

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. IPR2025-01051
U.S. Patent No. 11,687,971

**DECLARATION OF SUNDEEP RANGAN IN SUPPORT OF PETITION
FOR *INTER PARTES* REVIEW OF U.S. PATENT NO. 11,687,971**

TABLE OF CONTENTS

	Page
I. INTRODUCTION	18
II. BACKGROUND AND QUALIFICATIONS	19
III. INFORMATION CONSIDERED	21
IV. RELEVANT LEGAL STANDARDS	22
A. Claim Interpretation	22
B. Perspective of One of Ordinary Skill in the Art.....	22
C. Obviousness.....	23
V. LEVEL OF ORDINARY SKILL IN THE ART	25
VI. SUMMARY OF MY OPINIONS	27
VII. TECHNOLOGICAL BACKGROUND	27
A. Using Beacon Transmissions to Make Proximity Determinations Was Known	27
B. The Use of MAC Addresses, Unique Identifiers, and Beacon Service Identifiers to Identify Devices and Networks Was Known	32
C. Including Identifiers in Beacon Transmissions Was Known.....	45
D. Periodic Transmission of a Beacon Signal Was Known.....	53
E. Storing Information at Servers and Mobile Devices Communicating with Servers to Obtain Stored Information Was Known	56
F. Filtering Beacon Transmissions by Comparing Stored Information to Transmitted Information to Determine Matches Was Known	62
G. Taking Action if a Match is Determined Between the Stored Information and the Transmitted Information Was Known.....	65
H. Using Protocols Such as Bluetooth and Cellular for Communications Between Mobile Devices and Servers Was Known	70
I. Using A Processor and Memory with Instructions to Execute Functions on Mobile Devices Was Known.....	75

TABLE OF CONTENTS
(continued)

	Page
VIII. THE '971 PATENT AND ITS FILE HISTORY	80
IX. CLAIM CONSTRUCTION	84
X. OVERVIEW OF THE APPLIED PRIOR ART REFERENCES	84
A. Watanabe (Ex-1005, Ex-1006).....	84
B. Ribaudó (Ex-1007)	87
C. Behrens (Ex-1008)	89
XI. DETAILED EXPLANATION OF THE UNPATENTABILITY GROUNDS	90
A. Ground 1: Claims 1, 12-13, 15, 29-31, 34, 36, 50, 56, 61, 64-65, 67, and 80 are obvious over Watanabe in view of Ribaudó.	91
1. A POSITA would have been motivated to combine Watanabe's teachings with Ribaudó's teachings and would have had a reasonable expectation of success.	91
2. Independent Claims 1 and 50.....	96
a. Element 1[pre]: A method comprising: Element 50[pre]: A computer program product for installation in a non-volatile memory in a wireless device, the computer program product comprising computer program instructions that, when read from the non-volatile memory, and then executed by one or more processors in the wireless device, cause the wireless device to:.....	96

TABLE OF CONTENTS
(continued)

Page

b.	Elements 1[a]/50[a]: [receiving, at a wireless device,]/[process a first plurality of beacon transmissions, received at the wireless device] via a [short range]/[Bluetooth] wireless protocol, [a first plurality of beacon transmissions,] each beacon transmission comprising three fields (a) a MAC address, (b) a unique identifier, wherein the unique identifier of each respective beacon transmission does not directly identify a location of a beacon transmitter, and (c) a beacon service identifier, wherein the beacon service identifier of each respective beacon transmission identifies that the unique identifier is relevant to stored information associated with a wireless beacon service, wherein the stored information is not otherwise accessible to the wireless device utilizing the [short range]/[Bluetooth] wireless protocol;	98
c.	Elements 1[b]/50[b]: [receiving, at the wireless device via a second wireless protocol, the stored information from one or more servers,]/[process stored information transferred from one or more servers to the wireless device via a second wireless protocol, wherein] the stored information relat[ing]/[es] to [a particular]/[an] entity or object associated with a first unique identifier, and wherein the second wireless protocol is different from the [short range]/[Bluetooth] wireless protocol;	108

TABLE OF CONTENTS
(continued)

	Page
d. Elements 1[c]/50[c]: [causing selection of]/[select] one or more of the unique identifiers from the first plurality of beacon transmissions, by filtering the beacon transmissions which include a particular beacon service identifier indicating that a particular received beacon transmission is associated with a particular wireless beacon service; and	112
e. Elements 1[d]/50[d]: [taking]/[perform a] first further action[, the first further action] relating to the stored information, if the first unique identifier is present among the selected one or more unique identifiers.	117
3. Dependent Claims 12-13, 15, 29-31, 34, 36, 56, 61, 64-65, 67, and 80.....	119
a. Claims 12/64: The [method]/[computer program product] of claim [1]/[50] wherein the [taking] first further action [further]/[additionally] includes causing the wireless device[,] to: send the first unique identifier or information derived from the first unique identifier to at least one of the one or more servers, and [subsequently] receive the stored information in response [thereto].	119
b. Claims 13/65: The [method]/[computer program product] of claim [1]/[50] wherein the [computer program instructions, when executed by the one or more processors in the wireless device, further cause the wireless device to receive] stored information [is received] at the wireless device from at least one of the one or more servers prior to [the taking]/[performing] of the first further action.....	120

TABLE OF CONTENTS
(continued)

Page

c.	Claims 15/36/67/80: The [method]/[computer program product] of claim [1]/[50] [further comprising]/[wherein the] [computer program instructions][,]/[that,] [when executed by the one or more processors] [in the wireless device, further] [cause the wireless device to]: us[ing]/[e] the stored information to determine if the first unique identifier is present among the [first] selected one or more [of the] unique identifiers [from the first plurality of beacon transmissions]. 121	
d.	Claims 29/56: The [method/computer program product] of claim [1/50] wherein the first further action is [additionally] related to receiving advertising information for presentation to a user of the wireless device, based upon the [first] unique identifier, or [based upon] information derived from the first unique identifier. 121	
e.	Claim 30: The method of claim 1 wherein the first further action includes receiving content from a server based upon information derived from the first unique identifier. 122	
f.	Claims 31/61: The [method/computer program product] of claim [1/50,] wherein [following the taking of] the first further action[,/additionally includes causing the wireless device to send information to] a server associated with an account for a user of the wireless device[, and enabling the server to/performs a step of] send[ing] a[n email] message to an email address associated with the account for the user as a result of the first further action.....124	
g.	Claim 34: The method of claim 1 wherein the first further action is related to either a product tied to a location or an advertisement tied to a location. 125	

TABLE OF CONTENTS
(continued)

	Page
B. Ground 2: Claims 2-10, 14, 16, 18-19, 22-28, 35, 37-44, 46, 48-49, 51-55, 57-60, 62, 66, 68, 72, 75-79, and 81-83 are obvious over Watanabe in view of Ribaud and Behrens.....	126
1. A POSITA would have been motivated to combine Watanabe-Ribaud's teachings with Behrens' teachings and would have had a reasonable expectation of success.....	127
2. Independent Claim 37	137
a. Element 37[pre]: A mobile wireless device comprising:	137
b. Element 37[a]: one or more radios for providing reception and transmission for each of a Bluetooth wireless protocol and a second wireless protocol;	137
c. Element 37[b]: one or more processors; and.....	138
d. Element 37[c]: 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:	139
e. Element 37[d]: receiving from a beacon transmitter, using the Bluetooth wireless protocol, a first plurality of beacon transmissions during a first time period, each of the beacon transmissions including (a) a MAC address, (b) a unique identifier, the unique identifier does not directly identify a location of the beacon transmitter, and (c) a beacon service identifier, wherein the beacon service identifier of each respective beacon transmission identifies that the unique identifier is relevant to stored information associated with a wireless beacon service, wherein the stored information is not otherwise accessible to the wireless device utilizing the Bluetooth wireless protocol;	142

TABLE OF CONTENTS
(continued)

	Page
f. Element 37[e]: receiving from one or more servers, using the second wireless protocol, stored information related to a entity or object associated with a first unique identifier;	145
g. Element 37[f]: selecting one or more unique identifiers from the first plurality of beacon transmissions, by filtering the beacon transmissions which include a particular beacon service identifier indicating that a particular received beacon transmission is associated with the particular wireless beacon service;	146
h. Element 37[g]: taking first further action relating to the stored information, if the first unique identifier is present among the selected one or more unique identifiers;	146
i. Element 37[h]: receiving, by the wireless device, using the Bluetooth wireless protocol, during a second time period, a second plurality of beacon transmissions, each of the second plurality of beacon transmissions comprising three fields (a) a MAC address, (b) a unique identifier, wherein the unique identifier of each respective beacon transmission does not directly identify a location of a beacon transmitter, and (c) the beacon service identifier, wherein the beacon service identifier of each respective beacon transmission identifies that the unique identifier is relevant to stored information associated with a wireless beacon service, wherein the stored information is not accessible to the wireless device utilizing the Bluetooth wireless protocol;	147

TABLE OF CONTENTS
(continued)

	Page
j. Element 37[i]: selecting one or more of the unique identifiers from the second plurality of beacon transmissions, by filtering the beacon transmissions which include the same particular beacon service identifier indicating that a particular received beacon transmission is associated with the same particular wireless beacon service;.....	150
k. Element 37[j]: taking second further action relating to the stored information, if a second unique identifier is present among the one or more unique identifiers selected from the second plurality of beacon transmissions, wherein the second unique identifier is associated with the same entity or object, and wherein the second unique identifier is not equal to the first unique identifier, and further wherein the received beacon transmissions including the first and second unique identifiers are received from a same transmitting device; and	151
l. Element 37[k]: wherein the MAC address received in a beacon transmission including the second unique identifier is different from the MAC address received in a beacon transmission including the first unique identifier, but each such beacon transmission includes the same particular beacon service identifier.....	154
3. Dependent Claims 2-10, 14, 16, 18-19, 22-28, 35, 38-44, 46, 48-49, 51-55, 57-60, 62, 66, 68, 72, 75-79, and 81-83....	157
a. Claims 2 and 51	157

TABLE OF CONTENTS
(continued)

Page

b.	Claims 3/52: The [method]/[computer program product] of claim [2]/[51] wherein the MAC address received in a beacon transmission including the second unique identifier is different from the MAC address received in a beacon transmission including the first unique identifier, but each such beacon transmission includes the same particular beacon service identifier, and wherein a plurality of beacon transmissions including the particular [beacon] service identifier and the first unique identifier are received in the first time period, and no beacon transmissions including the same [particular] service identifier and the second unique identifier are received in the first time period.....	159
c.	Claims 4/40/53: The [method]/[mobile wireless device]/[computer program product] of claim [3]/[37]/[52] wherein the second further action is based upon a function currently being performed on a device associated with the wireless beacon service.	161
d.	Claims 5/41/54: The [method]/[mobile wireless device]/[computer program product] of claim [4]/[40]/[53] wherein the function is related to a current phone call, music being played, a video being played, a multi-player game, or a shared application.....	162
e.	Claims 6/55: The [method]/[computer program product] of claim [2]/[51] wherein the first or the second further action is [additionally] related to receiving advertising information for presentation to a user of the wireless device, based upon the first or the second unique identifier, or information derived from the first or second unique identifier.	163

TABLE OF CONTENTS
(continued)

Page

f.	Claims 7/42/57: The [method]/[mobile wireless device]/[computer program product] of claim [2]/[37]/[51] wherein one or more of the first further action and the second further action [additionally] includes [causing the wireless device to] receiv[ing]/[e] content from a server based upon information derived from either the first unique identifier or the second unique identifier.....	164
g.	Claims 8/43/59: The [method]/[mobile wireless device]/[computer program product] of claim [2]/[37]/[51], wherein the first or second further action [additionally] includes [sending a message] [or] [causing a server to send a message]/[causing the wireless device to send a message] to another device associated with an account related to the first and the second unique identifiers[, or information derived from the first or the second unique identifiers].....	164
h.	Claim 9: The method of claim 2 wherein following the taking of the first or second further action, a server associated with an account for a user of the wireless device performs a step of sending an email message to an email address associated with the account for the user, the email message relating to the particular entity or object.....	166
i.	Claims 10/44/62: The [method]/[mobile wireless device]/[computer program product] of claim [2]/[37]/[51] wherein the second further action [additionally] includes [causing the wireless device to] prevent[ing] sending of the second unique identifier or information derived from the second unique identifier by the [mobile] wireless device to at least one of the one or more servers.	166

TABLE OF CONTENTS
(continued)

	Page
j. Claims 14/66: The [method]/[computer program product] of claim [2]/[51] wherein the [computer program instructions, when executed by the one or more processors in the wireless device, further cause the wireless device to: receive] stored information [is received] at the wireless device from at least one of the one or more servers prior to performing one or more of the first and the second further action.	167
k. Claims 16/68: The [method]/[computer program product] of claim [2]/[51] wherein all beacon transmitter devices participating in the particular wireless beacon service have the same particular beacon service identifier.	168
l. Claim 18: The method of claim 2 wherein the steps performed at the wireless device are performed as a result of an application program executing on the wireless device.	168
m. Claims 19/72: The [method]/[computer program product] of claim [2]/[51] wherein the second further action is [additionally] related to either a product tied to a location or an advertisement tied to a location.	169
n. Claims 22/48/75: The [method]/[mobile wireless device]/[computer program product] of claim [2]/[37]/[51] wherein the second further action [additionally] includes [causing the wireless device to] allow[ing] a user associated with the [mobile] wireless device to [be provided] access to an object or device associated with the wireless beacon service.	169

TABLE OF CONTENTS
(continued)

Page

o.	Claims 23/35/49/76: The [method]/[mobile wireless device]/[computer program product] of claim [2]/[3]/[37]/[51] wherein the [taking]/[first or] second further action additionally comprises: controlling further communications between the [mobile] wireless device and at least one device or server associated with an entity or object in proximity to the wireless device [based upon information derived from the first or second unique identifier].	170
p.	Claims 24/82/77: The [method]/[mobile wireless device]/[computer program product] of claim [3]/[37]/[52] [further comprising:]/[wherein the operations further comprise]/[wherein the computer program instructions, when executed by the wireless device, further cause the wireless device to:] receiv[ing]/[e], at the [mobile] wireless device, timing notification information for coordination of active times for beacon transmissions.....	171
q.	Claims 25/83/78: The [method]/[computer program product] of claim [24]/[53]/[77] wherein the [receiving, at the wireless device of the] timing notification information is not [received] directly from the beacon transmitter.....	172

TABLE OF CONTENTS
(continued)

Page

r.	Claims 26/38/79: The [method]/[mobile wireless device]/[computer program product] of claim [2]/[37]/[51] [further comprising:]/[wherein the operations further comprise]/[wherein the computer program instructions, when executed by the wireless device, further cause the wireless device to:] us[ing]/[e] the stored information to determine if the second unique identifier is present among the selected one or more of the unique identifiers from the second plurality of beacon transmissions.....	173
s.	Claims 27/39/81: The [method]/[mobile wireless device]/[computer program product] of claim [1]/[37]/[50] wherein [the]/[each] MAC address [or a respective beacon transmission] is a randomly generated 48 bit number matching a format of a Bluetooth BD_ADDR.....	173
t.	Claim 28: The method of claim 3 wherein the short range protocol is derived from Bluetooth.....	175
u.	Claim 46: The mobile wireless device of claim 37 wherein the operations further comprise: using the stored information to determine if the first unique identifier is present among the first selected one or more unique identifiers.	176
v.	Claim 58: The computer program product of claim 52 wherein the first further action additionally includes causing the wireless device to receive content from a server based upon information derived from the first unique identifier.	176

TABLE OF CONTENTS
(continued)

	Page
w. Claim 60: The computer program product of claim 51, wherein the computer program instructions, when executed by the one or more processors in the wireless device, further cause the wireless device to: after the first or second further action: send information to a server associated with an account for a user of the wireless device, to enable the server to send a message to an email address associated with the account for the user.	176
XII. CONCLUSION.....	177

LIST OF EXHIBITS

Ex. No.	Description
Ex-1001	U.S. Patent No. 11,687,971 (“the ’971 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. 11,687,971
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
Ex-1016	INTENTIONALLY LEFT BLANK
Ex-1017	INTENTIONALLY LEFT BLANK

Ex. No.	Description
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) (“Bluetooth Specification v.2.0 + EDR”)
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 802.15 Specification IEEE Standard 802.15.1, Part 15.1: Wireless medium access control and physical layer (PHY) specifications for wireless personal area networks (WPANs) (June 2005) (“Bluetooth Specification”)
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-1033	US Patent Publication No. 2003/0220114 to Langensteiner et al. (“Langensteiner”)

Ex. No.	Description
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) (Mar. 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-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 1-10, 12-16, 18-19, 22-31, 34-44, 46, 48-62, 64-68, 72, and 75-83 of U.S. Patent No. 11,687,971 (“the ’971 Patent”) (Ex-1001), which I understand is currently assigned to Secure Communication Technologies, LLC (“PO”).¹ 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

¹ Where appropriate, I refer to exhibits that I understand are attached to the petition for IPR of the ’971 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 '971 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 '971 Patent.

III. INFORMATION CONSIDERED

15. In preparation for my Declaration, I have considered the materials I discuss in my Declaration, including, for example, the '971 Patent, the references cited by the '971 Patent, the prosecution history of the '971 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 '971 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 '971

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 '971 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 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 '971 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 1-10, 12-16, 18-19, 22-31, 34-44, 46, 48-62, 64-68, 72, and 75-83 of the '971 Patent would have been obvious under 35 U.S.C. §103 on the following grounds:

- **Ground 1:** Claims 1, 12-13, 15, 29-31, 34, 36, 50, 56, 61, 64-65, 67, and 80 are obvious over JP Patent Publication No. 2005/12973 to Watanabe (“Watanabe”) (Ex-1005, Ex-1006) in view of U.S. Patent Publication No. 2007/0030824 to Ribauda (“Ribauda”) (Ex-1007);
- **Ground 2:** Claims 2-10, 14, 16, 18-19, 22-28, 35, 37-44, 46, 48-49, 51-55, 57-60, 62, 66, 68, 72, 75-79, and 81-83 are obvious over Watanabe in view of Ribauda and PCT Patent Publication No. WO2008/132241 to Behrens (“Behrens”) (Ex-1008).

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.

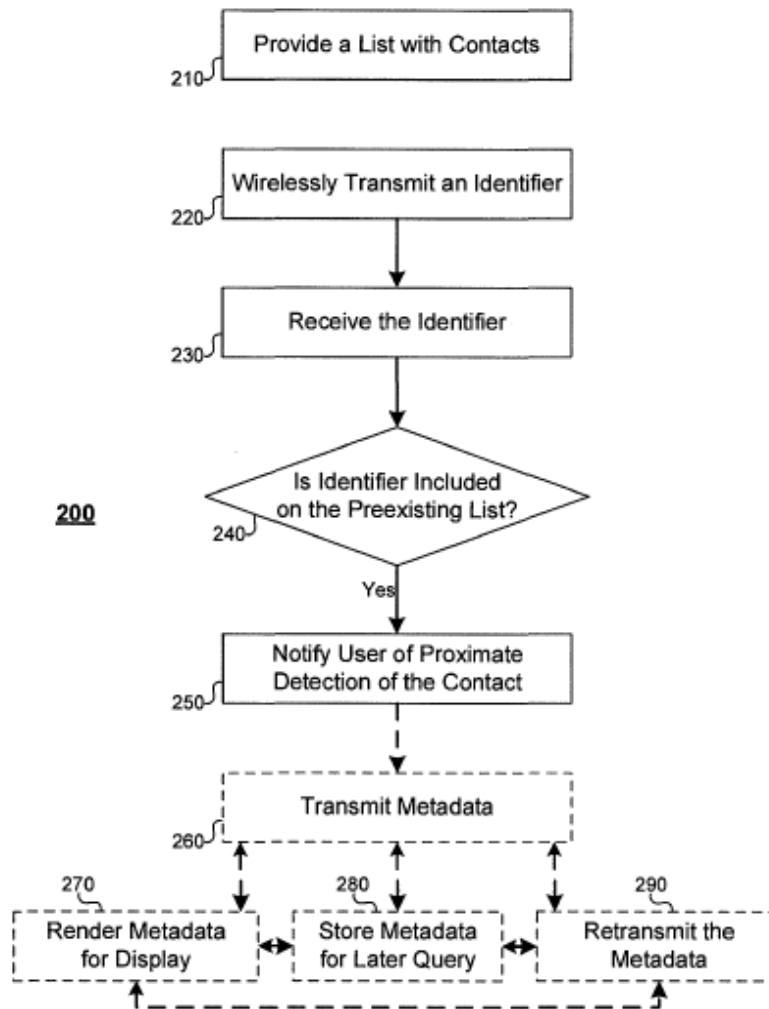


Fig. 2

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.”); US2005/0174975 to Mgrdechian (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 (Godfrey) ¶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. US2005/0174975 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) (June 2005)) (“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.

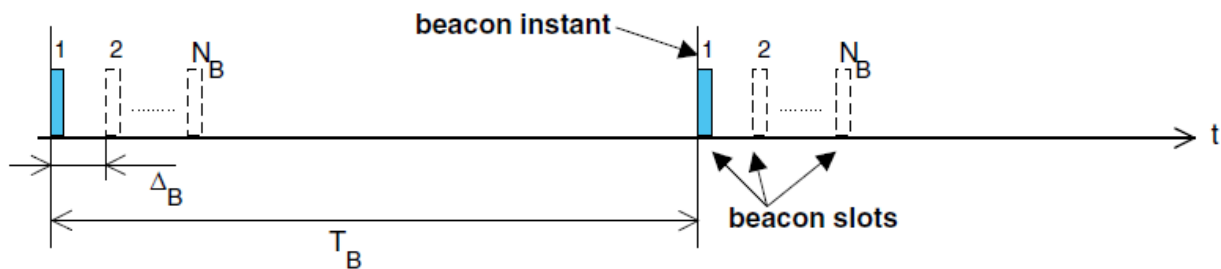


Figure 72—General beacon train format

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 (June 2007)) (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.

