

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner

v.

SECURE COMMUNICATION TECHNOLOGIES, LLC,
Patent Owner

Case IPR2026-00447
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**

Mail Stop "PATENT BOARD"

Patent Trial and Appeal Board
U.S. Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	BACKGROUND AND QUALIFICATIONS	2
III.	INFORMATION CONSIDERED	4
IV.	RELEVANT LEGAL STANDARDS	5
A.	Claim Interpretation	5
B.	Perspective of One of Ordinary Skill in the Art.....	5
C.	Obviousness.....	6
V.	LEVEL OF ORDINARY SKILL IN THE ART	9
VI.	SUMMARY OF MY OPINIONS	10
VII.	TECHNOLOGICAL BACKGROUND	11
A.	Using Beacon Transmissions to Make Proximity Determinations Was Known	11
B.	The Use of MAC Addresses, Unique Identifiers, and Beacon Service Identifiers to Identify Devices and Networks Was Known	16
C.	Including Identifiers in Beacon Transmissions Was Known.....	29
D.	Periodic Transmission of a Beacon Signal Was Known.....	37
E.	Storing Information at Servers and Mobile Devices Communicating with Servers to Obtain Stored Information Was Known	40
F.	Filtering Beacon Transmissions by Comparing Stored Information to Transmitted Information to Determine Matches Was Known	47
G.	Taking Action if a Match is Determined Between the Stored Information and the Transmitted Information Was Known.....	50
H.	Using Protocols Such as Bluetooth and Cellular for Communications Between Mobile Devices and Servers Was Known	55
I.	Using A Processor and Memory with Instructions to Execute Functions on Mobile Devices Was Known.....	60

VIII. THE '971 Patent AND ITS FILE HISTORY.....	65
IX. CLAIM CONSTRUCTION	70
X. OVERVIEW OF THE APPLIED PRIOR ART REFERENCES	70
A. Ribaudo (EX1007)	70
B. Watanabe (EX1005, EX1006).....	73
C. Behrens (EX1008).....	76
D. Nordman (EX1046).....	78
XI. DETAILED EXPLANATION OF THE UNPATENTABILITY GROUNDS	80
A. Ground 1: Claims 1, 11-13, 15, 20, 29-32, 34, 36, 50, 56, 61, 63-65, 67, 70, 73, and 80 are obvious over Ribaudo in view of Watanabe.	80
1. A POSITA would have been motivated to combine Ribaudo's teachings with Watanabe's teachings and would have had a reasonable expectation of success.	80
2. Independent Claims 1 and 50.....	86
(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:.....	86
(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;	87
(i) Receiving at a wireless device a first plurality of beacon transmissions via Bluetooth	88
(ii) Overview of beacon transmission components.....	93
(iii) MAC address.....	95
(iv) Unique identifier.....	96
(v) Beacon service identifier.....	97
(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;	103
(i) Receiving at the wireless device stored information from a server.....	103
(ii) Using a second wireless protocol different from Bluetooth	105
(iii) Stored information relates to an entity or object associated with a first unique identifier	108
(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	109
(i) Filtering the beacon transmissions that include a particular beacon service identifier	110
(ii) Selecting one or more unique identifiers from the beacon transmissions	113
(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.	115
3. Dependent Claims 11-13, 15, 20, 29-32, 34, 36, 56, 61, 63-65, 67, 70, 73, and 80	119
(a) Claims 11/32/63: The [method]/[computer program product] of claim [1]/[50] wherein the [taking] first further action [further comprises]/[additionally includes]: [causing the wireless device to] [determine]/[determining], based upon at least a portion of the stored information, that at least one beacon transmitter is associated with a predetermined location.....	119
(b) 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].	122
(c) 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 of]/[performing] the first further
action.....125

(d) 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]. 126

(e) Claim 20/73: The [method]/[computer program
product] of claim [1]/[50] wherein the first further
action [additionally] includes [causing the wireless
device to determine]/[determining] an address or
location associated with the wireless device based
at least in part upon the first unique identifier
being associated with a pre-determined location,
and wherein the wireless device is located indoors
where a GPS signal may not be available. 127

