Ribauda teaches Element 26[c].

175. Ribauda teaches that the server stores a user’s purchasing practices or requests from the servers related to the associated entity information as stored proximity user behavior. For example, Ribauda explains that “[d]ata center 14 may collect and store personality attributes and group attributes of users who encounter certain networks over time,” and that “[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. Ribauda further specifies that

“[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).

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

176. In my opinion, Ribauda teaches Element 26[d].

177. For example, Ribauda teaches that a data center generates match data by processing, evaluating, and/or comparing “user profiles 24.” Ex-1007, ¶¶6, 40-41. In turn, Ribauda teaches that 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,” Ex.1007, ¶94, thereby storing multiple email addresses associated with respective users of respective mobile devices.

178. As I discuss 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 associated with the mobile device, in order to “facilitate sales initiated by emails.” Ex-1007, ¶140.

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

179. In my opinion, Ribaudo teaches Element 26[e].

180. As discussed for Elements 26[c] and 26[d], Ribaudo teaches that the 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.

181. Ribaudo also discloses scenarios in which “*customized content*,” which may be based on such “stored proximity user behavior,” is sent via email from the server to a user. For example, Ribaudo explains that a “plug-in” may be added to an email application to “*display what the first and second users share in common*,” and that this feature allows “sales people ... to facilitate sales initiated by emails” that “may increase the chances of a response by allowing the recipient to view what he shares in common with the sales person.” Ex-1007, ¶140. Ribaudo 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.”).

- 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.**

182. In my opinion, Ribaudo teaches Claim 27. *See* Claim 25 and Elements 1[h] and 9[d] above.

- 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.**

183. In my opinion, Ribaudo teaches Claim 29.

184. As discussed for Elements 1[f] and 9[b] above, in Ribaudo's system, mobile devices are "beacon transmitters." For example, Ribaudo explains that mobile devices "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 being employed." Ex-1007, ¶57; *see also id.*, ¶76. Accordingly, in Ribaudo's system, a given mobile device is *not required* to first transmit anything to the transmitting devices, in order to receive the beacon transmissions.

n. Claim 30:

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

185. In my opinion, Ribauda teaches Element 30[pre]. *See* Claim 1, above.

(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:

186. In my opinion, Ribauda teaches Element 30[a].

187. As discussed for Element 1[e] above, Ribauda 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.

188. Ribauda further teaches that such match data includes, or considers a “list of contact information.” For example, Ribauda teaches that data center generates match data (*i.e.*, identifier related information) by processing, evaluating, and/or comparing “user profiles 24.” Ex-1007, ¶¶6, 40-41. In turn, Ribauda teaches that a user profile may include a list of contacts for that user. Specifically, 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.” Ex.1007, ¶94; *see also id.*, ¶27 (“User profile information may include ... contacts.”).

189. Ribaudó also teaches that 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.

- (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;**

190. In my opinion, Ribaudó discloses Element 30[b].

191. As discussed for Element 30[a], Ribaudó teaches that each 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.” Ex-1007, ¶26. 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.

192. 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], Ribaudó teaches that 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], Ribaudó explains that 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, Ribaudó 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).

- (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.**

193. In my opinion, Ribaudó teaches Element 30[c].

194. Specifically, Ribaudó 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.

195. Further the receiving “[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. Finally, Ribauda teaches that 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).

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

196. 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 indicating the type of service that can be provided via that access point” in a

proximity beacon transmission. *See* Ex.1006, ¶¶14-15, Fig. 2.

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.

197. In my opinion, in addition to the reasons set forth below, 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. Specifically, both Ribaudó and Watanabe teach devices with two communication interfaces – one, short-range and the second, long-range. For example, Watanabe teaches a Client Terminal that receives induction beacons to an access point via a first communication means and communicates through the Internet via a second communication means (see Ex-1006 Fig. 1). Similarly, the mobile devices in Ribaudó (shown, for example, as units 12a, 12b, ... in Fig. 1) have short range links to one another (“In Fig.1, links 28 illustrate example ad-hoc connections between mobile devices” Ex-1007 ¶66). At the same time, the mobile devices have a separate connection to a web service. For example, referring to Fig.1, Ribaudó states “Mobile devices 12 may connect to network 16, where appropriate, through a wired or wireless link” Ex-1007, ¶25.