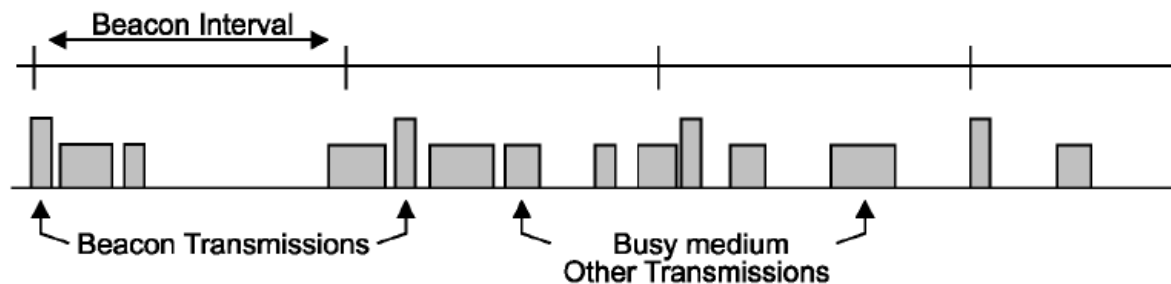


Figure 11-1—Beacon transmission on a busy network

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), 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 is in 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.

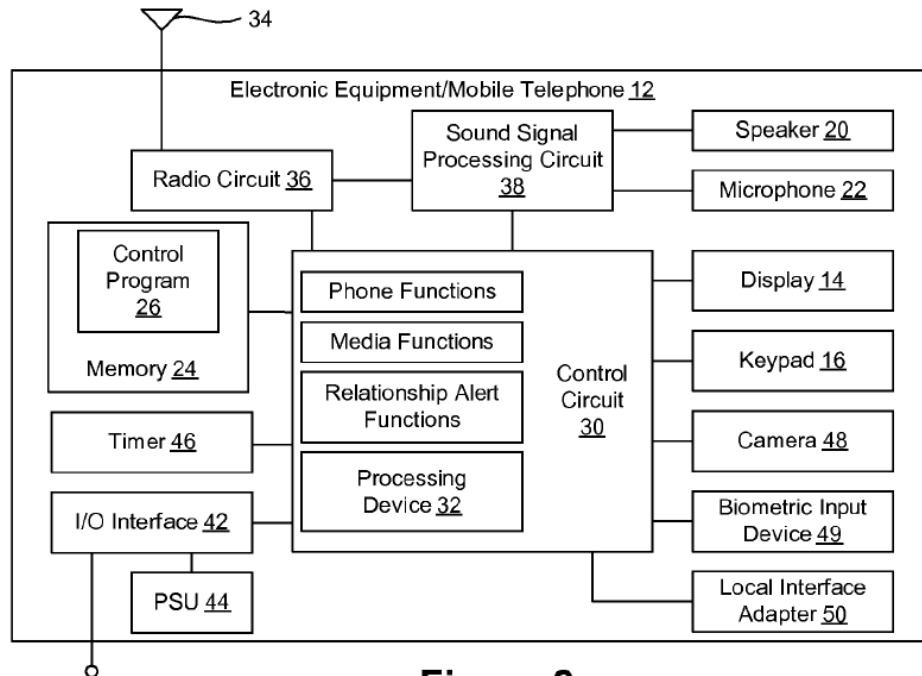


Figure 2

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 ’971 PATENT AND ITS FILE HISTORY

64. The ’971 Patent relates to techniques for mobile wireless devices (e.g., cellular phones) in proximity with one another to exchange information utilizing both a short range, first wireless capability and a second wireless capability that allows the devices “to communicate with a central server via the Internet.” Ex-1001, 1:49-63. The ’971 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, 1:11-36. The

'971 Patent proposes combining these two wireless capabilities to broker the exchange of information between two wireless devices. *Id.*, 1:51-56.

65. As shown in Figure 1 below,² “a central server 100 [red] is connected to devices 106 and 108” (blue) through “wide area wireless links 104 and 103 respectively” (green), via a combination of the Internet and a cellular network. Ex-1001, 3:44-55, Fig. 1 (annotated). The devices are also able to communicate directly with each other via “a short range wireless link 107” (yellow). *Id.*, 4:36-47.

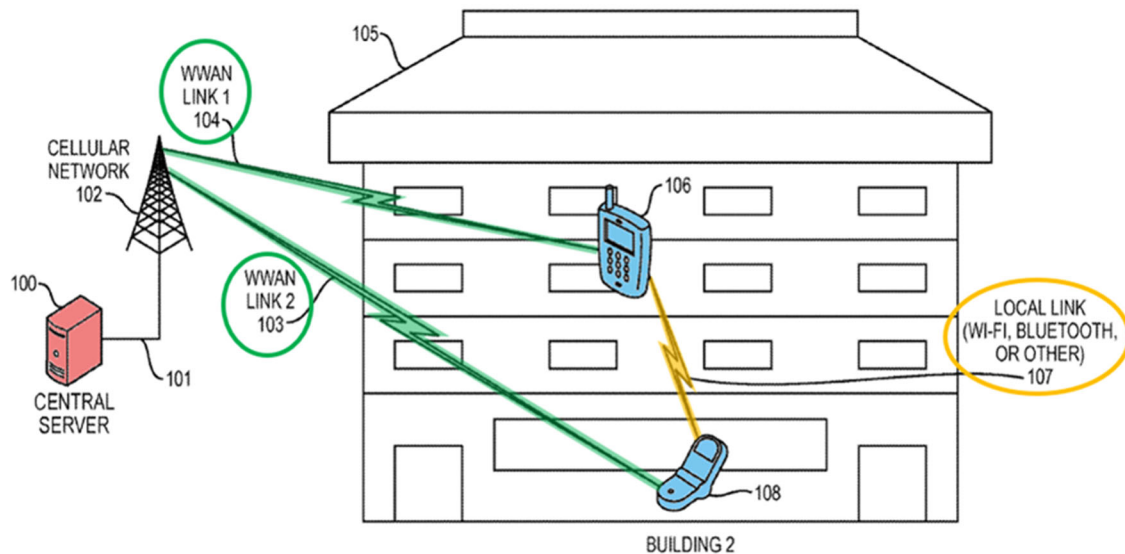


Figure 1

66. The '971 Patent uses the concept of “beacon service” transmissions to facilitate communications between nearby devices over the short range link first, before establishing communications using a long range, cellular link. Ex-1001, 1:49-

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

67. As shown in Figure 6 below, the beacon transmissions include MAC address, the basic service set identifier (BSSID), and ad-hoc network name (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.*, 8:25-38, Fig. 6 (annotated).

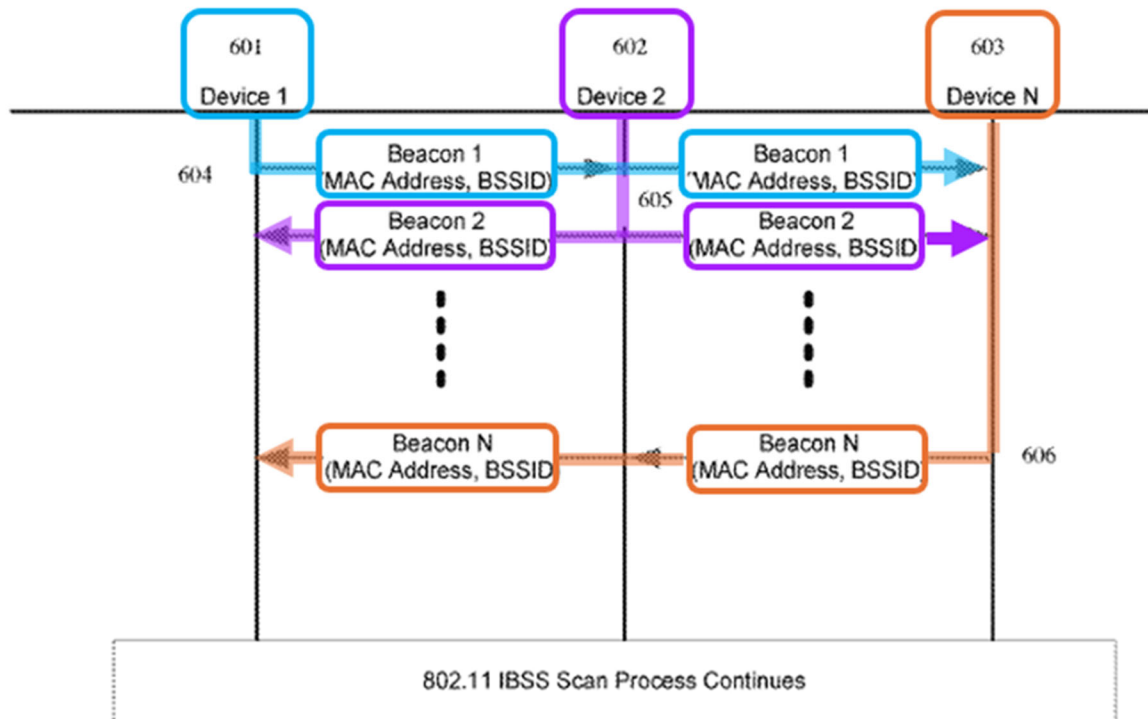


Figure 6 - 802.11 IBSS Beacon Process

67. The '971 Patent was filed September 12, 2022, as a continuation of a series of patents, the earliest of which was filed on February 3, 2009. The '971 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. On November 16, 2022, Applicant filed a Preliminary Amendment that

canceled then-pending claims 1-30 and added claims 31-113. Ex-1004, 93-116.

Applicant stated that the “claims presented here are similar to those that were allowed in U.S. Patent Application 17/366,826 (now issued as US Patent 11,443,344) to which this application claims priority. The difference with the claims in the present case is in the recitation of the ‘unique identifier’. In this case the ‘unique identifier’ is both ‘relevant to stored information associated with a wireless beacon service’ and ‘not otherwise accessible to the wireless device using the short range wireless protocol.’” Ex-1004, 113. Applicant further argued that “[e]xample embodiments also describe that the ‘stored information’ is not accessible using the short range wireless protocol, and instead being provided via the broadcast only beacon transmitters.” Ex-1004, 114. On April 24, 2023, the Examiner issued a Notice of Allowance without making any prior art rejections during prosecution. Ex-1004, 502-508. The Examiner stated that the reason for allowance is because “[t]he prior art fail to show a beacon service identifier wherein the beacon service identifier of each respective beacon transmission identifies that the unique identifier is relevant to stored information associated with a wireless beacon service, wherein the stored information is not otherwise accessible to the wireless device utilizing the short range wireless protocol, in combination with the other limitations in the independent claims.” Ex-1004, 507.

69. For the reasons I discuss below, the prior art teaches the claimed

method and apparatus for detecting nearby wireless devices and establishing communications and renders the challenged claims unpatentable. Accordingly, it is my opinion that Claims 1-10, 12-16, 18-19, 22-31, 34-44, 46, 48-62, 64-68, 72, and 75-83 of the '971 Patent are invalid as obvious over the prior art.

70. I understand from Counsel that all prior art references I discuss in my Declaration are prior art.

IX. CLAIM CONSTRUCTION

71. For the purposes of my Declaration, I do not believe that any term requires explicit construction to resolve the issues I present in my Declaration.

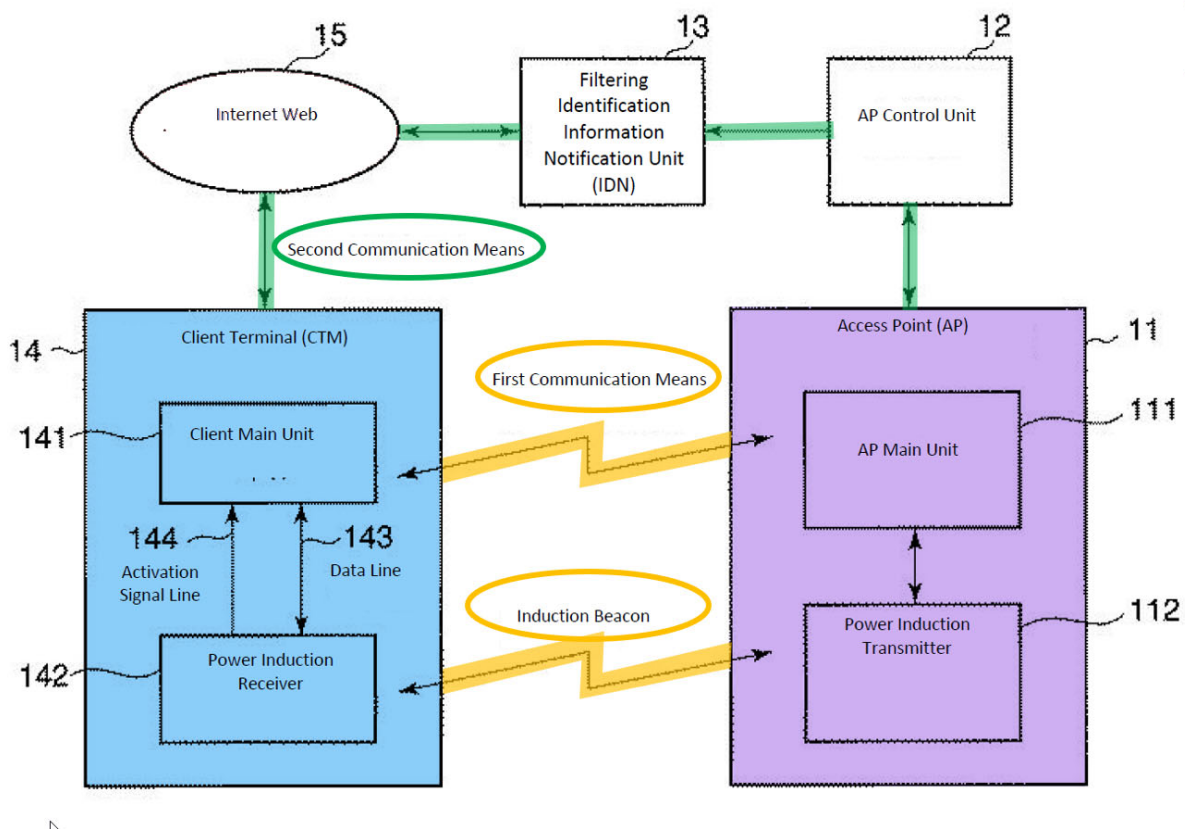
X. OVERVIEW OF THE APPLIED PRIOR ART REFERENCES

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

72. 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 '971 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.

73. 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.

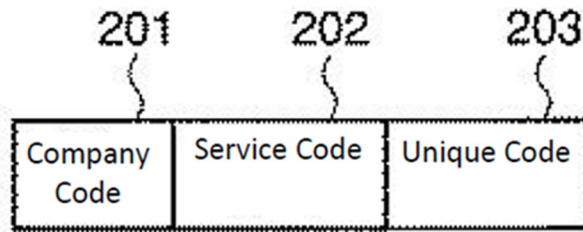
1 (annotated). “Each of the access points 11 has an AP main unit ... 111 as a first communication means” (yellow) “for [short or medium-distance] wireless communication (data communication) with the client terminal 14” (i.e., mobile device). Ex-1006 ¶¶14, 27. Client terminal 14 also has a “second communication means” (green) “for communicating, through the internet 15.” Ex-1006 ¶26.



74. 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

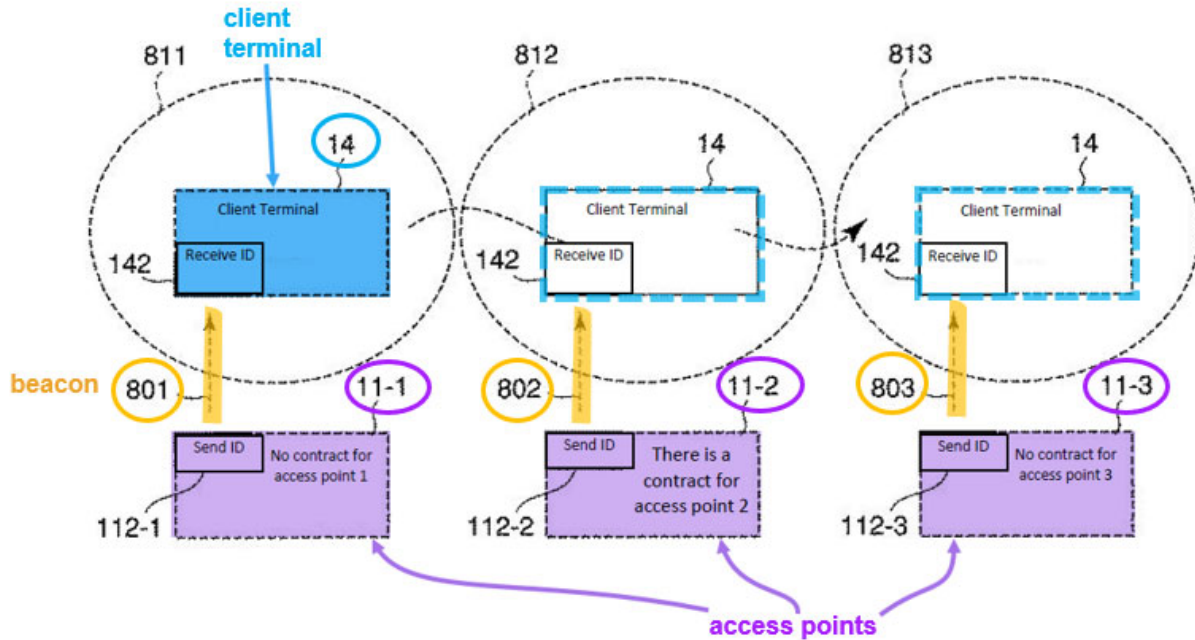
provided via that access point,” and “a unique code 203 unique to that power induction transmitter.” *Id.*, ¶15, Fig. 2.

[FIG. 2]



75. “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.

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



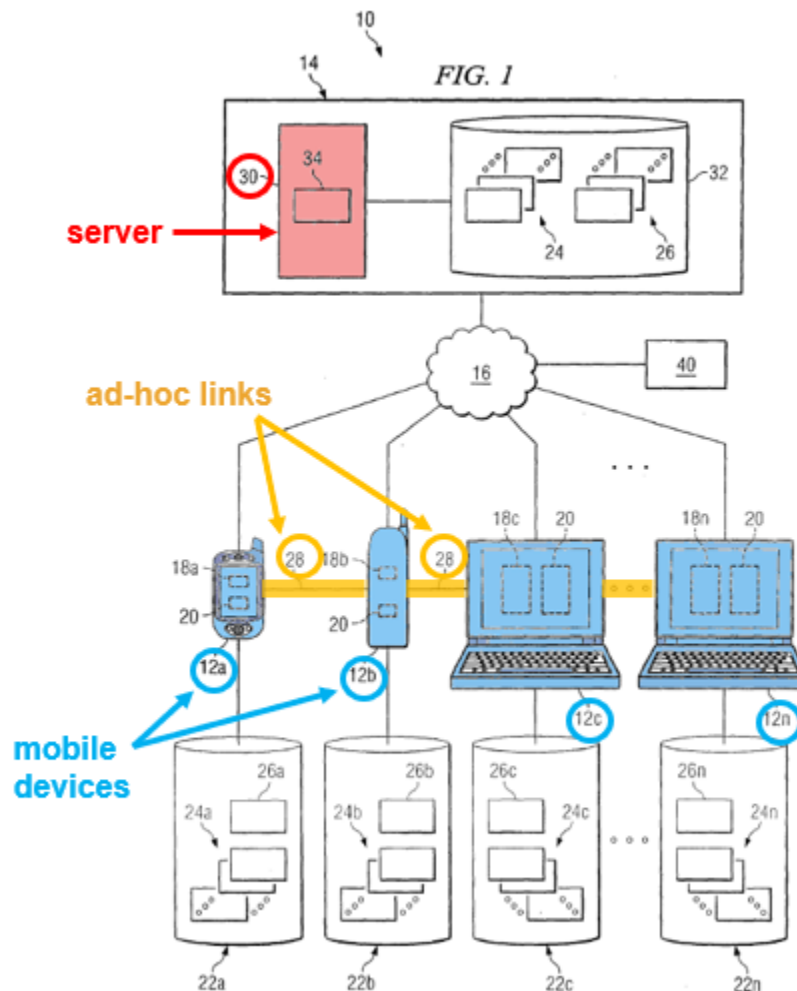
B. Ribaldo (Ex-1007)

77. Ribaldo (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 Ribaldo is §102(b) prior art to the ’971 Patent.

78. Ribaldo 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.

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



80. 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.

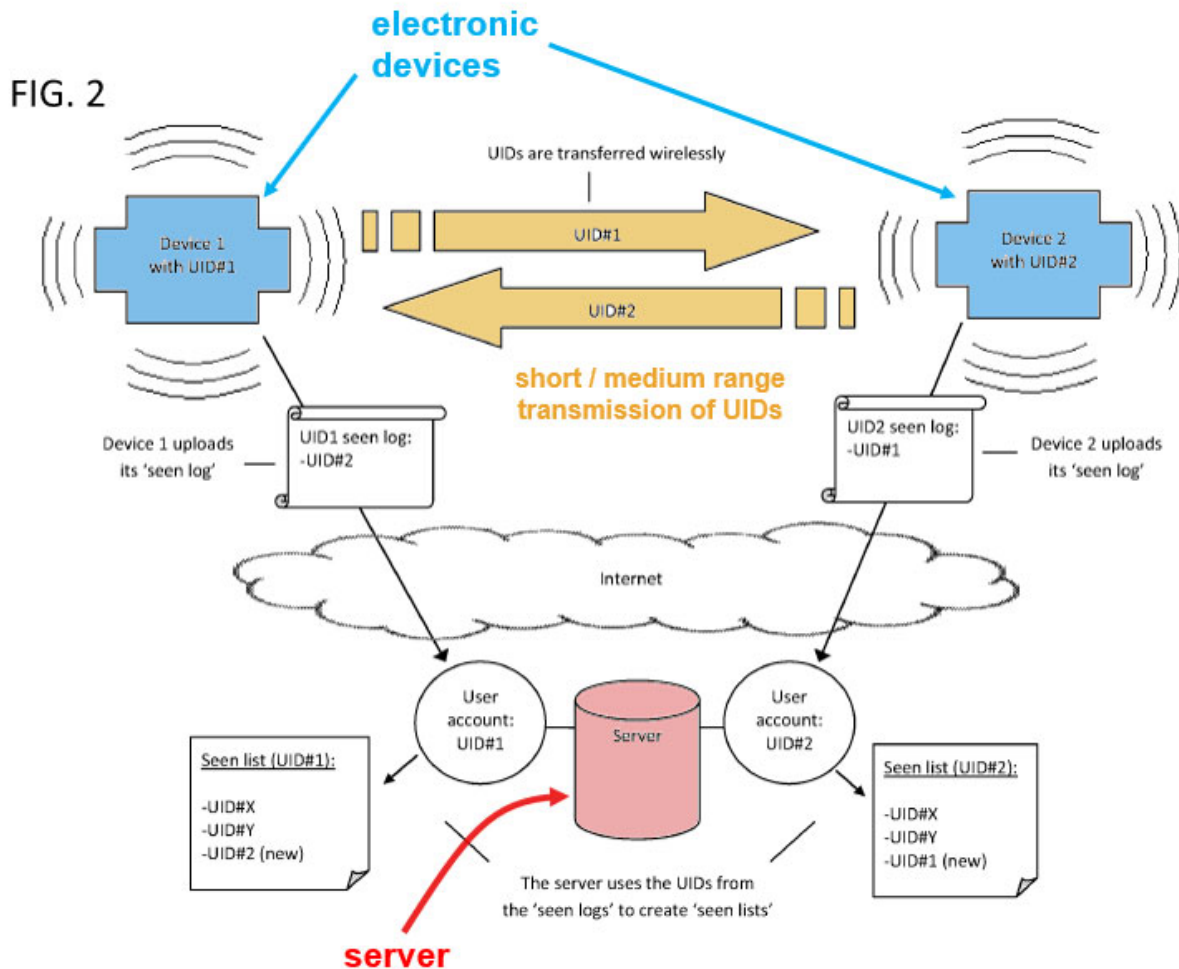
C. Behrens (Ex-1008)

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 and published on November 6, 2008. I understand from Counsel that Behrens is §102(e) prior art to the ’971 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.