(f) 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. 129

(g) 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. 130

(h) 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
(i)	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.	135
(j)	Claim 70: The computer program product of claim 50 wherein the first further action additionally includes causing the wireless device to display a current location, based at least in part upon a predetermined location associated with the first unique identifier, or based at least in part upon information derived from the first unique identifier.....	135
B.	Ground 2: Claims 2-10, 14, 16-19, 21-26, 28, 33, 35, 37-38, 40-49, 51-55, 57-60, 62, 66, 68-69, 71-72, 74-79, and 82-83 are obvious over Watanabe in view of Ribaud and Behrens.	137
1.	A POSITA would have been motivated to combine Ribaud-Watanabe’s teachings with Behrens’ teachings and would have had a reasonable expectation of success.....	138
2.	Independent Claim 37	142
(a)	Element 37[pre]: A mobile wireless device comprising:	142
(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;	144
(c)	Element 37[b]: one or more processors; and.....	146
(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:	147

- (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; 150
- (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; 153
- (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; 154
- (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; 154
- (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;.....155

(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;.....157

(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 159

(i) 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.....160

(ii) 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 160

- (iii) Received beacon transmissions including the first and second unique identifiers are received from a same transmitting device.....162
- (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.....164
 - (i) 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 164
 - (ii) Each beacon transmission includes the same particular beacon service identifier 166
- 3. Dependent Claims 2-10, 14, 16-19, 21-26, 28, 33, 35, 38, 40-49, 51-55, 57-60, 62, 66, 68-69, 71-72, 74-79, and 82-83.....167
 - (a) Claims 2 and 51 167
 - (i) 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 167
 - (ii) Elements 2[a]/51[a]: [wherein the method further comprises,] during a second time period:.....168

- (iii) 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; 168
- (iv) 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 168
- (v) 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.....169

- (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.....169
- (i) 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 170
- (ii) A plurality of beacon transmissions including the particular service identifier and the first unique identifier are received in the first time period 170
- (iii) No beacon transmissions including the same service identifier and the second unique identifier are received in the first time period....171
- (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. 171
- (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.....172
- (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.....174
- (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.....174
- (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].....175
- (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.....176

- (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. 177
- (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. 180
- (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. 181
- (l) Claims 17/33/45/69: The [method]/[computer program product]/[mobile wireless device] of claim [2/37/51] wherein [at least one of] the [first or] second further action comprises: determining[, based upon at least a portion of the stored information,] that the beacon transmitter is associated with a predetermined location.....182
- (m) 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.....183
- (n) 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.....184
- (o) Claims 21/47/74: The [method]/[mobile wireless device]/[computer program product] of claim [2]/[37]/[51] wherein the second further action includes [causing the wireless device to determine]/[determining] an address or location associated with the wireless device based at least in part upon the second unique identifier being associated with a pre-determined location, wherein the wireless device is located indoors where a GPS signal may not be available. 184
- (p) 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. 184
- (q) 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]. 185
- (r) 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.....	187
(s)	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.....	189
(t)	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.....	189
(u)	Claim 28: The method of claim 3 wherein the short range protocol is derived from Bluetooth.....	190
(v)	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.....	190
(w)	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.	190
(x)	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.....	191
(y)	Claim 71: The computer program product of claim 51 wherein the second further action additionally includes causing the wireless device to display a current location on the wireless device, based at least in part upon a predetermined location associated with the second unique identifier, or based at least in part upon information derived from the second unique identifier.....	191
C.	Ground 3: Ribaud-Watanabe-Behrens-Nordman Renders Obvious Claims 27, 39, and 81	191
XII.	CONCLUSION.....	1