198. In Ribaudó's wireless communication system, “when the user is in

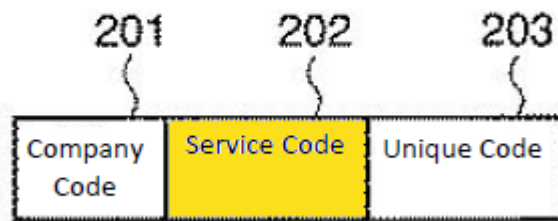
proximity to another user, the user's mobile device detects the presence of the other user's mobile device, receives an identifier associated with the detected other user, and compares the received identifier with the pre-processed match data stored on the user's mobile device to determine whether the other user is one of the user's predetermined matches." Ex-1007 ¶6. Ribaudó further teaches that its 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'...." Ex-1007, ¶123. Additionally, "[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.

199. As I discussed for Element 1[g] in Ground 1 above, a POSITA would have understood that Ribaudó'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, even assuming Ribaudó's SSID were *not* considered a PBSI, it nonetheless would have been obvious to include a PBSI in Ribaudó's beacon transmissions, based on Watanabe's teachings.

200. Watanabe discloses a wireless communication system including 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.” *Id.* Ex.1006, ¶¶14-15, Fig. 2.¹⁴

[FIG. 2]



201. 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 mentions that its “mobile devices 12 may be used as reference beacons in system 10 in a substantially similar

¹⁴ Moreover, as I explained in the Technological Background section, the use of MAC addresses, unique identifiers, and beacon service identifiers to identify devices and networks was known to a POSITA by 2008. *See, e.g.*, Section VII.B (citing, e.g., Ex-1009 (Krikorian) ¶¶21, 23, Fig. 3; Ex-1029 (Kondou) ¶35; Ex-1031 (Godfrey) ¶¶34, 54-55; Ex-1032 (Jansen), 23-24; Ex-1033 (Langensteiner) ¶38; Ex-1034 (Suresh) ¶¶39, 58; Ex-1028 (Gulin) ¶69; Ex-1010 (Mgrdechian) ¶¶50, 91; Ex-1035 (Tamura) ¶¶47-48, 173, Fig. 4; Ex-1039 (Sorte), 4-5; Ex-1037 (Suzuki) ¶¶46, 50, 55, 57).

manner to the manner in which network access points ... are used.” Ex-1007, ¶77. Ribaudo also states that “although MAC addresses and SSIDs are primarily described, [its] invention contemplates use of any other suitable identifiers ... according to particular needs.” Ex-1007, ¶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. 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.

202. Thus, a POSITA would have been motivated to include a service code, as taught by Watanabe, along with Ribaudo’s other identifiers (MAC addresses, SSIDs, and client IDs) in its beacon transmission, in order to help identify and facilitate communication with other devices relevant to a given service, while preserving bandwidth and other costs, in an ad hoc network as disclosed in Ribaudo.

203. A POSITA would have had a reasonable expectation of success in applying Watanabe’s teachings to Ribaudo. 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

204. As I explained for Ground 1 above, Ribaudo teaches Elements 1[pre], 1[a]-1[e], and 1[h]. *See supra* Section XI.A.1.

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

205. In my opinion, Ribaudo in view of Watanabe teaches Element 1[f].

206. As discussed for Element 1[f] in Ground 1, Ribaudo's disclosed "SSID" qualifies as a PBSI. *See* Section XI.A.1.g.(3). Regardless, it would have been obvious to a POSITA at the time of the alleged invention to incorporate a PBSI in Ribaudo's beacon transmissions, as taught by Watanabe. Watanabe discloses an 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. A POSITA would have been motivated to combine Watanabe and Ribaudó with a reasonable expectation of success for the reasons I explained in Section XI.B.1 above.

207. 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

b. Element 1[g]:

208. In my opinion, Ribaudó-Watanabe teaches Element 1[g].

209. As discussed for Element 1[g] in Ground 1, Ribaudó discloses that its “network identifiers,” such as “MAC address,” are “process[ed]” upon receipt, and are subsequently “compared” with pre-processed match data, which teaches that a receiving device determines that the beacon transmission includes such network identifiers. *See* Section XI.A.1.h. In the Ribaudó-Watanabe combination, such

“network identifiers” would additionally include Watanabe’s “service code.” *See* Ex-1006, ¶15 (disclosing “a service code 202 indicating the type of service that can be provided via that access point 11”). Accordingly, Ribaud-Watanabe teaches determining that the beacon transmissions include a MAC address and a PBSI as reflected below.

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

210. Further, the PBSI of Ribaud-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.

3. Independent Claim 9

211. In my opinion, the following limitations of Claim 9 are taught by either:

- (1) Ribaud, as shown in the corresponding limitations in for Claim 1 in Ground 1;
- (2) Ribaud-Watanabe, as shown in the corresponding limitations for Claim 1 in Ground 2 above.