XI. DETAILED EXPLANATION OF THE UNPATENTABILITY GROUNDS

A. Ground 1: Claims 1, 12-13, 15, 29-31, 34, 36, 50, 56, 61, 64-65, 67, and 80 are obvious over Watanabe in view of Ribaudó.

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

84. In addition to the reasons set forth below, a POSITA would have been motivated to combine the teachings of Watanabe and Ribaudó and had a reasonable expectation of success in doing so because each relates to detecting nearby wireless devices and establishing communications using both ad-hoc (e.g., WiFi or Bluetooth) and cellular network. Ex-1006, Abstract; Ex-1007, Abstract, ¶18.

85. Watanabe teaches that “access points 11-1, 11-2, and 11-3 either continuously or periodically transmit induction beacons 801, 802, and 803.” Ex-1006 ¶49. The beacons are transmitted using Bluetooth. Ex-1006 ¶¶14, 27. The induction beacons include “a company code that indicates the service provider that has installed and controls the access point 11, a service code that indicates the types of services provided by the access point 11, and a unique code that is unique to the power induction transmitter 112 of that access point 11.” Ex-1006 ¶49. Watanabe further teaches that “the transmitter identification information may have a field for embedding information other than the information set forth above.” Ex-1006 ¶19.

86. Watanabe also includes various teachings related to a MAC address.³

³ For example, “Each AP control unit 12 associates, and controls the storing of,

And a POSITA would have been motivated to include the MAC address in the transmitter identification information in the transmitter identification information in Watanabe's beacon transmission in light of Ribaud. Ribaud teaches a wireless communication system in which nearby devices transmit beacons to each other. Ex-1007 ¶6. Ribaud further teaches that its devices "may beacon data such as the client ID of the user" (Ex-1007 ¶57) and an SSID of a wireless network (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. This would have been motivated by, for example, a POSITA's desire to comply with the Bluetooth standard, which states that each Bluetooth address (i.e., BD_ADDR) is created in accordance with the IEEE standard for MAC addresses. Ex-1021 (Bluetooth Specification v2.0 + EDR), 66 ("Each Bluetooth device shall be allocated a unique 48-bit Bluetooth device address (BD_ADDR)," which "shall be obtained from the IEEE Registration Authority."), 185 ("BD_ADDR is the address used by a Bluetooth device as defined in [1]. It is received from a remote device during the device discovery procedure."), 773 ("The Bluetooth device address (BD_ADDR) is the 48-bit address. The BD_ADDR can be obtained via user interactions, or, automatically, via an inquiry routine by a device."); *see also* Ex-1043 (IEEE 802

individual identifiers, *such as MAC addresses*, or the like, that are assigned to each of the associated access points 11." Ex-1006 ¶22.

2002), 20-21 (describing the “standard representation of a 48-bit LAN MAC address”); Ex-1026 (Bluetooth Specification), 5 (“3.9 Bluetooth device address (BD_ADDR): The address used to identify a device conforming to this Standard.”), 54-55 (“Each IEEE 802.15.1-2005 device shall be allocated a unique 48-bit device address (BD_ADDR). This address shall be obtained from the IEEE Registration Authority.”). Moreover, a POSITA would have been aware that Bluetooth systems broadcast the MAC address. For example, the ’971 Patent itself acknowledges that “the MAC address is always broadcast in any operation of a Bluetooth or Wi-Fi link” to “provide for an additional level of security for the device.” Ex-1001, 8:42-46. Thus, a POSITA would have understood that Watanabe’s broadcast message over Bluetooth should include a MAC address that complies with the Bluetooth standard, consistent with the express teachings of Ribaud. And particularly in light of Watanabe’s teaching that additional fields for embedding information other than the information disclosed may be included in the transmitter identification information. Ex-1006 ¶19.

87. A POSITA would also have been motivated to include Watanabe’s MAC address in the induction beacon, as taught by Ribaud, because a MAC address was a well-known identifier assigned to a network interface controller for use as a network address in wireless communication systems by 2008. Indeed, MAC addresses have long been used in various wireless networking technologies and are

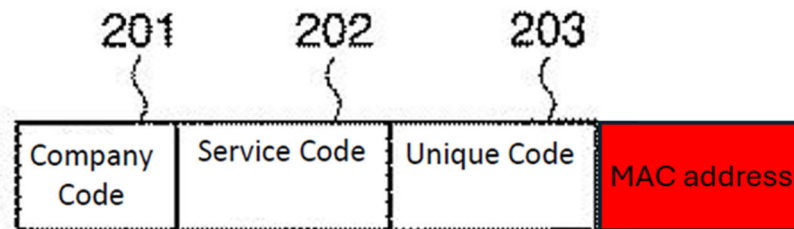
crucial for network communications. For example, the 802.11g-2003 beacon frame has a “source address” which is the MAC address of the transmitting access point. Ex-1044 at 11. Similarly, in the 802.15.4-2003 standard for Bluetooth, the beacon frames include MAC addressing fields (*see*, for example, Section 5.4.3.1). Ex-1045, 21. These MAC addressing fields contain a source address (*see*, for example, Section 7.2.1 (Ex-1045, 112-120)), that can be the 8-byte extended address, which is generally a unique MAC address assigned in manufacturing. Watanabe explicitly discusses using such common identifying mechanisms. For example, Watanabe states: “For example, as shown in FIG. 2, the transmitter identification information is assigned ... a unique code 203 unique to that power induction transmitter 112. ... The unique code 203 can also be used to identify the access point 11 individually. This field structure of the transmitter identification information is a common structure used when utilizing various types of internet services. Ex-1006 ¶15.

88. Moreover, as I explained in the Technological Background section of my Declaration, 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). Additionally, as I explained in the Technological Background section of my Declaration, including identifiers such as MAC addresses in beacon transmissions was known. *See, e.g.*, Section VII.C (citing, e.g., Ex-1009 (Krikorian), Abstract, ¶¶4-5, 8, 22; Ex-1027 (Lazaridis), Abstract, 1:16-20, 2:37-45, 7:65-8:14; Ex-1010 (Mgrdechian) ¶¶13-14, 26-28, 42; Ex-1037 (Suzuki) ¶¶59, 63, 66, 68-70, 77-79, 83, Figs. 6-7, 9-11).

89. In the Watanabe-Ribaudo combination, the beacon would thus have at least the following elements, shown in Figure 2' below (Watanabe's beacon message as modified by Ribaudo's teaching to include a MAC address (red)):

[FIG. 2']



Moreover, Ribaudo specifically teaches that including a MAC address in the beacon has certain benefits, such as, for example, “shield[ing] the true identity of the user, for privacy purposes.” Ex-1007 ¶¶46, 68. Thus, a POSITA would have been motivated to include Watanabe's MAC address in the induction beacon with the company code, service code, and unique code to identify and facilitate communication with the proper access point to achieve these security benefits.

90. A POSITA would have had a reasonable expectation of success in combining the teachings of Watanabe and Ribaud. Both describe receiving beacon transmissions comprising identification information associated with a nearby access point (or other device) at a mobile device using Bluetooth, receiving stored information relating to an entity associated with the identification information from a server using the Internet, comparing the beacons identification information to preset identification information stored at the mobile device to determine if it matches, and taking further action relating to the stored information (such as activating the device or connecting with the other device to communicate) if it matches. 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 well-understood and predictable combinations.

2. Independent Claims 1 and 50⁴

a. Element 1[pre]: A method comprising:

Element 50[pre]: A computer program product for installation in a non-volatile memory in a wireless device, the computer program product comprising computer program instructions that, when read from

⁴ Independent Claims 1, 37, and 50 contain substantially similar limitations with Claim 37 adding additional limitations, as discussed in Ground 2. Substantially similar claim elements are discussed together in the below element-by-element analysis. *See* Ex-1020. Any meaningful differences between the claims or elements are individually identified and discussed.

the non-volatile memory, and then executed by one or more processors in the wireless device, cause the wireless device to:

91. In my opinion, Watanabe in view of Ribaudó (“Watanabe-Ribaudó”) teaches⁵ the preamble, to the extent it is limiting. Both teach wireless devices configured to communicate with other devices in proximity. For example, Watanabe’s Figures 7-8 depict “a sequence diagram for explaining the operation of the client terminal” of Watanabe’s wireless communication system. Ex-1006 ¶63. And Ribaudó teaches mobile devices 12 that “each have an associated memory module 22,” which includes “any suitable memory, database, or other data storage arrangement” (Ex-1007 ¶32), wherein “each include any suitable combination of hardware, software, and firmware to provide the functionality described” including “one or more applications 20 that are based on one or more programming languages” to “facilitate communication with other mobile devices 12” and the data center. Ex-1007 ¶19. A POSITA would have understood the memory to be non-volatile memory so that software or firmware program instructions are not lost when the device loses power.

92. Moreover, as I explained in the Technological Background section of my Declaration, using a processor and memory with instructions to execute

⁵ 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.

functions on mobile devices was known by 2008. *See, e.g.*, Section VII.I (citing, e.g., Ex-1009 (Krikorian) ¶¶6, 30-32; Ex-1028 (Gulin), ¶¶29, 79-80, Fig. 2; Ex-1029 (Kondou) ¶¶23, 29).

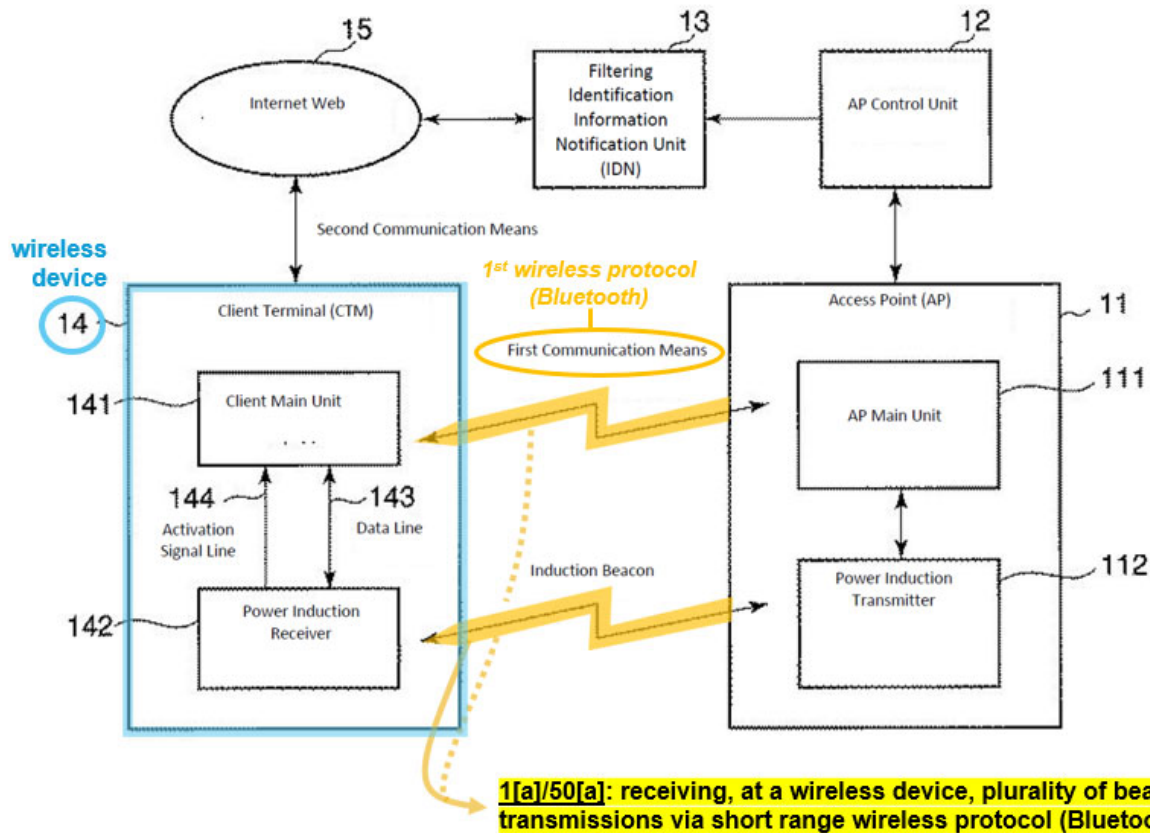
- b. **Elements 1[a]/50[a]: [receiving, at a wireless device,]/[process a first plurality of beacon transmissions, received at the wireless device] via a [short range]/[Bluetooth] wireless protocol, [a first plurality of beacon transmissions,] each beacon transmission comprising three fields (a) a MAC address, (b) a unique identifier, wherein the unique identifier of each respective beacon transmission does not directly identify a location of a beacon transmitter, and (c) a beacon service identifier, wherein the beacon service identifier of each respective beacon transmission identifies that the unique identifier is relevant to stored information associated with a wireless beacon service, wherein the stored information is not otherwise accessible to the wireless device utilizing the [short range]/[Bluetooth] wireless protocol;**

93. In my opinion, Watanabe-Ribaudo teaches Elements 1[a]/50[a].

(1) Receiving at a wireless device a first plurality of beacon transmissions via Bluetooth

94. Watanabe teaches that “[e]ach of the access points 11 has an AP main unit (AP-side data communication unit) 111 as a first communication means for wireless communication (data communication) with the client terminal 14.” Ex-1006 ¶14. Client terminal 14 is a “wireless device.” The first communication means includes “short- and medium-distance wireless communication devices,” such as “*wireless communication devices based on Bluetooth.*” Ex-1006 ¶27. Watanabe

further teaches that “power induction transmitters 112-1, 112-2, and 112-3 of access points 11-1, 11-2, and 11-3 either *continuously or periodically transmit induction beacons* 801, 802, and 803 to provide a power supply to the client terminal 14 at locations within the areas that are covered by each.” Ex-1006 ¶49. As shown in annotated Figure 1 below, client terminal 14 “has a power induction receiver 142 that is started up by *receiving a beacon* from” the power induction transmitters. Ex-1006 ¶26, Fig. 1.



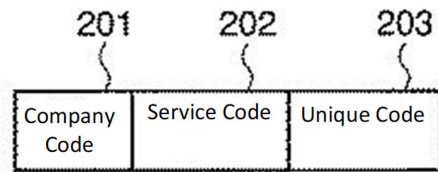
95. Watanabe further teaches that “each induction beacon includes ... a unique code that is unique to the power induction transmitter 112 of that access point

11.” Ex-1006 ¶49. For example, “the identification information ‘C1:S1:U1’ is included in the induction beacon sent from access point 11-1.” When client terminal 14 enters area 811, for example, which is covered by access points 11-1, power induction receiver 142 receives induction beacon 801 and compares the transmitter identification information such as “C1:S1:U1” included therein, respectively, to the filtering identification information. Ex-1006 ¶¶51-52. Induction beacon 801, which is continuously or periodically transmitted, corresponds to the recited “first plurality of beacon transmissions.” Client terminal 14 is thus a wireless device that receives Bluetooth beacon transmissions.

(2) Each beacon transmission includes: a MAC address

96. Watanabe teaches that “[e]ach AP control unit 12 associates, and controls the storing of, individual identifiers, such as MAC addresses, or the like, that are assigned to each of the associated access points 11.” Ex-1006 ¶22. Watanabe further teaches that the transmitter identification information provided in the beacon transmissions includes a number of identifiers, as shown in Figure 2 below. Ex-1006 ¶15, Fig. 2.

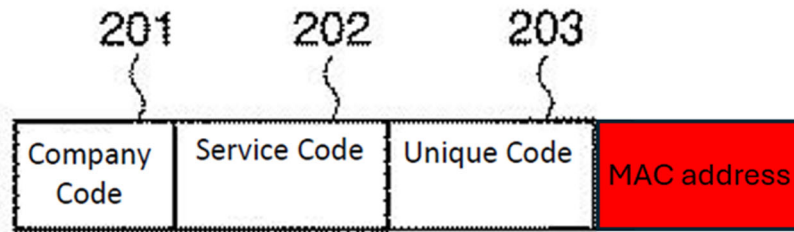
[FIG. 2]



97. As discussed above in Section XI.A.1, a POSITA would have been motivated to add the MAC address to the transmitter identification information in light of Ribaudó's disclosure that the "unique MAC address of mobile device 12a may be beacons when the BLUETOOTH interface of mobile device 12a is active." Ex-1007 ¶157. And as explained in Section XI.A.1, Ribaudó teaches that including a MAC address in the beacon transmission has certain benefits, such as for example, "shield[ing] the true identity of the user, for privacy purposes." Ex-1007 ¶¶46, 68. Indeed, the '971 Patent itself acknowledges that "the MAC address is always broadcast in any operation of a Bluetooth or Wi-Fi link" to "provide for an additional level of security for the device." Ex-1001, 8:42-46.

98. In the Watanabe-Ribaudó combination, the beacon would thus have at least the following elements, shown in Figure 2' below (Watanabe's beacon message as modified by Ribaudó's teaching to include a MAC address):

[FIG. 2']

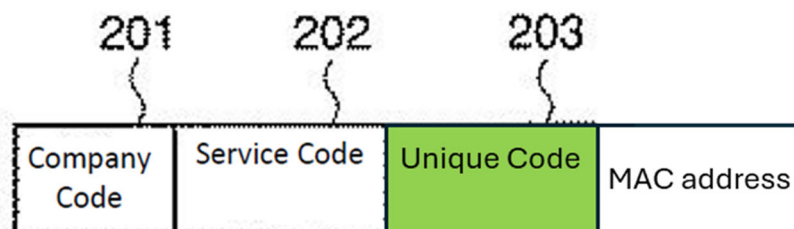


And the transmitter identification information provided in Watanabe's beacon transmissions would include a MAC address code along with the other identifier codes. For example, the transmitter identification information would include "C1:S1:U1[:M1]," where M1 is the code for the MAC address.

(3) Unique identifier

99. Watanabe teaches that the transmitter identification information provided in the beacon transmissions also includes "a unique code 203 unique to that power induction transmitter 112," which "can also be used to identify the access point 11 individually." Ex-1006 ¶15, Fig. 2 (above). In the Watanabe-Ribaudo combination, the unique identifier is shown in Figure 2' below (green):

[FIG. 2']



100. Unique code 203 corresponds to the recited “unique identifier” because it is unique to the power induction transmitter (i.e., beacon transmitter) and may identify the access point, but does not directly identify a location of the transmitter. The ’971 Patent specification does not describe what “does not directly identify a location of a beacon transmitter” means in terms of the unique identifier—this phrase only appears in the claims. *Id.* But Watanabe explains that “a unique code 203 [is] unique to that power induction transmitter.” Ex-1006 ¶15. For example, unique code U1 is beaconsed by the power induction transmitter for access point 11-1. U1 is thus unique to the power induction transmitter by naming convention (U1 corresponds to 11-1, etc.). Other than this naming convention, Watanabe does not suggest, nor would it have made sense to a POSITA, that the unique codes contain any additional information that would directly identify a location of a beacon transmitter such as if the AP is relocated but still uses unique code U1. Indeed, unique codes, such as, for example, MAC addresses, are typically set at the time of manufacturing and remain constant independent of the location of the device.

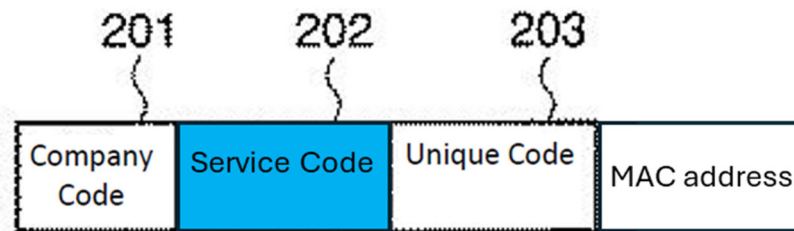
(4) Beacon service identifier

(a) Identifies the unique identifier is relevant to stored information associated with a wireless beacon service

101. Watanabe teaches that the transmitter identification information provided in the beacon transmissions also includes “[a] service code 202 indicating

the type of service that can be provided via that access point 11.” Ex-1006 ¶15, Fig. 2 (above). In the Watanabe-Ribaudo combination, the beacon service identifier is shown in Figure 2’ below (blue):

[FIG. 2’]



102. Watanabe’s service code 202 corresponds to the recited “beacon service identifier” because it identifies that the unique identifier is relevant to stored information associated with a wireless beacon service. For example, Watanabe explains that its “service code” is “indicating the type of service that can be provided via that access point 11.” Ex-1006 ¶15. Moreover, AP control units 12 “*stores and controls, in mutual association, the transmitter identification information and AP identifier* [i.e., unique identifier] that are included therein.” Ex-1006 ¶31. As Watanabe explains, the service code thus indicates that the unique identifier is relevant to stored information associated with the available services.

(b) **Stored information is not otherwise accessible utilizing Bluetooth**

103. The ’971 Patent specification does not describe what “the stored information is not otherwise accessible to the wireless device” means in terms of the

beacon service identifier—this phrase only appears in the claims. *Id.* But Watanabe teaches that “a group ID is set to the access point on the basis of a service provider with a relationship to that access point, and a field for representing the group ID is provided in the transmitter identification information so that *data communication can be carried out with only the access point with a relationship to a specific service provider.*” Ex-1006, Cl. 11; *see also id.* ¶18, Cl. 10 (“a group ID is set to the access point corresponding to a service provided by that access point, and a field for representing the group ID is provided in the transmitter identification information so that *data communication can be carried out with only the access point providing a specific service*”). A POSITA would thus have understood that the stored information is not otherwise accessible to the wireless device utilizing Bluetooth. Watanabe explains why the stored information is only accessible in this manner: “because ... the first radio portion of the client terminal 14 does not carry out wireless communication with an access point 11 for which wireless communication is not allowed (one for which there is no contract), this not only can achieve a reduction in unnecessary radio traffic and a reduction in power consumption, but can extend battery life as well.” Ex-1006 ¶59; *see also id.* ¶16. Moreover, during prosecution of the '971 Patent, Applicant added this phrase to the independent claims in a Preliminary Amendment (Ex-1004, 93-116) and explained that the stored information “is not accessible using the short range wireless protocol, and instead

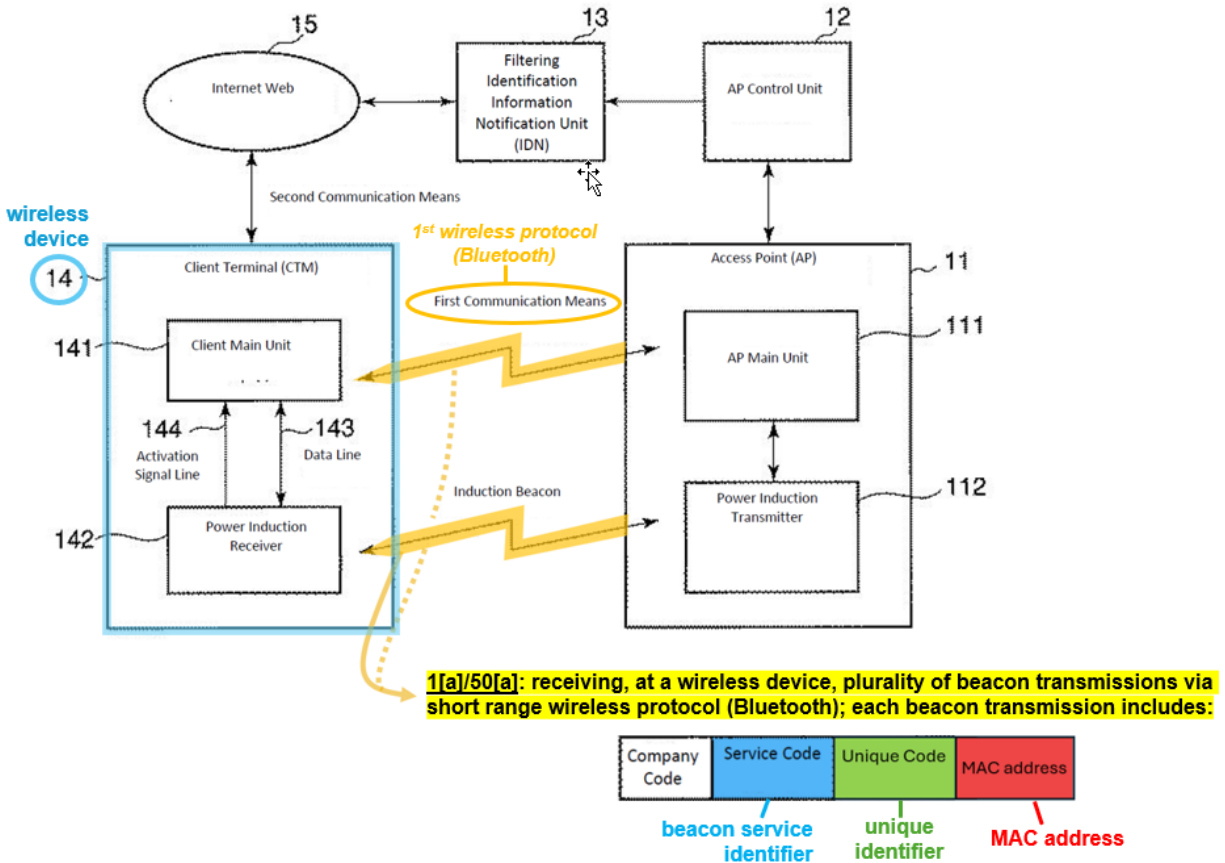
being provided via the broadcast only beacon transmitters.” *Id.*, 114 (citing Ex-1001, 13:1-4, 15:43-51). Watanabe’s power induction transmitter 112 is a “broadcast only” device because it “continuously or intermittently (cyclically) generates an induction beacon (power supply signal) ... to supply power contactlessly” to client terminal 14. Ex-1006 ¶¶9, 14. A separate power induction receiver at the client terminal receives the beacons over Bluetooth. Ex-1006 ¶9. Thus, as Applicant explained during prosecution, the stored information is not otherwise accessible to the wireless device using Bluetooth.

104. In addition to Watanabe-Ribaudó’s teachings above, as I explained in the Technological Background section of my Declaration, using beacon transmissions to make proximity determinations was known to a POSITA by 2008. *See, e.g.*, Section VII.A (citing, e.g., 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). Furthermore, using protocols such as Bluetooth for communications between mobile devices and servers was known. *See, e.g.*, Section VII.H (citing, e.g., Ex-1010 (Mgrdechian) ¶¶33, 72; Ex-1027 (Lazaridis), 1:26-32, 2:55-3:5; Ex-1028 (Gulin) ¶¶2, 72, 84, 86; Ex-1040 (Blake), 5:20-24, 7:53-59; Ex-1033 (Langensteiner) ¶13; Ex-1009 (Krikorian) ¶¶3, 8, 19).

105. Moreover, as I explained in the Technological Background section of

my Declaration, 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, 53, 140, 173, Fig. 4; 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). Additionally, including identifiers in beacon transmissions was known. *See, e.g.,* Section VII.C (citing, *e.g.,* Ex-1009 (Krikorian), Abstract, ¶¶4-5, 8, 22; Ex-1027 (Lazaridis), Abstract, 1:16-20, 2:37-45, 7:65-8:14; Ex-1010 (Mgrdechian) ¶¶13-14, 26-28, 42; Ex-1037 (Suzuki) ¶¶59, 63, 66, 68-70, 77-79, 83, Figs. 6-7, 9-11; Ex-1040 (Blake), 2:39-46; Ex-1033 (Langensteiner) ¶14; Ex-1030 (Quigley) ¶¶15-16; Ex-1039 (Sorte), 1-2).

106. In sum, as shown in Figure 1, Watanabe-Ribauda teaches Elements 1[a]/50[a].



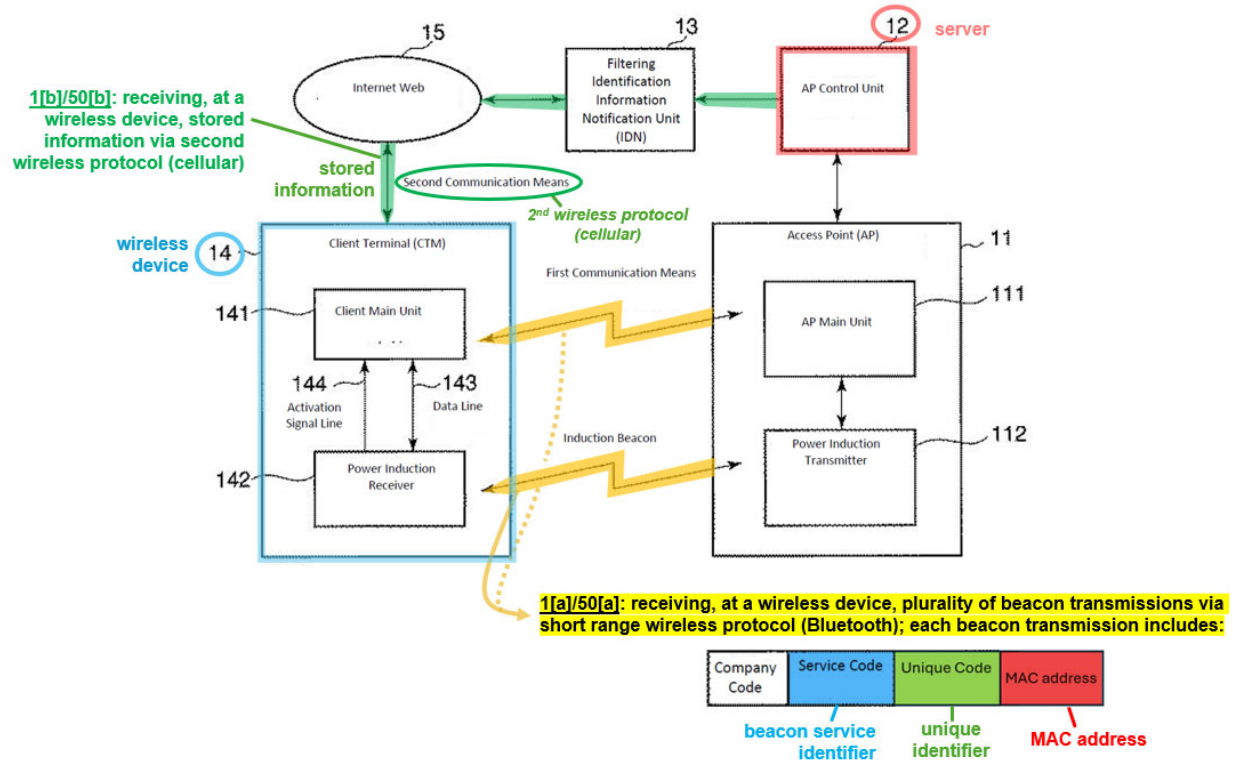
- c. Elements 1[b]/50[b]: [receiving, at the wireless device via a second wireless protocol, the stored information from one or more servers,]/[process stored information transferred from one or more servers to the wireless device via a second wireless protocol, wherein] the stored information relat[ing]/[es] to [a particular]/[an] entity or object associated with a first unique identifier, and wherein the second wireless protocol is different from the [short range]/[Bluetooth] wireless protocol;

107. In my opinion, Watanabe-Ribaudo teaches Elements 1[b]/50[b].

(1) Receiving at the wireless device stored information from a server

108. Watanabe teaches that AP control unit 12 (i.e., the “server”), shown in Figure 1 below, “stores ... the transmitter identification information and AP

identifier.” Ex-1006 ¶31, Fig. 1. Watanabe further teaches that client terminal 14 (i.e., the wireless device) communicates through the internet 15 with filtering identification information notification unit 13. Ex-1006 ¶26. Moreover, Watanabe teaches that “unit 13, in response to ... a request from a client terminal 14 generates, from information controlled by the AP control units 12, identification information for filtering ... corresponding to the client terminal 14.” Ex-1006 ¶25. And “the filtering identification information notification unit 13 sends, to the applicable client terminal through the internet 15, the identification information for filtering that has been generated.” Ex-1006 ¶33. Accordingly, AP control unit 12 corresponds to the recited “server” and the stored “transmitter identification information and AP identifier” corresponds to the recited “stored information.” Therefore, Watanabe’s wireless device receives via the second wireless protocol stored information from the server.



(2) Using a second wireless protocol different from Bluetooth

109. Watanabe teaches that client terminal 14 includes a “second communication means for communicating, through the internet 15, with the filtering identification information notification unit 13” to receive the generated identification information for filtering. Ex-1006 ¶26. “Mobile telephone devices, stationary telephone sets, or physically wired LANs, or the like, are envisioned as the second communication means by which the client terminal 14 accesses the internet 15.” *Id.* ¶27. Watanabe’s second wireless protocol (using a mobile telephone device to communicate over internet 15) is different from its first wireless protocol (Bluetooth). A POSITA would have understood to implement Watanabe’s second

wireless protocol using a known cellular protocol (e.g., CDMA, 3G, LTE). *See, e.g.*, Ex-1007 ¶¶16, 18 (teaching that GSM or CDMA mobile devices receive data from server via network).

(3) Stored information relates to an entity or object associated with a first unique identifier

110. Watanabe teaches that the stored information (i.e., the stored “transmitter identification information and AP identifier”) relates to a particular entity or object associated with a first unique identifier because, as explained in Section XI.A.2.b, Watanabe’s “unique code 203” (i.e., first unique identifier) that is beacons with the transmitter identification information assigned to the access point “can also be used to identify the access point 11 individually.” Ex-1006 ¶¶10, 15. Watanabe further teaches that “[o]ne access point 11 is ordinarily installed for each service provider.” Ex-1006 ¶13. Thus, the stored information relates to an entity of object (e.g., Netflix) that provides streaming services using the service provider company (e.g., C1, C2) for the access point. The content service provider (e.g., Netflix) corresponds to the recited “entity or object” associated with the first unique identifier.

111. In addition to Watanabe-Ribaudo’s teachings above, as I explained in the Technological Background section of my Declaration, using protocols such as Bluetooth and cellular for communications between mobile devices and servers was known to a POSITA by 2008. *See, e.g.*, Section VII.H (citing, e.g., Ex-1010

(Mgrdechian) ¶¶33, 72; Ex-1027 (Lazaridis), 1:26-32, 2:55-3:5; Ex-1028 (Gulin) ¶¶2, 72, 84, 86; Ex-1040 (Blake), 5:20-24, 7:53-59; Ex-1033 (Langensteiner) ¶13; Ex-1009 (Krikorian) ¶¶3, 8, 19). Additionally, storing information at servers and mobile devices communicating with servers to obtain stored information was known. *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; Ex-1029 (Kondou) ¶10).

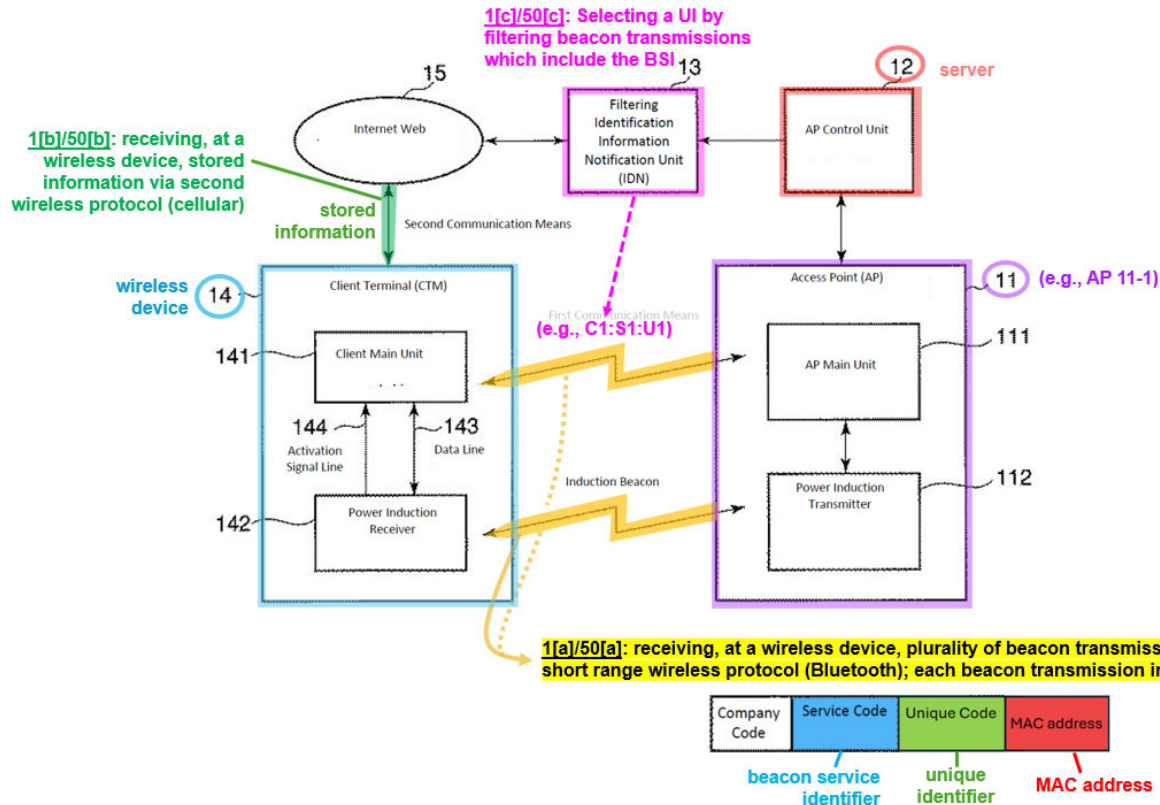
- d. **Elements 1[c]/50[c]: [causing selection of]/[select] one or more of the unique identifiers from the first plurality of beacon transmissions, by filtering the beacon transmissions which include a particular beacon service identifier indicating that a particular received beacon transmission is associated with a particular wireless beacon service; and**

112. In my opinion, Watanabe-Ribaudo teaches Elements 1[c]/50[c].

- (1) **Selecting a unique identifier from the first plurality of beacon transmissions by filtering the beacon transmissions**

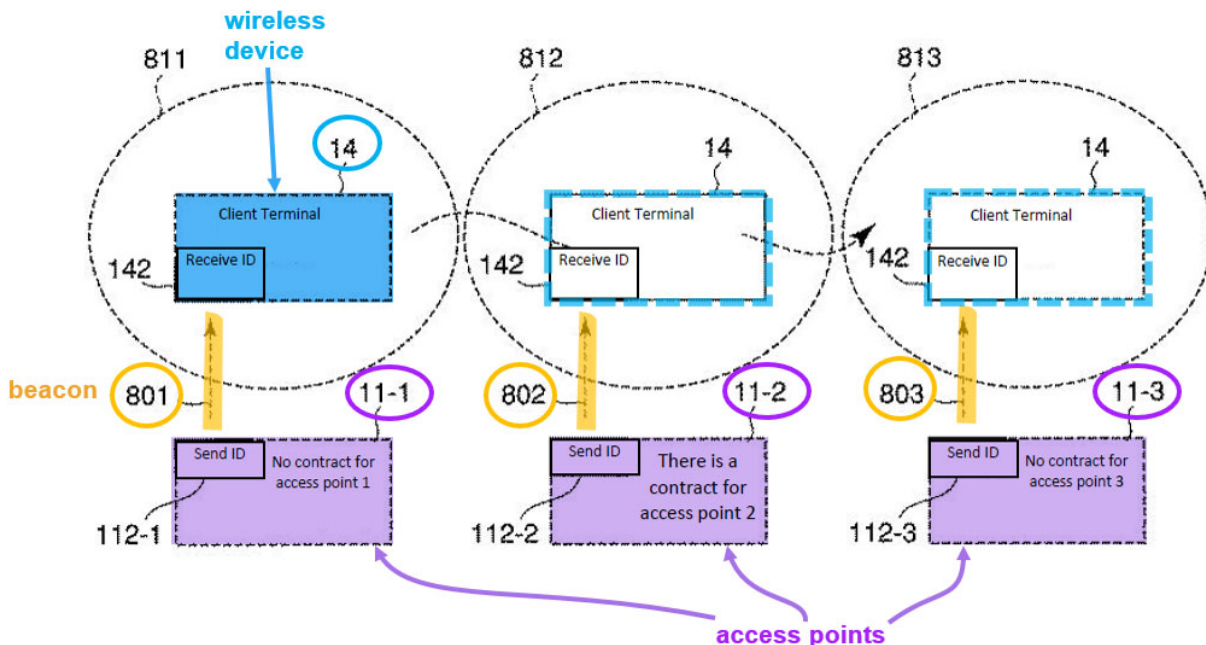
113. Watanabe teaches filtering the beacon transmissions. Watanabe's "filtering identification information notification unit 13 selects and combines appropriate codes from the information that has been obtained, to generate identification information for filtering in accordance with the client terminal 14." Ex-1006 ¶41. And in Watanabe, the beacon transmitters are filtered to associate

beacon transmissions with the device transmitting the beacon. For example, “three access points 11-1, 11-2, and 11-3” are “provided by service providers C1, C2, and C3, respectively” (Ex-1006 ¶48); “service codes indicating each of the services” provided by those companies are represented by “S1,” “S2,” and “S3” (Ex-1006 ¶41); and unique codes for the power induction transmitters of the access points are represented by “U1,” “U2,” and “U3.” Ex-1006 ¶49. Thus, as shown below, “the identification information ‘C1:S1:U1’ is included in the induction beacon sent from access point 11-1, the identification information ‘C2:S2:U2’ is included in the induction beacon sent from access point 11-2, and the identification information ‘C3:S3:U3’ is included in the induction beacon sent from access point 11-3.” Ex-1006 ¶49, Fig. 1.



114. Watanabe teaches selecting unique identifier(s) from the first plurality of beacon transmissions by filtering them. Watanabe describes an example where “the client terminal 14 has a contract with only service provider C2.” Ex-1006 ¶48. In this case, when client terminal 14 enters area 811 covered by access point 11-1, “the power induction receiver 142 receives the induction beacon 801 and is started up, and compares the transmitter identification information ‘C1:S1:U1,’ included therein, to the identification information for filtering that has been set in advance (which here is assumed to be ‘C2:S2’).” Ex-1006 ¶51. Because the company codes “C1” and “C2” are not a match, “a determination of no match is made,” “no comparison is carried out for the service codes,” and “[t]he operation of the power

induction receiver 142 is stopped when there is no match between the transmitter identification information and the identification information for filtering in this way.” Ex-1006 ¶51. As shown in Figure 8 below, when client terminal 14 enters into area 812 covered by access point 11-2, “the power induction receiver 142 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.” Ex-1006 ¶52, Fig. 8. Now “the company codes and service codes match, so the power induction receiver 142 determines that the identification information matches” and “transmits an activation signal to the client main unit 141 through a start line 144, to start up the client main unit 141.” Ex-1006 ¶52, Fig. 8.



Watanabe further teaches that “power induction transmitters 112-1, 112-2, and 112-3 of access points 11-1, 11-2, and 11-3 either continuously or periodically transmit induction beacons 801, 802, and 803 to provide a power supply to the client terminal 14 at locations within the areas that are covered by each.” Ex-1006 ¶49. Watanabe thus teaches that a plurality of beacon transmissions may be continuously received from a single AP. Moreover, Watanabe teaches filtering the plurality of beacon transmissions received from the same AP to determine whether the user has a contract to receive the services provided by the AP. Ex-1006, ¶57, Fig. 8.