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

212. In my opinion, Ribaud-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 XI.A.3.a and XI.A.3.c-n.

a. Claim 5:

213. In my opinion, Ribaud teaches the added limitation of Claim 5, for the reasons I discussed in Ground 1 above. *See supra* Section XI.A3.b.

214. In my opinion, Watanabe also teaches this limitation. For example, 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..

215. Accordingly, Ribaudo-Watanabe teaches dependent Claim 5.

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.

216. In my opinion, in addition to the reasons set forth below, 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 XI.A.1, XI.B.1. As I discussed for Ground 2 above (see Section XI.B.1), both Ribaudo and Watanabe teach devices with two communication interfaces – one short-range and the second, long-range. Behrens (Ex-1008) also teaches devices with two such interfaces. For example, Fig. 2 of Behrens shows two devices transferring unique identifiers wirelessly between one another (“the device is a portable electronic device (a) transmitting continuously / repeatedly one or more unique identifiers (UID) via non-directional wireless radio frequency signals,” Ex-

1008, 28:16-18). At the same time, the devices have a second interface to transfer the “seen log” to a server. For example, it is stated that “the software may also allow the device to transfer the seen logs to a server. This could include uploading the seen log information directly to the server via any available connection such as GSM, UMTS, or WLAN, for example.” Ex. 1008, 22:15-18.

217. As explained for Grounds 1 and 2 above, Ribaud, 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”).

218. 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.

219. 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,” Ex-1007, ¶46. Ribaudo also teaches “***time-slicing*** to join and bounce between several networks.” Ex-1007, ¶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).” Ex-1007, ¶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.*

220. 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. 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 the Ribaudo-Behrens and Ribaudo-Watanabe-Behrens combinations, 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.

221. A POSITA would have had a reasonable expectation of success in combining Ribaudo or Ribaudo-Watanabe with Behrens. 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, Ribaudó already contemplates a system that may assign multiple unique identifiers to a given user in order to “shield” or “reveal” her true identity in different circumstances. Ex-1007, ¶¶45, 68. A POSITA would thus have understood that applying Behrens’ teachings to the Ribaudó and Ribaudó-Watanabe systems would have yielded predictable results.

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.**

222. In my opinion, Ribaudó-Behrens and Ribaudó-Watanabe-Behrens teach Claim 2.

223. As discussed for Element 1[f] above, Ribaudó 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 (Bluetooth Core Specification V.2.0 (2004)) at 232. 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.”).

224. 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. *See, e.g.*, Huang, L. et al., *Enhancing wireless location privacy using silent period*, IEEE WIRELESS COMMUNICATIONS AND NETWORKING CONFERENCE, (Vol. 2, pp. 1187-1192) (March, 2005) (Ex-1042, “Huang”). This paper discusses the use of randomized MAC addresses in combination with other techniques for improved location privacy. *Second*, Ribaudó itself teaches that “substantial privacy” may be an important consideration for its wireless system. Ex-1007, ¶226. Randomizing a MAC address obscures the identity of the users and also make correlations between different transmissions more difficult. 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.

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:**

225. In my opinion, Ribaudó and Ribaudó-Watanabe teach Element 3[pre].
See Claim 1 for Grounds 1 or 2 above.

- (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**

226. In my opinion, Ribaudó and Ribaudó-Watanabe teach Element 3[a].
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.

- (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**

227. In my opinion, Ribaud-Behrens and Ribaud-Watanabe-Behrens teach Element 3[b].

228. *First*, as discussed for Element 1[f] in Ground 1 above, Ribaud’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-1025 (Wi-Fi Specification) at 420 (“Beacon interval”); Ex-1026 (Bluetooth Specification) at 131-132, Fig. 72 (“beacon train”)); Ex-1007, ¶148. In my opinion, 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).”).

229. *Second*, as discussed in Section XI.C.1, Ribaud 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.

230. *Third*, as further discussed in Section XI.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.

231. 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.

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

232. 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.”

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

233. In my opinion, Ribaud-Behrens and Ribaud-Watanabe-Behrens teach Element 3[c]. *See* Element 3[b] above. As explained in Section XI.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.).

c. Claim 7:

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

234. In my opinion, Ribaudó-Behrens and Ribaudó-Watanabe-Behrens teach Element 7[pre]. *See* Claim 3 above.

(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:

235. In my opinion, Ribaudó-Behrens and Ribaudó-Watanabe-Behrens teach Element 7[a]. *See* Element 30[a] above.

(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

236. In my opinion, Ribaudó-Behrens and Ribaudó-Watanabe-Behrens teach Element 7[b]. *See* Element 30[b] above.

- (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.**

237. In my opinion, Ribaudó-Behrens and Ribaudó-Watanabe-Behrens teach Element 7[c]. *See* Element 30[c] above.

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:**

238. In my opinion, Ribaudó-Behrens and Ribaudó-Watanabe-Behrens teach Element 8[pre]. *See* Element 3[pre] above.

- (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**

239. In my opinion, Ribaudó-Behrens and Ribaudó-Watanabe-Behrens teach Element 8[a]. *See* Element 3[b] above.

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

240. In my opinion, Ribaudó-Behrens and Ribaudó-Watanabe-Behrens teach Element 8[b]. *See* Element 3[c] above.

e. Claim 10:

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

241. In my opinion, Ribaudó-Behrens and Ribaudó-Watanabe-Behrens teach Element 10[pre]. *See* Claim 9 above.

(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

242. In my opinion, Ribaudó-Behrens and Ribaudó-Watanabe-Behrens teach Element 10[a]. *See* Elements 1[f] and 3[a] above.

(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

243. In my opinion, Ribaudó-Behrens and Ribaudó-Watanabe-Behrens teach Element 10[b]. *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.

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.**

244. In my opinion, Ribauda-Behrens and Ribauda-Watanabe-Behrens teach Element 10[c]. *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.

- 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.**

245. In my opinion, Ribauda-Behrens and Ribauda-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. *See* Claim 2 above.

g. Claim 12:

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

246. In my opinion, Ribauda-Behrens and Ribauda-Watanabe-Behrens teach Element 12[pre]. *See* Claim 9 above.

(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

247. In my opinion, Ribauda-Behrens and Ribauda-Watanabe-Behrens teach Element 12[a]. *See* Elements 1[f] and 3[a] above.

(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

248. In my opinion, Ribauda-Behrens and Ribauda-Watanabe-Behrens teach Element 12[b]. *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 Ribaudó (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).

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.**

249. In my opinion, Ribaudó-Behrens and Ribaudó-Watanabe-Behrens teach Element 12[c]. *See* Element 10[c] above.

- 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.**

250. In my opinion, Ribaudó-Behrens and Ribaudó-Watanabe-Behrens disclose Claims 13 and 15.

251. 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. Indeed, Behrens itself teaches the concept of sending only most recently seen unique identifiers to the server—for example, Fig. 2 shows that the “seen list” of UID#1 at the servers has three items (UID#X, UID#Y and UID#2 (new)), while the “seen list” at Device 1 is only UID#2. 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 the unique identifier.

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:**

252. In my opinion, Ribaud-Behrens and Ribaud-Watanabe-Behrens

teach Element 31[pre]. *See* Element 3[pre] above.

- (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**

253. In my opinion, Ribaudó-Behrens and Ribaudó-Watanabe-Behrens teach Element 31[a]. *See* Element 3[b] above.

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

254. In my opinion, Ribaudó-Behrens and Ribaudó-Watanabe-Behrens teach Element 31[b]. *See* Element 3[c] above.

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

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

255. In my opinion, Ribaudó in view of Mgrdechian (Ribaudó-Mgrdechian), or Ribaudó in view of Watanabe and Mgrdechian (“Ribaudó-Watanabe-Mgrdechian”), teach Claim 23. As explained for Claim 22 in Grounds 1 and 2 above, Ribaudó 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).

256. For context, 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**.” Ex-1007, ¶18. While not mentioned explicitly, it would have been obvious, based on Ribaudo’s teachings, that the nearby user’s “application,” for which “further information” is received by the mobile device, is a multiuser game. Mgrdechian demonstrates this.

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

258. As one example, Mgrdechian explains that its invention can be applied to “**gaming applications operating on mobile devices**.” Ex-1010, ¶86. Specifically:

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.

259. Accordingly, it would have been obvious in view of Mgrdechian's teachings to use the Ribaudó or Ribaudó-Watanabe systems in connection 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. 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,

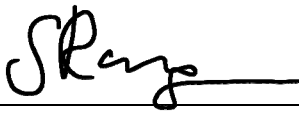
¶6. Further, a POSITA would have had a reasonable expectation of successfully implementing Mgrdechian's gaming application in Ribaudó or Ribaudó-Watanabe, since all three references aim to detect nearby wireless devices and establish communications over Bluetooth and Internet, and since Ribaudó itself contemplates that gaming applications may be used with its system, teaching that its "mobile devices" may be "game consoles." Ex-1007, ¶18.

XII. CONCLUSION

260. For the reasons above, it is my opinion that Claims 1-20 and 22-31 of the '918 Patent are obvious based on each of the grounds specified in my Declaration.

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

Date: May 23, 2025



Dr. Sundeep Rangan