(2) Beacon transmissions include a particular beacon service identifier indicating that a particular received beacon transmission is associated with a particular wireless beacon service

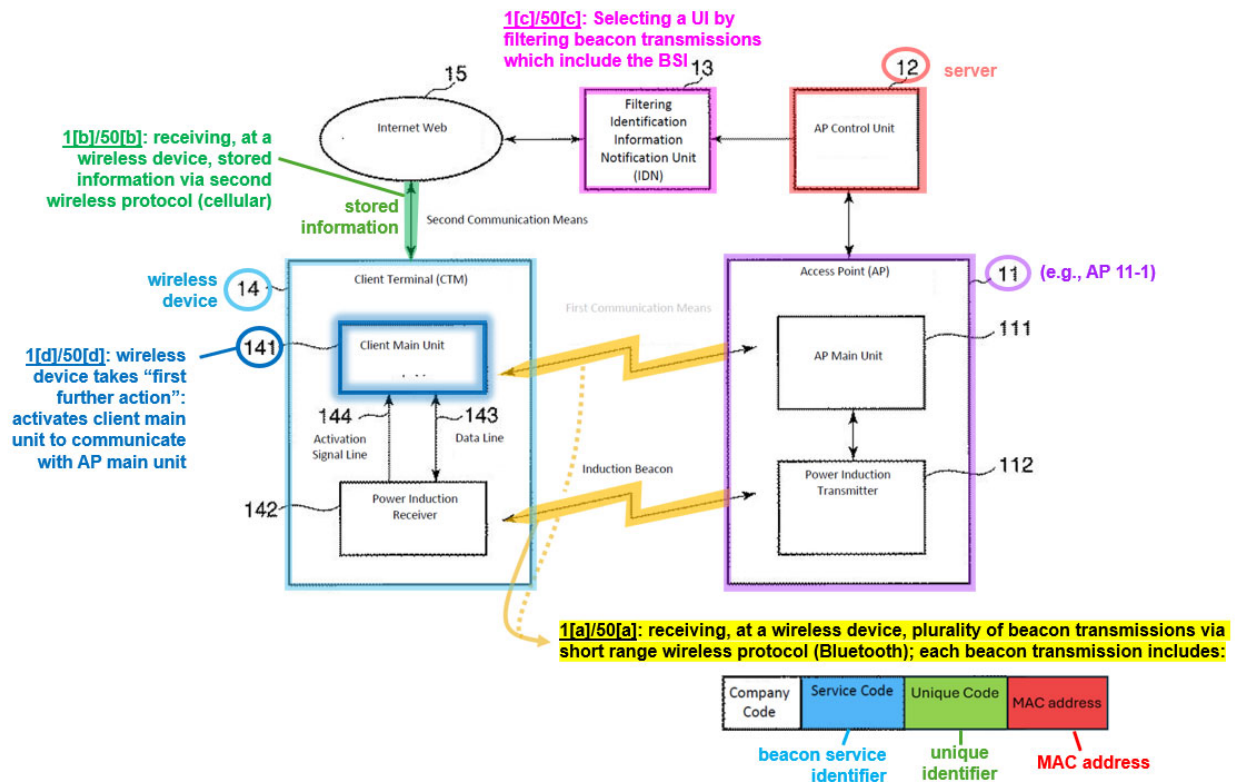
115. As explained in Sections XI.A.2.b-XI.A.2.c, each of Watanabe’s beacon transmissions includes a beacon service identifier (i.e., service codes S1, S2, S3), which identifies a wireless beacon service such as a streaming service like Netflix. Ex-1006 ¶15. Watanabe’s service code thus indicates that a particular received beacon transmission is associated with the particular wireless beacon service associated with that code. As described above, Watanabe explicitly distinguishes the service code from, for example, a network identifier or channel. In contrast, for example, the service can be associated with a “service content.” Ex-1006 ¶16.

116. In addition to Watanabe-Ribaudo's teachings above, as I explained in the Technological Background section of my Declaration, 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, e.g., Ex-1031 (Godfrey) ¶¶11, 35; Ex-1009 (Krikorian) ¶¶4-5, 26; Ex-1032 (Jansen), 8).

- e. **Elements 1[d]/50[d]: [taking]/[perform a] first further action[, the first further action] relating to the stored information, if the first unique identifier is present among the selected one or more unique identifiers.**

117. In my opinion, Watanabe-Ribaudo teaches Elements 1[d]/50[d].

118. Watanabe teaches performing a first further action relating to the stored information, if the first unique identifier is present among the selected one or more unique identifiers. Watanabe teaches that “[w]hen 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; *see also id.* ¶52 (as a result of a match, “power induction receiver 142 transmits an activation signal to the client main unit 141 through a start line 144, to start up the client main unit 141”). “When the client main unit 141 is started up in this way, the client main unit 141 establishes a communication channel with AP main unit 111, through a publicly known scanning



(Krikorian), Abstract, ¶¶4-5, 27-28; Ex-1027 (Lazaridis), 4:21-24, 4:31-53, 4:54-5:7, 5:8-28, 5:29-51, 5:52-65; Ex-1039 (Sorte), 4, 7-8; Ex-1040 (Blake), 7:43-49; Ex-1010 (Mgrdechian) ¶¶34-36, 41).

120. Thus, Watanabe-Ribaudo renders obvious Claims 1 and 50.

3. Dependent Claims 12-13, 15, 29-31, 34, 36, 56, 61, 64-65, 67, and 80

- a. Claims 12/64: The [method]/[computer program product] of claim [1]/[50] wherein the [taking] first further action [further]/[additionally] includes causing the wireless device[,] to: send the first unique identifier or information derived from the first unique identifier to at least one of the one or more servers, and [subsequently] receive the stored information in response [thereto].**

121. In my opinion, Watanabe-Ribaudo teaches Claims 12 and 64.

122. Ribaudo teaches causing the mobile device to send the unique identifier or information derived from it to the server and receiving the stored information in response. Ribaudo teaches that the “*data center may process the network address information received from mobile device 12,*” which “involves *comparing the network address information received from mobile device 12* to network address information received from one or more other mobile devices 12.” Ex-1007 ¶175. For instance, “if two mobile devices 12 report having the same MAC address in range, then data center 14 may determine that these two devices are in proximity to one another” and even if they are not using the same network, “the two mobile devices

12 could be notified of one another (e.g., by data center 14) and may be able to communicate with one another, via data center 14.” Ex-1007 ¶175.

123. Watanabe teaches that the first further action is related to the first unique identifier for the reasons explained in Section XI.A.2.e. In the Watanabe-Ribaudo-Behrens combination, taking first further action additionally includes causing Watanabe’s wireless device to send the first unique identifier or information derived from it to one or more servers, and receive the stored information in response, as taught by Ribaudo.

- b. Claims 13/65: The [method]/[computer program product] of claim [1]/[50] wherein the [computer program instructions, when executed by the one or more processors in the wireless device, further cause the wireless device to receive] stored information [is received] at the wireless device from at least one of the one or more servers prior to [the taking]/[performing] of the first further action.**

124. In my opinion, Watanabe-Ribaudo teaches Claims 13 and 65 for the reasons explained in Sections XI.A.2.c (receiving stored information at the wireless device from the server relating to an entity/object with a first unique identifier (Ex-1006 ¶¶10, 13, 15, 25-26, 31, 33, Fig. 1)), XI.A.2.d (selecting a unique identifier(s) by filtering (Ex-1006 ¶¶41, 48-49, 51-52, Fig. 8)), and XI.A.2.e (taking first further action relating to the stored information if the first unique identifier is present among the selected unique identifier(s) (Ex-1006 ¶¶47, 52-53)).

- c. **Claims 15/36/67/80: The [method]/[computer program product] of claim [1]/[50] [further comprising]/[wherein the] [computer program instructions][,]/[that,] [when executed by the one or more processors] [in the wireless device, further] [cause the wireless device to]: us[ing]/[e] the stored information to determine if the first unique identifier is present among the [first] selected one or more [of the] unique identifiers [from the first plurality of beacon transmissions].**

125. In my opinion, Watanabe-Ribaudo teaches Claims 15, 36, 67, and 80 for the reasons explained in Sections XI.A.2.c (receiving stored information relating to an entity/object with a first unique identifier (Ex-1006 ¶¶10, 13, 15, 25-26, 31, 33, Fig. 1)), XI.A.2.d (selecting a unique identifier(s) by filtering (Ex-1006 ¶¶41, 48-49, 51-52, Fig. 8)), and XI.A.2.e (taking first further action relating to the stored information if the first unique identifier is present among the selected unique identifier(s) (Ex-1006 ¶¶47, 52-53)).

- d. **Claims 29/56: The [method/computer program product] of claim [1/50] wherein the first further action is [additionally] related to receiving advertising information for presentation to a user of the wireless device, based upon the [first] unique identifier, or [based upon] information derived from the first unique identifier.**

126. In my opinion, Watanabe-Ribaudo teaches Claims 29 and 56.

127. Ribaudo teaches receiving advertising information for presentation to a user of the wireless device. Ribaudo teaches that data center 14 “may collect and store content generated by users of mobile devices 12” such as by associating “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. Ribaudó also teaches that "advertisements, personal advertisements, and classified advertisements may be served on a per wireless access point basis (e.g., a per MAC address basis or per cell tower ID basis)" and "displayed on mobile devices 12 using application 20." Ex-1007 ¶217.

128. Watanabe teaches that the first further action is based upon the first unique identifier or information derived from it for the reasons explained in Section XI.A.2.e. In the Watanabe-Ribaudó combination, the first further action is related to receiving advertising information for presentation to the user's wireless device, as taught by Ribaudó, based upon the first unique identifier or information derived from it, as taught by Watanabe.

- e. **Claim 30: The method of claim 1 wherein the first further action includes receiving content from a server based upon information derived from the first unique identifier.**

129. In my opinion, Watanabe-Ribaudó teaches Claim 30.

130. Watanabe teaches that the first further action (i.e., activating the client device to establish communication with a server of the service provider through the AP) is based upon information derived from the first unique identifier for the reasons explained in Section XI.A.2.e. A POSITA would have understood that the first

further action also includes receiving content from a server because Watanabe teaches that the client terminal 14 “receive[s], thereafter, the contracted services through the access point 11.” Ex-1006 ¶44.

131. Ribaud also teaches retrieving content from a server. Ribaud teaches that “data center 14 is operable to gather and store information regarding users of mobile devices 12, networks detected by users of mobile devices 12,” and “encounters between users of mobile devices 12, and other suitable information.” Ex-1007 ¶17. Moreover, “[d]ata center 14 may retrieve appropriate match data 26 for the first and second users ... based on the login information provided by the second user” by looking “up the second user’s client ID and the match ID associated with the first user to determine what, if anything, should be displayed to the second user (e.g., commonalities with the first user or other suitable information).” Ex-1007 ¶134. For example, “[w]hen 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.” Ex-1007 ¶47; *see also id.* ¶78. The displayed information corresponds to the recited content retrieved from a server.

132. In the Watanabe-Ribaud combination, the first further action is related to retrieving content from a server, as taught by Watanabe-Ribaud, based upon

information derived from the first unique identifier, as taught by Watanabe.

- f. Claims 31/61: The [method/computer program product] of claim [1/50,] wherein [following the taking of] the first further action[,/additionally includes causing the wireless device to send information to] a server associated with an account for a user of the wireless device[, and enabling the server to/performs a step of] send[ing] a[n email] message to an email address associated with the account for the user as a result of the first further action.**

133. In my opinion, Watanabe-Ribaudo teaches Claims 31 and 61.

134. Ribaudo teaches that the wireless device sends information to a server associated with the user's account and the server sends an email message to an email address associated with the account for the user. Ribaudo teaches that "the second user may enter an identifier of another user (e.g., the first user) such as an email address ... into the web site associated with data center 14 (and possibly the proprietor of system 10) to view what the second user shares in common with the first user." Ex-1007 ¶140. Or "if a first user sends a second user an email ... then the plug-in may display what the first and second users share in common." Ex-1007 ¶140. Ribaudo teaches that "sales people may use this capability to facilitate sales initiated by emails or other forms of communication." Ex-1007 ¶140. Ribaudo further teaches that "the user may have a window of opportunity (e.g., forty-eight hours) to communicate anonymously with a matched user, using an online messenger tool, email anonymizer, SMS, email, or another suitable mechanism."

Ex-1007 ¶152. Ribaudó also teaches that “if any other relevant users of other mobile devices 12 (e.g., users who are matches for the first user) are also reported to data center 14 as being nearby (i.e., either via BLUETOOTH scan, Wi-Fi, GSM, or otherwise), then the first user may receive a notification from data center 14 via SMS, email, or another suitable type of communication.” Ex-1007 ¶157.

135. Watanabe teaches that the first further action has already been performed for the reasons explained in Section XI.A.2.e. In the Watanabe-Ribaudó combination, the wireless device sends information to a server associated with the user’s account, the server sends an email message to an email address associated with the account for the user, as taught by Ribaudó, and the email would relate to the same particular entity or object associated with the first unique identifier as a result of the first further action, as taught by Watanabe.

g. Claim 34: The method of claim 1 wherein the first further action is related to either a product tied to a location or an advertisement tied to a location.

136. In my opinion, Watanabe-Ribaudó teaches Claim 34.

137. Watanabe-Ribaudó teaches that the first further action is related to an advertisement tied to a location for the reasons explained in Section XI.A.3.d. Ribaudó teaches that data center 14 “may collect and store content generated by users of mobile devices 12” such as by associating “the URLs of a user’s 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 also teaches that “*advertisements*, personal advertisements, and classified advertisements *may be served on a per wireless access point basis* (e.g., a per MAC address basis or per cell tower ID basis)” and “displayed on mobile devices 12 using application 20.” Ex-1007 ¶217. A POSITA would have understood that an advertisement tied to a cell tower ID would be tied to a location. Indeed, since the transmissions from an access point or cell tower have a limited radio range, the transmissions from the access point or cell tower would only reach users in the vicinity of that transmitter.

B. Ground 2: Claims 2-10, 14, 16, 18-19, 22-28, 35, 37-44, 46, 48-49, 51-55, 57-60, 62, 66, 68, 72, 75-79, and 81-83 are obvious over Watanabe in view of Ribaud and Behrens.

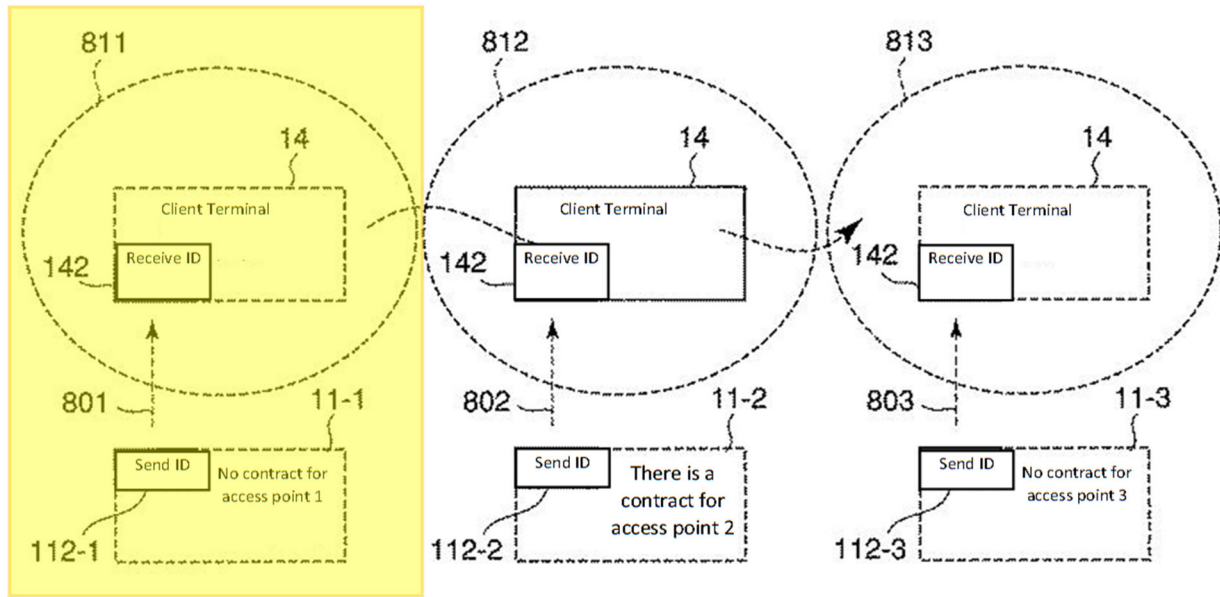
138. Independent Claim 37 appears to take the limitations of independent Claims 1 and 50 and repeat them twice. Specifically, Claim 37 recites the same first plurality of beacon transmissions as Claims 1 and 50 (*see* Ex-1020 (claim mapping table comparing 37[pre]-37[g] and 1[pre]/50[pre]-1[d]/50[d])) and adds a second plurality of beacon transmissions (*id.* 37[h]), which have different unique identifiers and MAC addresses from those in the first plurality of beacon transmissions but are received from the same transmitting device and have the same beacon service identifier as the first plurality of beacon transmissions (*id.* 37[i]-37[j]).

139. Claim 37 thus recites a system with a beacon transmitter that is like that

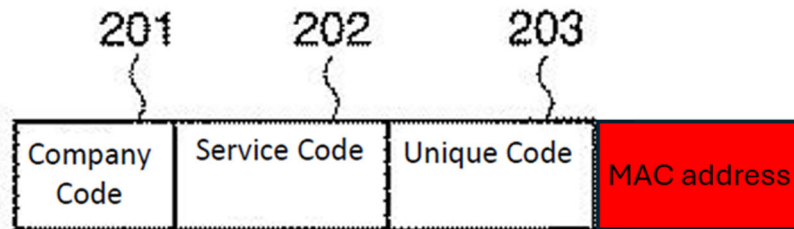
of Claims 1 and 50 in a first time period, but during a second time period, the beacon transmitter transmits the same service identifier but with a different unique identifier and with a different MAC address. The '971 Patent does not explain why the beacon transmitter would behave this way, but the prior art demonstrates why such a configuration would have been obvious.

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

140. In addition to the reasons set forth below, as explained in Section XI.A.1, the Watanabe-Ribaudó combination teaches receiving at the mobile device a first plurality of beacon transmissions during a first time period, which each include a MAC address (e.g., M1), a unique identifier (e.g., U1), and a beacon service identifier (e.g., S1). For example, as shown in Figures 2' and 8 below, when client terminal 14 enters area 811 (yellow), which is covered by access point 11-1, power induction receiver 142 receives continuous and periodic induction beacons 801 and filters based on the transmitter identification information, such as C1:S1:U1:M1. Ex-1006 ¶¶51-52.



[FIG. 2']



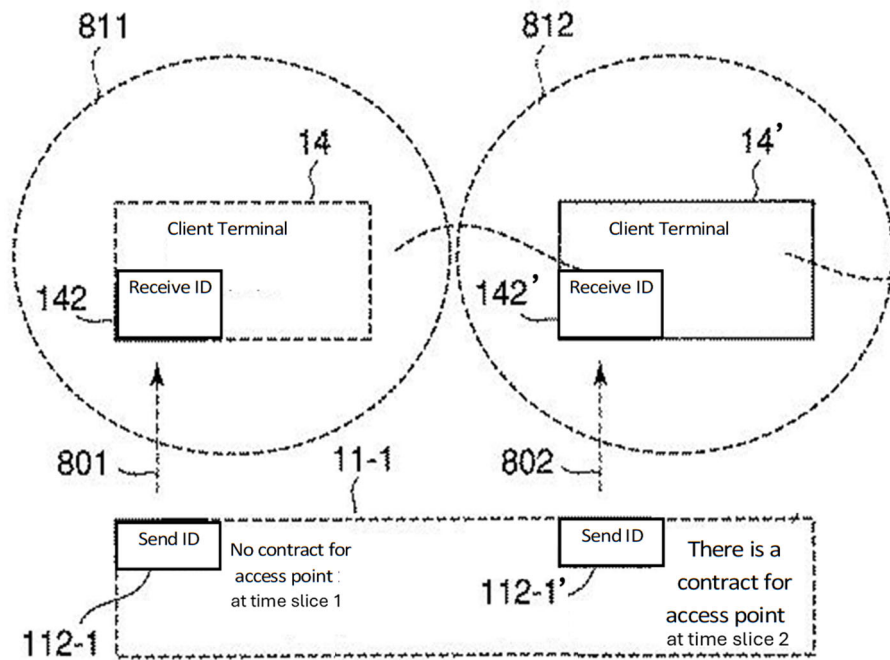
141. Watanabe further explains that certain of the codes transmitted by the beacon transmitter could also be used to distinguish between companies for which the client terminal (mobile device) has a preexisting relationship or contract. Ex-1006 ¶40. Watanabe states that these plurality of codes may come from several different access points (e.g. Watanabe 112-1, 112-2, and 112-3). Watanabe does not state that a plurality of distinct codes would come from a single access point, but this feature is taught by both Behrens and Ribaud.

142. Behrens teaches electronic devices that “continuously/repeatedly transmit” “unique identifiers (UID) via non-directed wireless radio frequency transmission.” Ex-1008, 11:1-5. Behrens teaches that a unique identifier (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. 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.” Ex-1008, 23:1-5. A POSITA would thus have understood that Behrens teaches that multiple unique identifiers may be associated with a single device.

143. Additionally, Ribauda 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. Ribauda explains that a single device with multiple distinct IDs is beneficial for shielding a true identity. Ex-1007 ¶46 (“[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”). Ribauda also teaches “time-slicing to join and bounce between several networks.” Ex-1007 ¶72. Ribauda 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. Ribaudó 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.* (alternatively associating with one network for detecting users in proximity and another network for accessing internet resources).

144. In the Watanabe-Ribaudó-Behrens combination, Watanabe’s wireless communication system would have been implemented in view of Ribaudó’s and Behrens’ teachings that *multiple unique identifiers* may be associated with the same device. The combined system would thus look like the below modified Watanabe figure, in which two different access points are replaced by a single physical access point that provides distinct codes at different time slices, as taught by Ribaudó.



145. A POSITA would have been motivated to modify Watanabe in this way for a number of reasons. It is a well-established principle that a POSITA would have been motivated to simplify a system by combining two different physical structures into one. As discussed for Claims 1/50, Watanabe-Ribaudo discloses an access point 11-1 (beacon transmitter) that transmits a plurality of beacons including company code, service code, unique identifier, and MAC address C1:S1:U1:M1. Watanabe-Ribaudo also teaches a second access point 11-2 that might transmit C2:S2:U2:M2. Watanabe also teaches that certain services might be provided by more than one company. For example, C1 may provide services S1, S2, S3, and C2 may provide S2 and S3. Ex-1006 ¶40. Because both C1 and C2 provide service S2, for example, a POSITA would have understood that it would be more efficient if the two

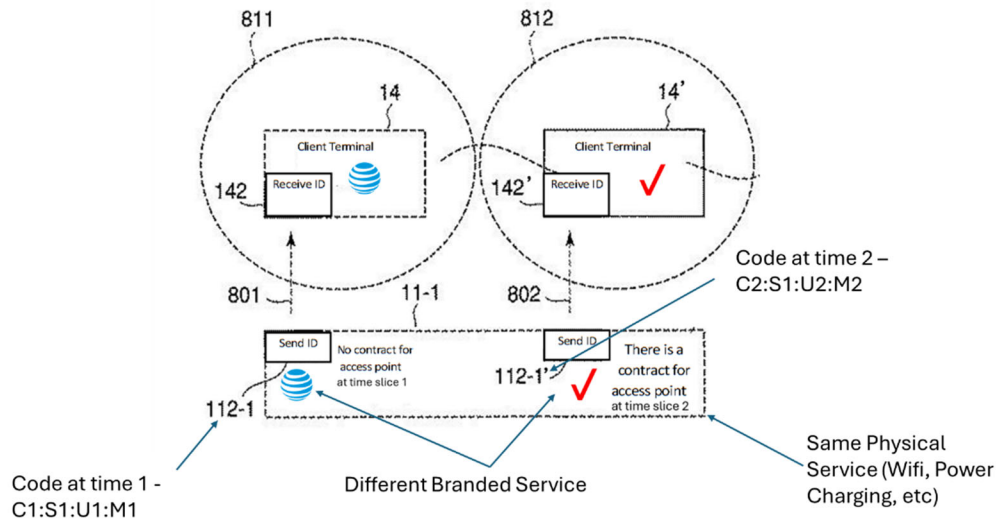
companies could share an access point instead of providing two separate ones so that C1 could provide service S2 at certain times and C2 could provide service S2 at other times. These services could have different unique identifiers. If two or more companies offer the same service from the same access point, it would be natural, in view of Behrens, to have a single access point transmit multiple beacons for different companies. The use of multiple beacon transmissions from the same access point with different unique identifiers and service identifiers would reduce the physical access points required saving cost and simplify the network.

146. Moreover, Watanabe explains that in some cases “there are contracts with a plurality of service providers to receive different services from each” and also that in some cases “there are contracts with a plurality of service providers for identical services.” Ex-1006 ¶62. So “services may be received from a plurality of service providers.” *Id.* In such cases, an individual may have contracts or pre-existing relationships for a particular service from one company, but not have a relationship for the same service from another. This may happen for any number of reasons, such as brand or company loyalty. For example, a user may prefer AT&T services over Verizon services, despite that the underlying service provided (e.g., Netflix’s streaming service) is exactly the same and may be provided by the exact same hardware. In such a case where the same services are being provided, a POSITA would have been motivated to use the same underlying hardware to provide

the same service, despite that a user may have contracts or business relationships with different companies that offer the same service.

147. Additionally Ribaudó teaches a further benefit of using two different IDs for a single device: shielding identities. In the combined system, the fact that similar services are being provided to, for example, Verizon users would have been “shielded” to a user that was brand-loyal to AT&T, as taught by Ribaudó. Ex-1007 ¶46. Behrens also teaches a similar benefit, namely that the same service, as taught by Watanabe, can be provided by companies with “different online identities,” as taught by Behrens (Ex-1008, 23:1-5), using the same underlying hardware. Thus, in the combined system, pre-existing business, company, and brand relationships between different entities can be shielded from the fact that the same underlying hardware infrastructure is in use.

148. In the Watanabe-Ribaudó-Behrens combination, Watanabe’s multiple unique identifiers received in the first and second plurality of beacon transmissions would be received via Bluetooth from the same transmitting device, as taught by Ribaudó and/or Behrens. Specifically, as shown in Figure 8’ below, Watanabe’s access point 11-1 would be modified to incorporate Ribaudó’s time slicing teachings such that during a first time period, the transmitter identification information C1:S1:U1:M1 would be transmitted, and during a second time period, the transmitter identification information C2:S1:U2:M2 would be transmitted.



This would allow two different companies to transmit the same service using the same hardware infrastructure but using different unique identifiers and MAC addresses so that the identity of the access point is shielded from the client. As Behrens explains, doing so would provide the user benefit of having “different online identities.” Ex-1008, 23:2-4; *see also* Ex-1007 ¶46 (Ribaud explaining the benefits of having multiple IDs “to shield the true identity of the user, for privacy purposes”).

149. Moreover, as I explained in the Technological Background section of my Declaration, continuously or periodically transmitting a beacon signal was known to a POSITA by 2008. *See, e.g.*, Section VII.D (citing, e.g., Ex-1026 (Bluetooth Specification), Fig. 72, 131-132; Ex-1025 (Wi-Fi Specification), 80-81, 419-420, Fig. 11-1; Ex-1009 (Krikorian) ¶25; Ex-1027 (Lazaridis), 2:3-10, 3:44-46, 3:59-65). It was also known that a plurality of MAC addresses could be used to

identify a single device and/or network. *See, e.g.*, Section VII.B (citing, e.g., Ex-1035 (Tamura) ¶¶47-48, Fig. 4).

150. Additionally, as I explained in the Technological Background section of my Declaration, 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). Moreover, including identifiers such as MAC addresses in beacon transmissions was known. *See, e.g.*, Section VII.C (citing, e.g., Ex-1009 (Krikorian), Abstract, ¶¶4-5, 8, 22; Ex-1027 (Lazaridis), Abstract, 1:16-20, 2:37-45, 7:65-8:14; Ex-1010 (Mgrdechian) ¶¶13-14, 26-28, 42; Ex-1037 (Suzuki) ¶¶59, 63, 66, 68-70, 77-79, 83, Figs. 6-7, 9-11).

151. A POSITA would have had a reasonable expectation of success in combining the teachings of Watanabe-Ribaudo and Behrens. All three describe receiving beacon transmissions comprising identification information associated with a nearby access point (or other device) at a mobile device using Bluetooth, receiving stored information relating to an entity associated with the identification information from a server using the Internet, comparing the beacons identification

information to preset identification information stored at the mobile device to determine if it matches, and taking further action relating to the stored information (such as activating the device or connecting with the other device to communicate) if it matches. Ex-1006 ¶¶46-55; Ex-1007 ¶¶6-7; Ex-1008, Abstract, 6:1-30, 19:5-14. The combination simply replaces multiple physical access points with a single one, and provides updated names of identification codes, all of which is within the routine level of skill in this art. Indeed, Ribaud teaches a mechanism to do exactly that in a way that is transparent to the user by a method it calls “time-slicing to join and bounce between several networks.” Ex-1007 ¶72. For example, “adaptor 18a may use NDIS and a WLAN driver to automatically associate mobile device 12a with both ad-hoc” networks to detect other users in proximity and infrastructure networks to access Internet resources, simultaneously, “staying within the timeout threshold for a given network[,] ... which may create virtualized simultaneous networks.” Ex-1007 ¶72. Behrens further teaches that “[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. A POSITA would thus have understood that these references disclose interrelated teachings based on well-understood technologies that would have been amenable to various well-understood and predictable combinations.

2. Independent Claim 37

a. Element 37[pre]: A mobile wireless device comprising:

152. In my opinion, Watanabe in view of Ribaud and Behrens (“Watanabe-Ribaud-Behrens”) teaches the preamble. *See* Section XI.A.2.a. Ex-1006, Abstract, ¶2.

b. Element 37[a]: one or more radios for providing reception and transmission for each of a Bluetooth wireless protocol and a second wireless protocol;

153. In my opinion, Watanabe-Ribaud-Behrens teaches Element 37[a]. *See* Sections XI.A.2.b and XI.A.2.c. Ex-1006 ¶27 (“wireless communication devices based on Bluetooth” are “the first communication means for achieving wireless communication between the AP main unit 111 and the client main unit 141” and “physically wired LANs, or the like” are “the second communication means by which the client terminal 14 accesses the internet 15”).

154. In addition to Watanabe-Ribaud-Behrens’ teachings above, as I explained in the Technological Background section of my Declaration, using protocols such as Bluetooth and cellular for communications between mobile devices and servers was known to a POSITA by 2008. *See, e.g.,* Section VII.H (citing, e.g., Ex-1010 (Mgrdechian) ¶¶33, 72; Ex-1027 (Lazaridis), 1:26-32, 2:55-3:5; Ex-1028 (Gulin) ¶¶2, 72, 84, 86; Ex-1040 (Blake), 5:20-24, 7:53-59; Ex-1033 (Langensteiner) ¶13; Ex-1009 (Krikorian) ¶¶3, 8, 19). Additionally, storing

information at servers and mobile devices communicating with servers to obtain stored information was known. *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; Ex-1029 (Kondou) ¶10).

c. Element 37[b]: one or more processors; and

155. In my opinion, Watanabe-Ribauda-Behrens teaches Element 37[b]. *See* Section XI.A.2.a. Ex-1007 ¶19. Ribauda teaches mobile devices 12 that “each include any suitable combination of hardware, software, and firmware to provide the functionality described” including “one or more applications 20 that are based on one or more programming languages” to “facilitate communication with other mobile devices 12” and the data center. Ex-1007 ¶19. Accordingly, a POSITA would have appreciated Ribauda as teaching one or more processors, as such hardware (e.g., a microprocessor or microcontroller, programmed with software or firmware) would be necessary to provide the described functionality. Virtually all embedded communication devices, both at the time of ’971 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) describes a

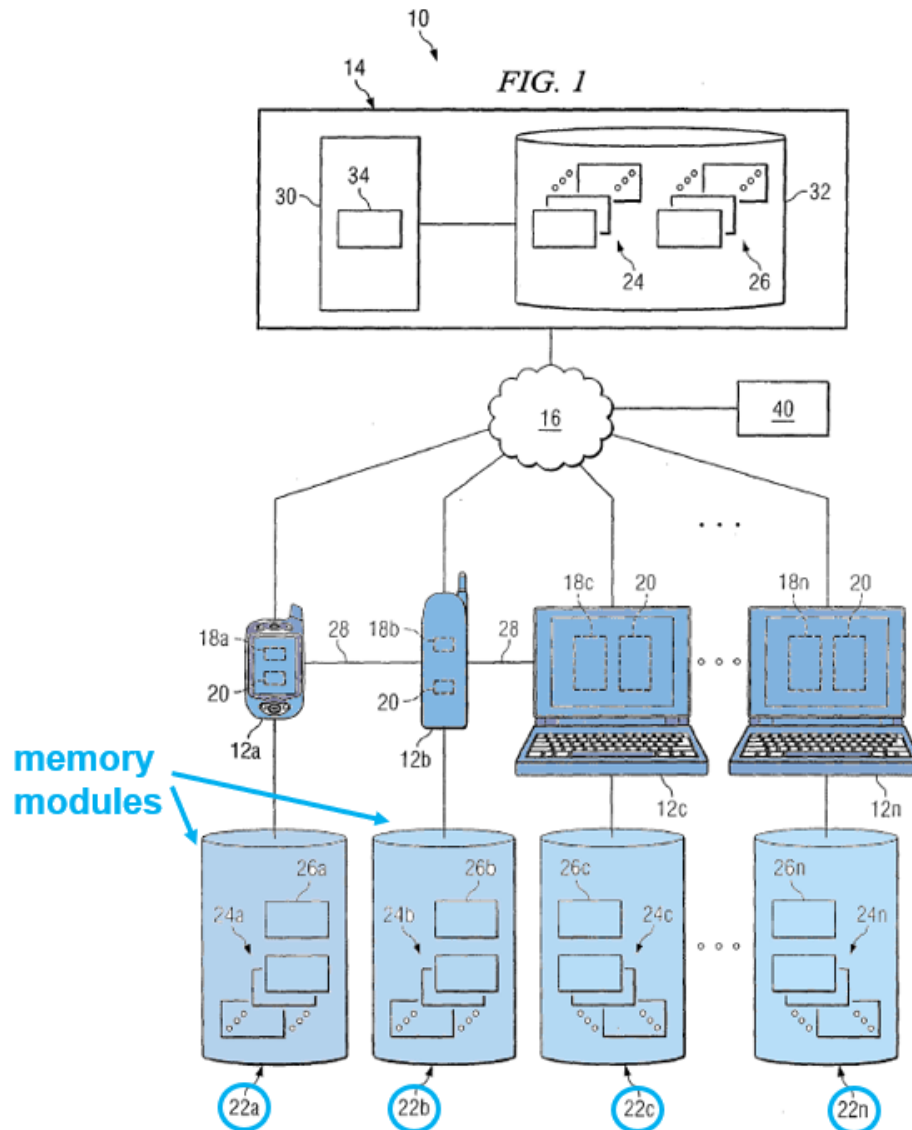
typical design. Here, the modem PHY functions are implemented in an ASIC (hardware). The host software interfaces to the hardware via firmware running on an embedded ARM processor. Ex-1041 at 1926-27. A POSITA would have also understood that processors are inherent components in mobile telephones, as taught by Behrens. Behrens teaches “a small, battery-powered handheld device” such as a mobile phone, having “the components necessary for sending out, via short-range and/or medium-range radio frequency, at least one [unique identifier] UID” including “at least one microprocessor for managing the wireless radio transmissions as well as for processing and storing data.” Ex-1008, 20:31-21:15.

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

- d. Element 37[c]: 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:**

157. In my opinion, Watanabe-Ribaudo-Behrens teaches Element 37[c]. *See* Section XI.A.2.a. Ex-1007 ¶¶19, 32. Ribaudo explains that its “[m]obile devices 12 may each have an associated memory module 22”—or “any suitable memory

modules 22 according to particular needs”—that may be “operable to store data as one or more compressed binary files.” Ex-1007, ¶32; Fig. 1.



158. 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). Along with data, the memory module stores software instructions for performing the functions described below. Ex-1007, Cl. 31 (directed to “[s]oftware for proximity determination, the software being embodied in a computer-readable medium and when executed, operable to” perform the claimed functions). Accordingly, a POSITA would have understood Ribaudo as teaching that its memory modules are coupled to the one or more processors, and store a set of software instructions that when executed by the processors, cause the processors to perform the operations described further below.

159. A POSITA would have also understood that Element 37[c] recites components that are inherent in mobile telephones, as taught by Behrens. Behrens teaches a mobile phone including “memory, which may be FLASH memory” and “at least one microprocessor for managing the wireless radio transmissions as well as for processing and storing data.” Ex-1008, 20:31-21:15.

160. Moreover, in addition to Watanabe-Ribaudo-Behrens’ teachings above, as I explained in the Technological Background section of my Declaration, using a processor and memory with instructions to execute functions on mobile devices was known by 2008. *See, e.g.*, Section VII.I (citing, e.g., Ex-1009 (Krikorian) ¶¶6, 30-

32; Ex-1028 (Gulin), ¶¶29, 79-80, Fig. 2; Ex-1029 (Kondou) ¶¶23, 29).

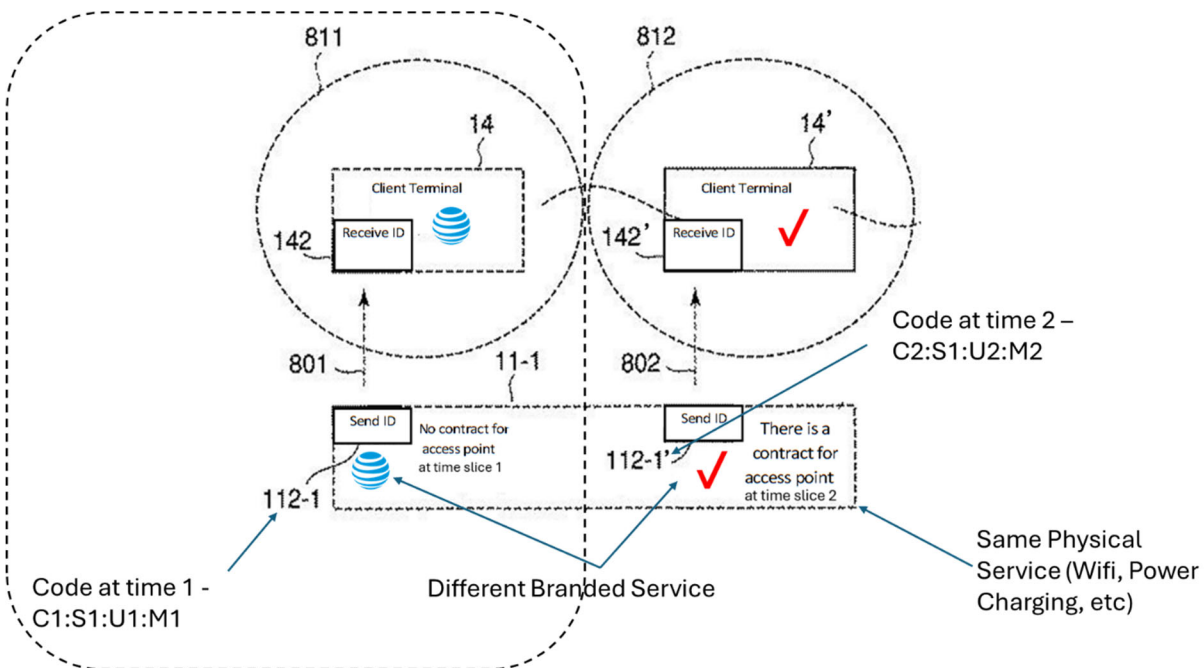
- e. **Element 37[d]: receiving from a beacon transmitter, using the Bluetooth wireless protocol, a first plurality of beacon transmissions during a first time period, each of the beacon transmissions including (a) a MAC address, (b) a unique identifier, the unique identifier does not directly identify a location of the beacon transmitter, and (c) a beacon service identifier, wherein the beacon service identifier of each respective beacon transmission identifies that the unique identifier is relevant to stored information associated with a wireless beacon service, wherein the stored information is not otherwise accessible to the wireless device utilizing the Bluetooth wireless protocol;**

161. In my opinion, Watanabe-Ribaud-Behrens teaches Element 37[d]. *See* Section XI.A.2.b.

162. Additionally, Ribaud teaches that the first plurality of beacon transmissions are received *during a first time period*. Ribaud teaches “time-slicing to join and bounce between several networks.” Ex-1007 ¶72. For example, “adaptor 18a may use NDIS and a WLAN driver to automatically associate mobile device 12a with both ad-hoc” networks to detect other users in proximity and infrastructure networks to access Internet resources, simultaneously, “staying within the timeout threshold for a given network[,] ... which may create virtualized simultaneous networks.” Ex-1007 ¶72. Ribaud 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 further teaches that adaptor 18a automatically weighs “the amount of time it spends on each mode, so that resources may be economically distributed.” Ex-1007 ¶72. In the Watanabe-Ribaudo-Behrens combination, Watanabe’s mobile device receives a first plurality of beacon transmissions over Bluetooth from a beacon transmitter during a first time period, as taught by Ribaudo.

163. As explained above in Section XI.B.1 and shown in Figure 8’ below, in the Watanabe-Ribaudo-Behrens combination, Watanabe’s multiple unique identifiers received in the first and second plurality of beacon transmissions would be received via Bluetooth from the same transmitting device in different time periods, as taught by Ribaudo and/or Behrens. During the recited “first time period,” the client terminal would receive the code C1:S1:U1:M1.



164. In addition to Watanabe-Ribaudo-Behrens’ teachings above, as I

explained in the Technological Background section of my Declaration, using beacon transmissions to make proximity determinations was known to a POSITA by 2008. *See, e.g.*, Section VII.A (citing, e.g., 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). Furthermore, using protocols such as Bluetooth for communications between mobile devices and servers was known. *See, e.g.*, Section VII.H (citing, e.g., Ex-1010 (Mgrdechian) ¶¶33, 72; Ex-1027 (Lazaridis), 1:26-32, 2:55-3:5; Ex-1028 (Gulin) ¶¶2, 72, 84, 86; Ex-1040 (Blake), 5:20-24, 7:53-59; Ex-1033 (Langensteiner) ¶13; Ex-1009 (Krikorian) ¶¶3, 8, 19).

165. Moreover, as I explained in the Technological Background section of my Declaration, 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, 53, 140, 173, Fig. 4; 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). Additionally, including identifiers in beacon transmissions was known. *See, e.g.*, Section VII.C (citing, e.g., Ex-1009

(Krikorian), Abstract, ¶¶4-5, 8, 22; Ex-1027 (Lazaridis), Abstract, 1:16-20, 2:37-45, 7:65-8:14; Ex-1010 (Mgrdechian) ¶¶13-14, 26-28, 42; Ex-1037 (Suzuki) ¶¶59, 63, 66, 68-70, 77-79, 83, Figs. 6-7, 9-11; Ex-1040 (Blake), 2:39-46; Ex-1033 (Langensteiner) ¶14; Ex-1030 (Quigley) ¶¶15-16; Ex-1039 (Sorte), 1-2). And, continuously or periodically transmitting a beacon signal was also known to a POSITA by 2008. *See, e.g.*, Section VII.D (citing, e.g., Ex-1026 (Bluetooth Specification), Fig. 72, 131-132; Ex-1025 (Wi-Fi Specification), 80-81, 419-420, Fig. 11-1; Ex-1009 (Krikorian) ¶25; Ex-1027 (Lazaridis), 2:3-10, 3:44-46, 3:59-65).

f. Element 37[e]: receiving from one or more servers, using the second wireless protocol, stored information related to a entity or object associated with a first unique identifier;

166. In my opinion, Watanabe-Ribauda-Behrens teaches Element 37[e]. *See* Section XI.A.2.c.

167. In addition to Watanabe-Ribauda-Behrens' teachings above, as I explained in the Technological Background section of my Declaration, using protocols such as Bluetooth and cellular for communications between mobile devices and servers was known to a POSITA by 2008. *See, e.g.*, Section VII.H (citing, e.g., Ex-1010 (Mgrdechian) ¶¶33, 72; Ex-1027 (Lazaridis), 1:26-32, 2:55-3:5; Ex-1028 (Gulin) ¶¶2, 72, 84, 86; Ex-1040 (Blake), 5:20-24, 7:53-59; Ex-1033 (Langensteiner) ¶13; Ex-1009 (Krikorian) ¶¶3, 8, 19). Additionally, storing information at servers and mobile devices communicating with servers to obtain

stored information was known. *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; Ex-1029 (Kondou) ¶10).

- g. Element 37[f]: selecting one or more unique identifiers from the first plurality of beacon transmissions, by filtering the beacon transmissions which include a particular beacon service identifier indicating that a particular received beacon transmission is associated with the particular wireless beacon service;**

168. In my opinion, Watanabe-Ribauda-Behrens teaches Element 37[f]. *See* Section XI.A.2.d.

169. In addition to Watanabe-Ribauda-Behrens' teachings above, as I explained in the Technological Background section of my Declaration, 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, *e.g.*, Ex-1031 (Godfrey) ¶¶11, 35; Ex-1009 (Krikorian) ¶¶4-5, 26; Ex-1032 (Jansen), 8).

- h. Element 37[g]: taking first further action relating to the stored information, if the first unique identifier is present among the selected one or more unique identifiers;**

170. In my opinion, Watanabe-Ribauda-Behrens teaches Element 37[g]. *See* Section XI.A.2.e.

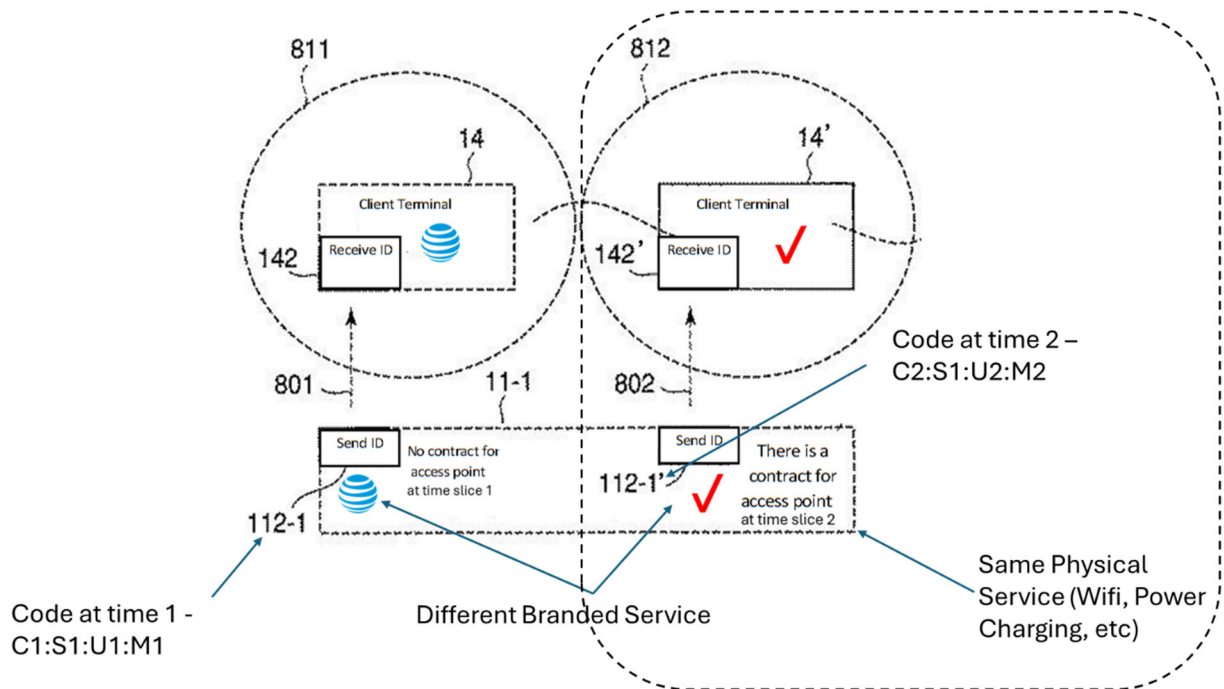
171. In addition to Watanabe-Ribauda-Behrens' teachings above, as I explained in the Technological Background section of my Declaration, taking action if a match is determined between the stored information and the transmitted information was known to a POSITA by 2008. *See, e.g.*, Section VII.G (citing, e.g., Ex-1009 (Krikorian), Abstract, ¶¶4-5, 27-28; Ex-1027 (Lazaridis), 4:21-24, 4:31-53, 4:54-5:7, 5:8-28, 5:29-51, 5:52-65; Ex-1039 (Sorte), 4, 7-8; Ex-1040 (Blake), 7:43-49; Ex-1010 (Mgrdechian) ¶¶34-36, 41).

- i. **Element 37[h]: receiving, by the wireless device, using the Bluetooth wireless protocol, during a second time period, a second plurality of beacon transmissions, each of the second plurality of beacon transmissions comprising three fields (a) a MAC address, (b) a unique identifier, wherein the unique identifier of each respective beacon transmission does not directly identify a location of a beacon transmitter, and (c) the beacon service identifier, wherein the beacon service identifier of each respective beacon transmission identifies that the unique identifier is relevant to stored information associated with a wireless beacon service, wherein the stored information is not accessible to the wireless device utilizing the Bluetooth wireless protocol;**

172. In my opinion, Watanabe-Ribauda-Behrens teaches Element 37[h].

173. As explained in Section XI.B, Claim 37 simply repeats the “receiving” step of Claims 1 and 50, but during a second time period the beacon transmitter transmits the same service identifier but with a different unique identifier and with a different MAC address. As explained in Section XI.B.1 and shown in Figure 8’

below, during the recited “second time period,” the client terminal would receive the code C2:S1:U2:M2. The second time period corresponds to the second period of Ribaudó’s “time slicing” for bouncing between networks. Ex-1007 ¶72.



174. Moreover, as explained in Section XI.B.1, a POSITA would have been motivated to modify Watanabe in this way for a number of reasons, including reducing the number of physical components and simplifying the hardware, allowing for multiple different companies to use the same hardware to provide the same service, and to protect different company brand identities and shield the end user from hardware implementation details. Thus, in the combined system, pre-existing business, company, and brand relationships between different entities can be shielded from the fact that the same underlying hardware infrastructure is in use.

175. In addition to Watanabe-Ribaudó-Behrens’ teachings above, as I

explained in the Technological Background section of my Declaration, using beacon transmissions to make proximity determinations was known to a POSITA by 2008. *See, e.g.*, Section VII.A (citing, e.g., 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). Furthermore, using protocols such as Bluetooth for communications between mobile devices and servers was known. *See, e.g.*, Section VII.H (citing, e.g., Ex-1010 (Mgrdechian) ¶¶33, 72; Ex-1027 (Lazaridis), 1:26-32, 2:55-3:5; Ex-1028 (Gulin) ¶¶2, 72, 84, 86; Ex-1040 (Blake), 5:20-24, 7:53-59; Ex-1033 (Langensteiner) ¶13; Ex-1009 (Krikorian) ¶¶3, 8, 19).

176. Moreover, as I explained in the Technological Background section of my Declaration, 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, 53, 140, 173, Fig. 4; 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). Additionally, including identifiers in beacon transmissions was known. *See, e.g.*, Section VII.C (citing, e.g., Ex-1009

(Krikorian), Abstract, ¶¶4-5, 8, 22; Ex-1027 (Lazaridis), Abstract, 1:16-20, 2:37-45, 7:65-8:14; Ex-1010 (Mgrdechian) ¶¶13-14, 26-28, 42; Ex-1037 (Suzuki) ¶¶59, 63, 66, 68-70, 77-79, 83, Figs. 6-7, 9-11; Ex-1040 (Blake), 2:39-46; Ex-1033 (Langensteiner) ¶14; Ex-1030 (Quigley) ¶¶15-16; Ex-1039 (Sorte), 1-2). And, continuously or periodically transmitting a beacon signal was also known to a POSITA by 2008. *See, e.g.*, Section VII.D (citing, e.g., Ex-1026 (Bluetooth Specification), Fig. 72, 131-132; Ex-1025 (Wi-Fi Specification), 80-81, 419-420, Fig. 11-1; Ex-1009 (Krikorian) ¶25; Ex-1027 (Lazaridis), 2:3-10, 3:44-46, 3:59-65).

- j. **Element 37[i]: selecting one or more of the unique identifiers from the second plurality of beacon transmissions, by filtering the beacon transmissions which include the same particular beacon service identifier indicating that a particular received beacon transmission is associated with the same particular wireless beacon service;**

177. In my opinion, Watanabe-Ribaudo-Behrens teaches Element 37[i]. As discussed in Section XI.B, the only meaningful difference between the first and second plurality of transmissions is that, in the modified system, Watanabe's transmissions are changed based on Ribaudo's time-slicing teachings. So, instead of the code being "C1:S1:U1:M1" as it was during the first time period, during these steps relating to the second time period, the code is "C2:S1:U2:M2." The software and processing steps work the same way; they just operate on this modified code. So, see above Sections XI.B.2.g and XI.A.2.d.

178. In addition to Watanabe-Ribauda-Behrens' teachings above, as I explained in the Technological Background section of my Declaration, 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, e.g., Ex-1031 (Godfrey) ¶¶11, 35; Ex-1009 (Krikorian) ¶¶4-5, 26; Ex-1032 (Jansen), 8).

- k. Element 37[j]: taking second further action relating to the stored information, if a second unique identifier is present among the one or more unique identifiers selected from the second plurality of beacon transmissions, wherein the second unique identifier is associated with the same entity or object, and wherein the second unique identifier is not equal to the first unique identifier, and further wherein the received beacon transmissions including the first and second unique identifiers are received from a same transmitting device; and**

179. In my opinion, Watanabe-Ribauda-Behrens teaches Element 37[j].

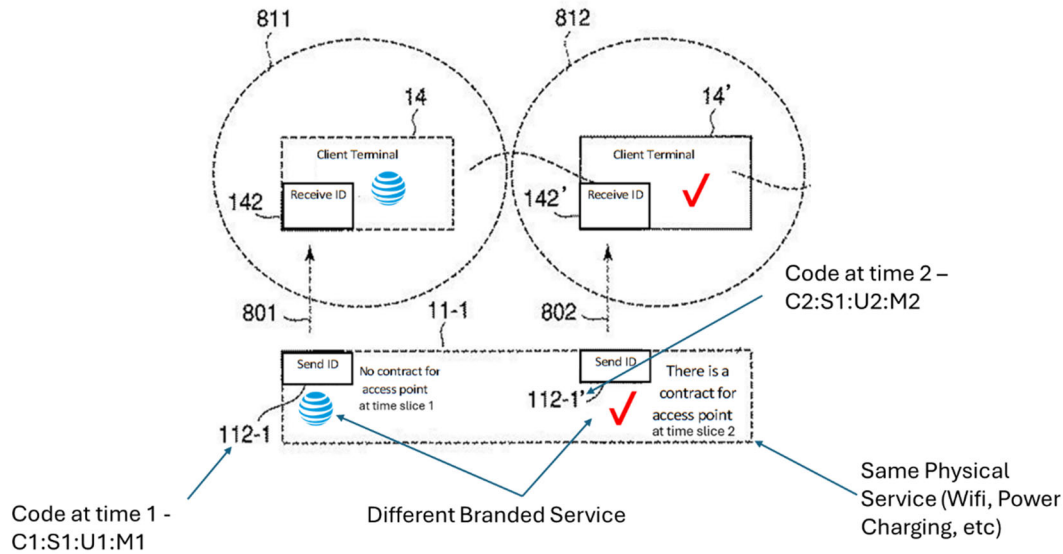
- (1) Taking second further action relating to the stored information, if a second unique identifier is present among the one or more unique identifiers selected from the second plurality of beacon transmissions, wherein the second unique identifier is associated with the same entity or object**

180. As discussed in Section XI.B, the only meaningful difference between the first and second further actions is that, in the modified system, Watanabe's transmissions are changed based on Ribauda's time-slicing teachings. So, instead of

the code being “C1:S1:U1:M1” as it was during the first time period, during these steps relating to the second time period, the code is “C2:S1:U2:M2.” The software and processing steps work the same way, they just operate on this modified code. So, see above Sections XI.B.2.h and XI.A.2.e. Moreover, the first and second unique identifiers are associated with the same entity or object because during both the first and second time periods, Netflix is the entity or object that provides its video streaming service to companies C1 and C2 (e.g., AT&T and Verizon) through the APs.

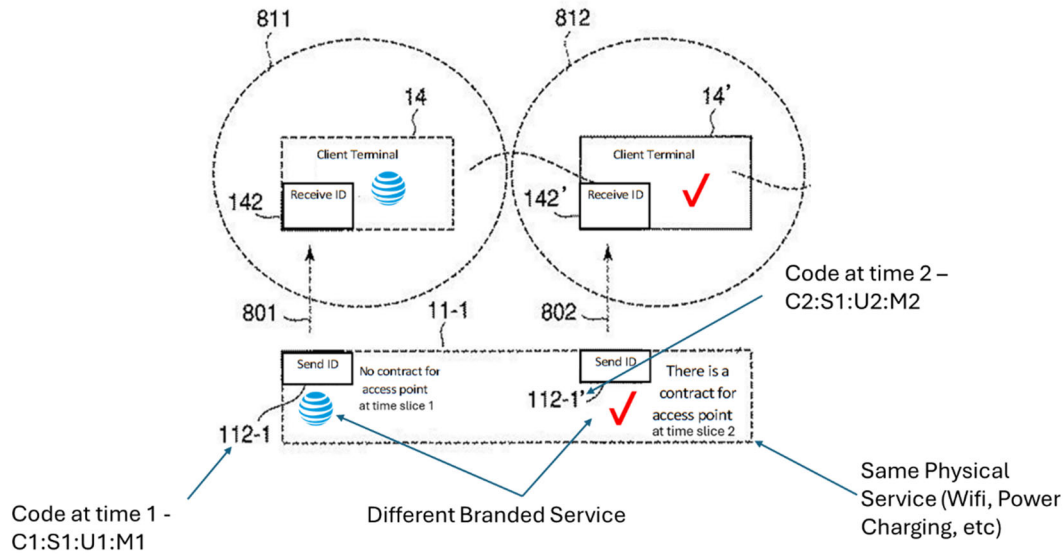
(2) Second unique identifier is not equal to the first unique identifier

181. As explained in Section XI.B.1 and shown in Figure 8’ below, in the Watanabe-Ribauda-Behrens combination, the plurality of beacon transmissions include different unique identifiers, as taught by Ribauda and/or Behrens. Specifically, an identifier such as U1 would be used when the access point is operating during a first time slice associated with an entity or object (e.g., Netflix) whose streaming services are provided by a first company C1 (e.g., AT&T), and a different identifier such as U2 would be used when the access point is operating during a second time slice associated with an entity or object (e.g., Netflix) whose streaming services are provided by a second company C2 (e.g., Verizon):



(3) Received beacon transmissions including the first and second unique identifiers are received from a same transmitting device

182. As explained in Section XI.B.1, in the Watanabe-Ribaudo-Behrens combination, Watanabe's multiple unique identifiers received in the first and second plurality of beacon transmissions would be received via Bluetooth from the same transmitting device, as taught by Ribaudo and/or Behrens. Specifically, they would have been received by transmitting device 11-1 in the modified/combined figure below:



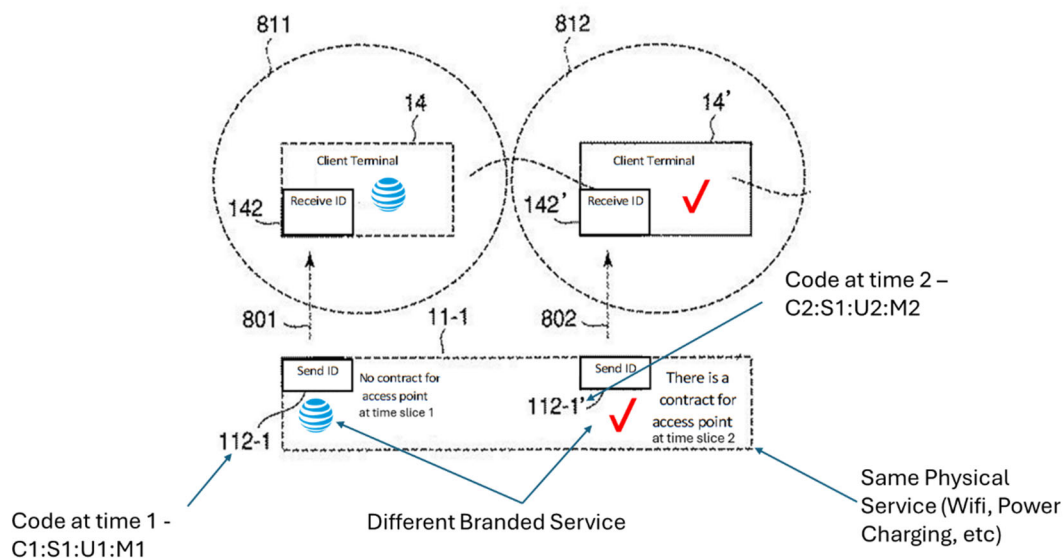
183. In addition to Watanabe-Ribaudo-Behrens' teachings above, as I explained in the Technological Background section of my Declaration, taking action if a match is determined between the stored information and the transmitted information was known to a POSITA by 2008. *See, e.g.*, Section VII.G (citing, e.g., Ex-1009 (Krikorian), Abstract, ¶¶4-5, 27-28; Ex-1027 (Lazaridis), 4:21-24, 4:31-53, 4:54-5:7, 5:8-28, 5:29-51, 5:52-65; Ex-1039 (Sorte), 4, 7-8; Ex-1040 (Blake), 7:43-49; Ex-1010 (Mgrdechian) ¶¶34-36, 41).

- I. **Element 37[k]: wherein the MAC address received in a beacon transmission including the second unique identifier is different from the MAC address received in a beacon transmission including the first unique identifier, but each such beacon transmission includes the same particular beacon service identifier.**

184. In my opinion, Watanabe-Ribaudo-Behrens teaches Element 37[k].

(1) MAC address received in beacon transmission including the second unique identifier is different from MAC address received in beacon transmission including the first unique identifier

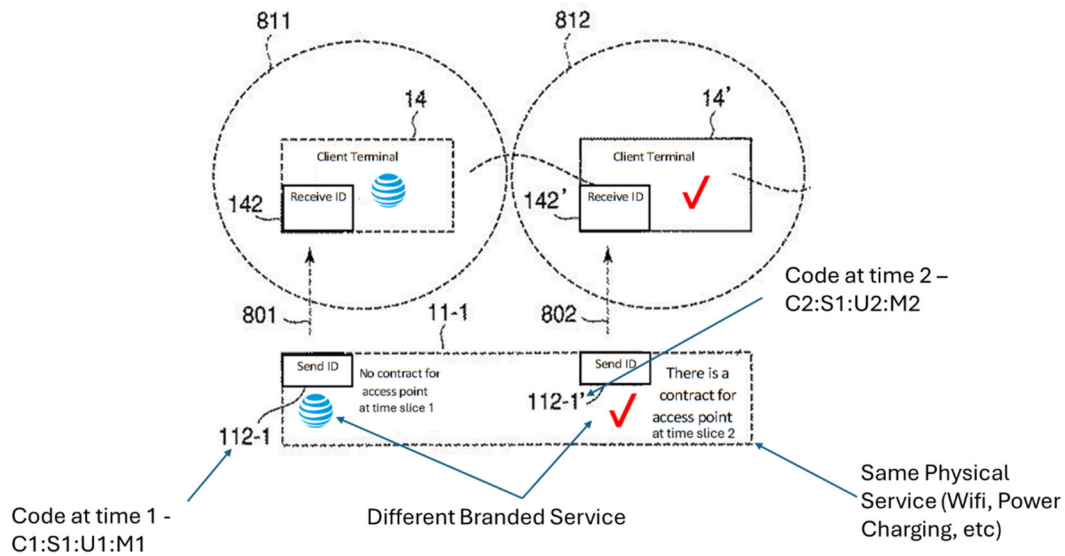
185. As explained in Section XI.B.1 and shown in Figure 8' below, in the Watanabe-Ribaudo-Behrens combination, the plurality of beacon transmissions have different MAC addresses. Specifically, MAC address M1 would be used when the access point is operating during a first time slice associated with a first company C1 (e.g., AT&T), and MAC address M2 would be used when the access point is operating during a second time slice associated with a second company C2 (e.g., Verizon):



(2) Each beacon transmission includes the same particular beacon service identifier

186. As shown in the combined figure, the same service identifier, S1, is used in all cases because the same physical service is being offered (e.g., Netflix),

just by a different company or brand.



187. In addition to Watanabe-Ribaudo-Behrens' teachings above, as I explained in the Technological Background section of my Declaration, it was known by 2008 that a plurality of MAC addresses could be used to identify a single device and/or network by 2008. *See, e.g.*, Section VII.B (citing, e.g., Ex-1035 (Tamura) ¶¶47-48, Fig. 4).

3. Dependent Claims 2-10, 14, 16, 18-19, 22-28, 35, 38-44, 46, 48-49, 51-55, 57-60, 62, 66, 68, 72, 75-79, and 81-83

a. Claims 2 and 51

(1) Element 2[pre]: The method of claim 1, wherein the receiving, at the wireless device, via a short range wireless protocol, of the first plurality of beacon transmissions occurs in a first time period, and,

Element 51[pre]: The computer program product of claim 50 wherein the computer program instructions, when executed by the one or more processors in the wireless device, cause the wireless device to: during a first time period: process the first plurality of beacon transmissions in the first time period, and

188. In my opinion, Watanabe-Ribaudo-Behrens teaches the preamble, to the extent it is limiting. *See* Section XI.B.2.e.

(2) Elements 2[a]/51[a]: [wherein the method further comprises,] during a second time period:

189. In my opinion, Watanabe-Ribaudo-Behrens teaches Elements 2[a]/51[a]. *See* Section XI.B.2.i.

- (3) **Elements 2[b]/51[b]: [receiving, at the wireless device, via a short range wireless protocol,]/[process] a second plurality of beacon transmissions, [received at the wireless device via the Bluetooth wireless protocol,] each of the [second plurality of] beacon transmissions comprising three fields (a) a MAC address, (b) a unique identifier, wherein the unique identifier of each respective beacon transmission does not directly identify a location of a beacon transmitter, and (c) a beacon service identifier, wherein the beacon service identifier of each respective beacon transmission identifies that the unique identifier is relevant to stored information associated with a wireless beacon service, wherein the stored information is not accessible to the wireless device utilizing the [short range]/[Bluetooth] wireless protocol;**

190. In my opinion, Watanabe-Ribauda-Behrens teaches Elements 2[b]/51[b]. *See* Section XI.B.2.i.

- (4) **Elements 2[c]/51[c]: [causing selection of]/[select] one or more of the unique identifiers from the second plurality of beacon transmissions, by filtering the beacon transmissions which include the same particular beacon service identifier indicating that the particular received beacon transmission is associated with the same particular wireless beacon service; and**

191. In my opinion, Watanabe-Ribauda-Behrens teaches Elements 2[c]/51[c]. *See* Section XI.B.2.j.

- (5) **Elements 2[d]/51[d]: [taking]/[perform a] second further action relating to the stored information, if a second unique identifier is present among the one or more unique identifiers selected from the second plurality of beacon transmissions, wherein the first unique identifier and the second unique identifier are both associated with the same particular entity or object, and wherein the second unique identifier is not equal to the first unique identifier, and further wherein the received beacon transmissions including the first and second unique identifiers are received from a same transmitting device.**

192. In my opinion, Watanabe-Ribaudo-Behrens teaches Elements 2[d]/51[d]. *See* Section XI.B.2.k.

- b. **Claims 3/52: The [method]/[computer program product] of claim [2]/[51] wherein the MAC address received in a beacon transmission including the second unique identifier is different from the MAC address received in a beacon transmission including the first unique identifier, but each such beacon transmission includes the same particular beacon service identifier, and wherein a plurality of beacon transmissions including the particular [beacon] service identifier and the first unique identifier are received in the first time period, and no beacon transmissions including the same [particular] service identifier and the second unique identifier are received in the first time period.**

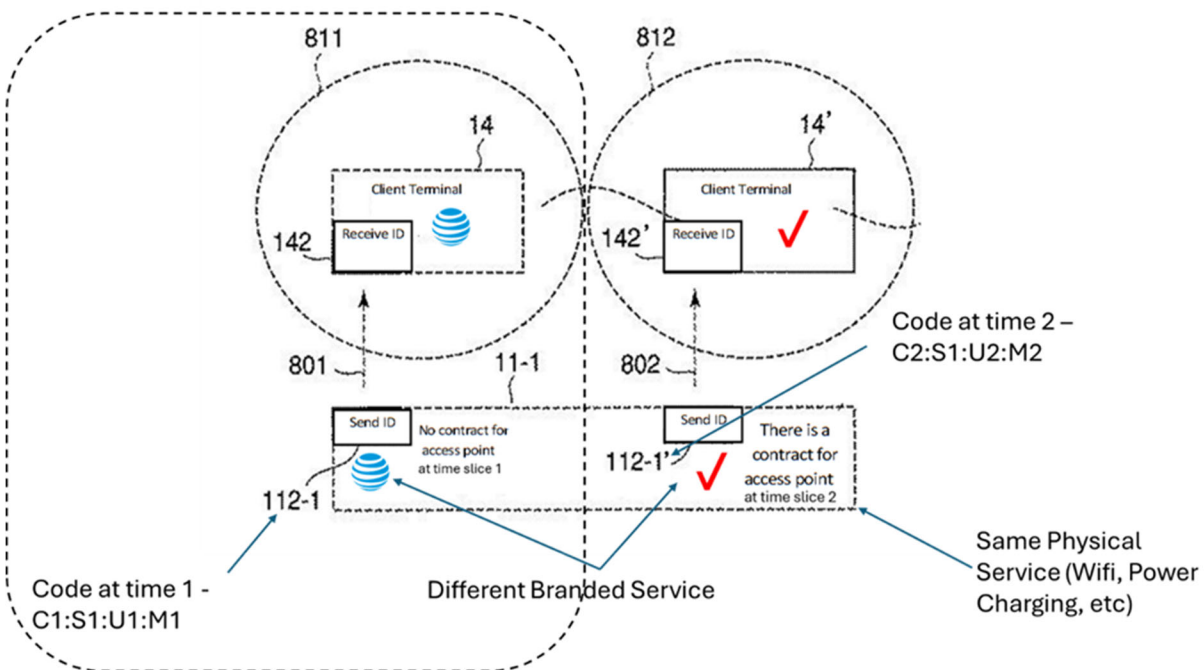
193. In my opinion, Watanabe-Ribaudo-Behrens teaches Claims 3 and 52.

- (1) **MAC address received in beacon transmission including the second unique identifier is different from MAC address received in beacon transmission including the first unique identifier but each beacon transmission includes the same beacon service identifier**

194. Watanabe-Ribaudo-Behrens teaches this limitation for the reasons explained in Section XI.B.2.1.

- (2) **A plurality of beacon transmissions including the particular service identifier and the first unique identifier are received in the first time period**

195. As explained in Sections XI.A.2.b and XI.B.2.e, the first plurality of beacon transmissions received during the first time period include the codes C1:S1:U1:M1, as shown in the annotated figure below.



196. See also Ex-1007 ¶72 (teaching “time-slicing to join and bounce

between several networks”).

(3) No beacon transmissions including the same service identifier and the second unique identifier are received in the first time period

197. As explained in Section XI.B.2.i, the plurality of beacon transmissions sent during the *second* time period include the identifiers C2:S1:U2:M2, whereas the beacon transmissions sent during the *first* time period include the identifiers C1:S1:U1:M1. Thus, unique identifier U1 is sent only during the first time period and unique identifier U2 is sent only during the second time period. So no transmissions during the first time period include both the second unique identifier (U2) and the same service identifier (S1).

c. Claims 4/40/53: The [method]/[mobile wireless device]/[computer program product] of claim [3]/[37]/[52] wherein the second further action is based upon a function currently being performed on a device associated with the wireless beacon service.

198. In my opinion, Watanabe-Ribaudo-Behrens teaches Claims 4, 40, and 53 because, as explained in Section XI.B.2.k, Watanabe teaches that activation of the client’s device (i.e., the second further action) is based upon the filter/comparison function currently being performed on the device associated with the wireless beacon service. Specifically, Watanabe teaches that “[w]hen 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 (S503)” and “[i]f the comparison result is *a match*, the client main unit 141 *is started up* (S504).” Ex-1006 ¶47; *see also id.* ¶52 (if “the company codes and service codes *match*, ... the power induction receiver 142 *transmits an activation signal* to the client main unit 141”).

- d. **Claims 5/41/54: The [method]/[mobile wireless device]/[computer program product] of claim [4]/[40]/[53] wherein the function is related to a current phone call, music being played, a video being played, a multi-player game, or a shared application.**

199. In my opinion, Watanabe-Ribaudo-Behrens teaches Claims 5, 41, and 54.

200. Ribaudo teaches that the function is related to a shared application. Ribaudo teaches allowing “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.” Ex-1007 ¶120; *see also id.* ¶¶123, 139 (second user may “acquire application 20 from another user ... to engage in messaging”), 220 (“an [Application Program Interface] API exposed on mobile devices 12 may expose data downloaded to mobile devices 12 to other applications, such as instant messengers, APPLE ITUNES, or any other suitable applications”). Moreover, Ribaudo’s shared application performs a number of functions including

a filter/comparison function to identify a match and authenticate users. Ex-1007

¶¶22 (“application 20 may perform certain functions to facilitate communication with data center 14, completion of user profiles, authentication of users, and other suitable functions described below”), 84 (“the user of mobile device 12a *launches application 20* on mobile device 12a,” which “may attempt to detect other mobile devices 12 in proximity to mobile device 12a” and “[u]sing 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”), 141 (“application 20 ... may access match data 26 stored in memory module 22 of the first user’s mobile device 12 to determine whether the first and second user’s are a match”). In the Watanabe-Ribaudo-Behrens combination, Watanabe’s filter/comparison function on the mobile device would be performed by a shared application, as taught by Ribaudo.

- e. **Claims 6/55: The [method]/[computer program product] of claim [2]/[51] wherein the first or the second further action is [additionally] related to receiving advertising information for presentation to a user of the wireless device, based upon the first or the second unique identifier, or information derived from the first or second unique identifier.**

201. In my opinion, Watanabe-Ribaudo-Behrens teaches Claims 6 and 55.

See Sections XI.A.2.e, XI.B.3.a.5, and XI.A.3.d.

- f. **Claims 7/42/57:** The [method]/[mobile wireless device]/[computer program product] of claim [2]/[37]/[51] wherein one or more of the first further action and the second further action [additionally] includes [causing the wireless device to] receiv[ing]/[e] content from a server based upon information derived from either the first unique identifier or the second unique identifier.

202. In my opinion, Watanabe-Ribaudo-Behrens teaches Claims 7, 42, and 57. *See* Sections XI.A.2.e, XI.B.3.a.5, and XI.A.3.e.

- g. **Claims 8/43/59:** The [method]/[mobile wireless device]/[computer program product] of claim [2]/[37]/[51], wherein the first or second further action [additionally] includes [sending a message] [or] [causing a server to send a message]/[causing the wireless device to send a message] to another device associated with an account related to the first and the second unique identifiers[, or information derived from the first or the second unique identifiers].

203. In my opinion, Watanabe-Ribaudo-Behrens teaches Claims 8, 43, and 59.

204. Ribaudo teaches sending a message to another device associated with an account. Ribaudo teaches that “adaptor 18a may use extensible messaging and presence protocol (XMPP) to relay XML-based messages and presence information between the user of mobile device 12a and the mobile device 12 of a matched user (e.g., mobile device 12b) ... anonymously within their ad-hoc wireless network to determine,” for example “a meeting place or other venue for interaction.” Ex-1007 ¶79. Ribaudo teaches that “adaptor 18a may use the TCP/IP protocol to create a

messaging connection between mobile devices 12a and 12b” but “[o]ther messaging mechanisms, such as short-range radio technologies, Wi-Fi, BLUETOOTH, short messaging services (SMS), voice over Internet protocol (VoIP), push-to-talk, cellular telephone, voicemail, video conferencing ... may also be used.” Ex-1007 ¶79. Moreover, Ribauda teaches that “each message that a user receives containing match data 26 identifying a match may include instructions for replying to the message” and “[i]f a user replies to the message, the message may be sent anonymously to the identified match using, for example, an SMS message routed through data center 14 or another suitable location.” Ex-1007 ¶164.

205. Watanabe teaches that the first or second further action is related to the first and the second unique identifiers or information derived from them for the reasons explained in Sections XI.A.2.e and XI.B.3.a.5. In the Watanabe-Ribauda-Behrens combination, the first or second further action includes sending a message to another device associated with an account, as taught by Ribauda, and the action is related to the first and the second unique identifiers or information derived from them, as taught by Watanabe.

- h. Claim 9: The method of claim 2 wherein following the taking of the first or second further action, a server associated with an account for a user of the wireless device performs a step of sending an email message to an email address associated with the account for the user, the email message relating to the particular entity or object.**

206. In my opinion, Watanabe-Ribauda-Behrens teaches Claim 9. *See* Sections XI.A.2.e, XI.B.3.a.5, and XI.A.3.f.

- i. Claims 10/44/62: The [method]/[mobile wireless device]/[computer program product] of claim [2]/[37]/[51] wherein the second further action [additionally] includes [causing the wireless device to] prevent[ing] sending of the second unique identifier or information derived from the second unique identifier by the [mobile] wireless device to at least one of the one or more servers.**

207. In my opinion, Watanabe-Ribauda-Behrens teaches Claims 10, 44, and 62.

208. Behrens teaches preventing sending of the second unique identifier or information derived from the second unique identifier by the wireless device to the one or more servers. 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.

209. Watanabe teaches that the second further action is related to the second unique identifier for the reasons explained in Section XI.B.3.a.5. In the Watanabe-Ribaudo-Behrens combination, the second further action involving the second unique identifier, as taught by Watanabe, includes preventing sending of the second unique identifier or information derived from the second unique identifier by the wireless device to at least one of the one or more servers, as taught by Behrens.

- j. Claims 14/66: The [method]/[computer program product] of claim [2]/[51] wherein the [computer program instructions, when executed by the one or more processors in the wireless device, further cause the wireless device to: receive] stored information [is received] at the wireless device from at least one of the one or more servers prior to performing one or more of the first and the second further action.**

210. In my opinion, Watanabe-Ribaudo teaches Claims 14 and 66 for the reasons explained in Sections XI.B.3.a.3 (receiving stored information at the wireless device from the server relating to a second plurality of beacon transmissions with a second unique identifier), XI.B.3.a.4 (selecting a unique identifier(s) by filtering), and XI.B.3.a.5 (taking second further action relating to the stored information if the second unique identifier is present among the selected unique

identifier(s)). *See also* Section XI.A.3.b.

- k. Claims 16/68: The [method]/[computer program product] of claim [2]/[51] wherein all beacon transmitter devices participating in the particular wireless beacon service have the same particular beacon service identifier.**

211. In my opinion, Watanabe-Ribaudo-Behrens teaches Claims 16 and 68. *See* Section XI.A.2.b. Ex-1006 ¶40 (“AP control unit 11-1 controls services S1, S2, and **S3**,” “AP control unit 11-2 controls services S2 and **S3**,” and “AP control unit 11-3 controls service **S3**”).

- l. Claim 18: The method of claim 2 wherein the steps performed at the wireless device are performed as a result of an application program executing on the wireless device.**

212. In my opinion, Watanabe-Ribaudo-Behrens teaches Claim 18.

213. Ribaudo teaches that the steps performed at the wireless device are as a result of an application program executing on the wireless device. Ribaudo teaches that “the user of mobile device 12a launches application 20 on mobile device 12a,” which “may attempt to detect other mobile devices 12 in proximity to mobile device 12a” by using match data “(e.g., the match IDs) downloaded from data center 14” and beaconing “data such as the client ID of the user associated with mobile device 12a.” Ex-1007 ¶84; *see also id.* ¶¶120 (“application 20 installed on mobile devices 12 may provide certain functionality associated with the operation of system 10”), 123 (“application 20 may beacon an SSID of ‘proprietor_name.net’”). In the

Watanabe-Ribaudo-Behrens combination, Ribaudo's application would be installed and executed on Watanabe's wireless device to perform the recited steps.

- m. Claims 19/72: The [method]/[computer program product] of claim [2]/[51] wherein the second further action is [additionally] related to either a product tied to a location or an advertisement tied to a location.**

214. In my opinion, Watanabe-Ribaudo-Behrens teaches Claims 19 and 72.

See Sections XI.A.3.g and XI.B.3.a.5.

- n. Claims 22/48/75: The [method]/[mobile wireless device]/[computer program product] of claim [2]/[37]/[51] wherein the second further action [additionally] includes [causing the wireless device to] allow[ing] a user associated with the [mobile] wireless device to [be provided] access to an object or device associated with the wireless beacon service.**

215. In my opinion, Watanabe-Ribaudo-Behrens teaches Claims 22, 48, and 75.

216. Watanabe teaches that “the user of the client terminal 14 and the service provider that is to carry out the service, such as providing information using the access point 11, enter into a contract for receiving services.” Ex-1006 ¶37. The user learns “how to access the filtering identification information notification unit 13 to acquire the identification information necessary for filtering in order to receive services based on the contract.” Ex-1006 ¶37. Therefore, the second further action (i.e., activation of the device), includes allowing a user associated with the wireless device to be provided access to an object or device associated with the wireless

beacon service. Ex-1006 ¶44 (“This enables the client terminal 14 to receive, thereafter, the contracted services through the access point 11.”).

217. Ribauda also teaches this claim. Ribauda teaches that “[m]obile device 12 may notify its user if such a match is detected in proximity, allowing the user to initiate an interaction with the detected match if desired.” Ex-1007 ¶26; *see also id.* ¶79 (“If both users are interested in the match, mobile devices 12a and 12b may use the XMPP-enabled adaptor 18 to message anonymously within their ad-hoc wireless network to determine a meeting place or other venue for interaction.”).

- o. Claims 23/35/49/76: The [method]/[mobile wireless device]/[computer program product] of claim [2]/[3]/[37]/[51] wherein the [taking]/[first or] second further action additionally comprises: controlling further communications between the [mobile] wireless device and at least one device or server associated with an entity or object in proximity to the wireless device [based upon information derived from the first or second unique identifier].**

218. In my opinion, Watanabe-Ribauda-Behrens teaches Claims 23, 35, 49, and 76. *See* Sections XI.A.2.e, XI.B.3.a.4, and XI.B.2.k. Moreover, Watanabe teaches that “[w]hen the client main unit 141 is started up in this way, the client main unit 141 establishes a communication channel with AP main unit 111, through a publicly known scanning method, to initiate data communication” and “communication is carried out with an access point 11 for which the group information is a match.” Ex-1006 ¶53. Thus, “client terminal 14 is able to carry out

data communication with a server, or the like, of the service provider through the access point 11-2.” *Id.*

- p. Claims 24/82/77: The [method]/[mobile wireless device]/[computer program product] of claim [3]/[37]/[52] [further comprising:]/[wherein the operations further comprise]/[wherein the computer program instructions, when executed by the wireless device, further cause the wireless device to:] receiv[ing]/[e], at the [mobile] wireless device, timing notification information for coordination of active times for beacon transmissions.**

219. In my opinion, Watanabe-Ribaudo-Behrens teaches Claims 24, 82, and 77.

220. Ribaudo teaches receiving, at the wireless device, timing notification information for coordination of active times for beacon transmissions. Ribaudo teaches that “matches may be filtered by time of the detected match in proximity.” Ex-1007 ¶64. For example, a “user of mobile device 12 may wish to be notified of all matches that are currently in proximity or, instead, may wish to also be notified of all matches that were at the same hotspot but at different points in time (e.g., an hour before the user, a day before the user, or at any other suitable length of time).” Ex-1007 ¶64. Ribaudo further teaches that “the user may be open to sharing more information” from the user’s profile(s) based on “the time of day the match is detected” or “one or more network identifiers detected at the time of the detected match.” Ex-1007 ¶78. As an example, “a user at a business conference may be

willing to share greater information from the user's business user profile 24 if a match is detected at one or more MAC addresses of one or more networks existing at the conference." Ex-1007 ¶78. Ribauda also teaches that "[w]hen a user later synchronizes the user's data with data center 14," the "date and time" of a "missed encounter" can be uploaded to the data center. Ex-1007 ¶152. Additionally, match data "may be sent to some or all users who are members of a particular group at a particular time or location." Ex-1007 ¶163. For example, "a conference schedule may include one or more breaks at which it might be appropriate for conference members to converse with one another." *Id.* Match data "may be sent to users during these breaks to facilitate discussions between certain attendees." Ex-1007 ¶163.

- q. Claims 25/83/78: The [method]/[computer program product] of claim [24]/[53]/[77] wherein the [receiving, at the wireless device of the] timing notification information is not [received] directly from the beacon transmitter.**

221. In my opinion, Watanabe-Ribauda-Behrens teaches Claims 25, 83, and 78 for the reasons explained in Section XI.B.3.p. Ribauda further teaches that data center 14 "may compare the information reported for John with information for other users who reported that MAC address at the same or different times." Ex-1007 ¶201. "Mary may then query data center 14 to see what other users were in the coffee shop previously that she knows or with whom she shares something in common" and, if data center 14 considers them a match, "Mary may see John in the results of his

query, possibly with an indication of when he was in the coffee shop.” Ex-1007

¶201. John “now falls within Mary’s time filter.” Ex-1007 ¶201. Ribaudó also teaches that the wireless device’s receipt of the timing notification information is not directly from the beacon transmitter because it is received from the data center not the mobile device. Ex-1007 ¶191 (“mobile devices 12 may be considered reference beacons in the wireless infrastructure of system 10” and “may beacon data that can be used to identify them”).

- r. **Claims 26/38/79: The [method]/[mobile wireless device]/[computer program product] of claim [2]/[37]/[51] [further comprising:]/[wherein the operations further comprise]/[wherein the computer program instructions, when executed by the wireless device, further cause the wireless device to:] us[ing]/[e] the stored information to determine if the second unique identifier is present among the selected one or more of the unique identifiers from the second plurality of beacon transmissions.**

222. In my opinion, Watanabe-Ribaudó-Behrens teaches Claims 26, 38, and 79. *See* Sections XI.B.3.a.3-XI.B.3.a.5 and XI.B.2.i- XI.B.2.k.

- s. **Claims 27/39/81: The [method]/[mobile wireless device]/[computer program product] of claim [1]/[37]/[50] wherein [the]/[each] MAC address [or a respective beacon transmission] is a randomly generated 48 bit number matching a format of a Bluetooth BD_ADDR.**

223. In my opinion, Watanabe-Ribaudó-Behrens teaches Claims 27, 39, and 81.

224. Ribauda teaches 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 Specification v.2.0 + EDR), 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. Behrens further teaches that “[i]n the case of Bluetooth, various address parts and lengths (e.g., *48-bit BD_ADDR*, 24-bit LAP, etc.), Friendly Names, as well as a combination thereof may be used.” Ex-1008, 19:12-14.

225. While Ribauda 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 Watanabe-Ribauda-Behrens system. First, it was well-known in the art that a Bluetooth MAC address may be configured to be either a static, public address, or else a randomly-generated address that changes periodically, as a privacy-enhancing option. Second, Ribauda itself teaches that “substantial privacy” may be an important consideration for its wireless system. Ex-1007 ¶226. *See*, for example, Huang, L., Matsuura, K., Yamane, H., & Sezaki, K., “Enhancing wireless location

privacy using silent period,” in *IEEE Wireless Communications and Networking Conference*, 2005 (Vol. 2, pp. 1187-1192) (Mar. 2005) (Ex-1042). 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.

t. Claim 28: The method of claim 3 wherein the short range protocol is derived from Bluetooth.

226. In my opinion, Watanabe-Ribaudó-Behrens teaches Claim 28. See Section XI.A.2.b. Ex-1006 ¶27 (“short- and medium-distance wireless communication devices, such as wireless LANs, wireless communication devices based on Bluetooth ... are ... the first communication means”).

- u. Claim 46: The mobile wireless device of claim 37 wherein the operations further comprise: using the stored information to determine if the first unique identifier is present among the first selected one or more unique identifiers.**

227. In my opinion, Watanabe-Ribauda-Behrens teaches Claim 46. *See* Section XI.A.3.c.

- v. Claim 58: The computer program product of claim 52 wherein the first further action additionally includes causing the wireless device to receive content from a server based upon information derived from the first unique identifier.**

228. In my opinion, Watanabe-Ribauda-Behrens teaches Claim 58. *See* Section XI.B.3f.

- w. Claim 60: The computer program product of claim 51, wherein the computer program instructions, when executed by the one or more processors in the wireless device, further cause the wireless device to: after the first or second further action: send information to a server associated with an account for a user of the wireless device, to enable the server to send a message to an email address associated with the account for the user.**

229. In my opinion, Watanabe-Ribauda-Behrens teaches Claim 60. *See* Sections XI.A.3.f and XI.B.3.h.

XII. CONCLUSION

230. For the reasons above, it is my opinion that Claims 1-10, 12-16, 18-19, 22-31, 34-44, 46, 48-62, 64-68, 72, and 75-83 of the '971 Patent are obvious based on each of the grounds specified in my Declaration.

231. 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

A handwritten signature in black ink, appearing to read 'S Rangan', written over a horizontal line.

Dr. Sundeep Rangan