LIST OF MATERIALS CONSIDERED

Exhibit No.	Description
1001	U.S. Patent No. 11,687,971 (“the ’971 patent”)
1003	<i>Curriculum Vitae</i> of Dr. Sundeep Rangan
1004	Prosecution History of U.S. Patent No. 11,687,971
1005	Japanese Patent Application Publication No. 2005/12973 to Watanabe
1006	Certified English-language translation of Japanese Patent Application Publication No. 2005/12973 to Watanabe (“Watanabe”)
1007	U.S. Patent Application Publication No. 2007/0030824 to Ribaudó (“Ribaudó”)
1008	International Patent Application Publication No. WO2008/132241 to Behrens (“Behrens”)
1009	International Patent Application Publication No. WO2008/076827 to Krikorian (“Krikorian”)
1010	U.S. Patent Application Publication No. 2005/00174975 to Mgrdechian (“Mgrdechian”)
1011	Declaration of James A. Proctor, Jr., filed April 20, 2020 in U.S. Patent Application No. 15/271,410
1012	U.S. Patent Application Publication No. 2002/0116494 to Kocol (“Kocol”)
1021	Bluetooth Specification v.2.0 + EDR (Nov. 2004) (“Bluetooth Specification v.2.0 + EDR”)
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”)

Exhibit No.	Description
1026	IEEE 802.15 Specification IEEE Standard 802.15.1, Part 15.1: Wireless medium access control and physical layer (PHY) specifications for wireless personal area networks (WPANs) (June 2005) (“Bluetooth Specification”)
1027	U.S. Patent No. 7,000,001 to Lazaridis et al. (“Lazaridis”)
1028	U.S. Patent Application Publication No. 2009/0239467 to Gulin et al. (“Gulin”)
1029	U.S. Patent Application Publication No. 2004/0248569 to Kondou et al. (“Kondou”)
1030	U.S. Patent Application Publication No. 2006/0287813 to Quigley et al. (“Quigley”)
1031	U.S. Patent Application Publication No. 2005/0130634 to Godfrey (“Godfrey”)
1032	Jansen et al., “Proximity Beacons and Mobile Device Authentication,” <i>National Institute of Standards and Technology</i> , (June 2005) (“Jansen”)
1033	U.S. Patent Application Publication No. 2003/0220114 to Langensteiner et al. (“Langensteiner”)
1034	U.S. Patent Application Publication No. 2008/0261526 to Suresh (“Suresh”)
1035	U.S. Patent Application Publication No. 2009/0059878 to Tamura (“Tamura”)
1036	U.S. Patent No. 8,411,662 (“Saund”)
1037	U.S. Patent Application Publication No. 2008/0045181 to Suzuki (“Suzuki”)
1038	International Patent Application Publication No. WO2006/028640 to Briancon et al. (“Briancon”)

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

I. INTRODUCTION

1. My name is Sundeeep 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 Apple 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 1-83 of U.S. Patent No. 11,687,971 (“the ’971 patent”) (EX1001), 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 \$750 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 EX1003.

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. In my work as a professor and entrepreneur, I worked with graduate students and others who had the

knowledge and experience of a POSITA in 2008, and I am able to render opinions from the perspective of a POSITA based on that knowledge and experience. My opinions concerning the '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 1-83 of the '971 patent would have been obvious under 35 U.S.C. §103 on the following grounds:

- **Ground 1:** Claims 1, 11-13, 15, 20, 29-32, 34, 36, 50, 56, 61, 63-65, 67, 70, 73, and 80 are obvious over U.S. Patent Application Publication No. 2007/0030824 to Ribauda ("Ribauda") (EX1007) in view of Japanese Patent Application Publication No. 2005/12973 to Watanabe ("Watanabe") (EX1005, EX1006);
- **Ground 2:** Claims 2-10, 14, 16-19, 21-26, 28, 33, 35, 37-38, 40-49, 51-55, 57-60, 62, 66, 68-69, 71-72, 74-79, and 82-83 are obvious over Watanabe in view of Ribauda and PCT Patent Publication No. WO2008/132241 to Behrens ("Behrens") (EX1008);
- **Ground 3:** Claims 27, 39, and 81 are obvious over Ribauda in view of Watanabe, Behrens, and U.S. Patent Application Publication No. 2002/0174364 to Nordman *et al.* ("Nordman").

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. EX1009, ¶¶4-5, FIG. 2.

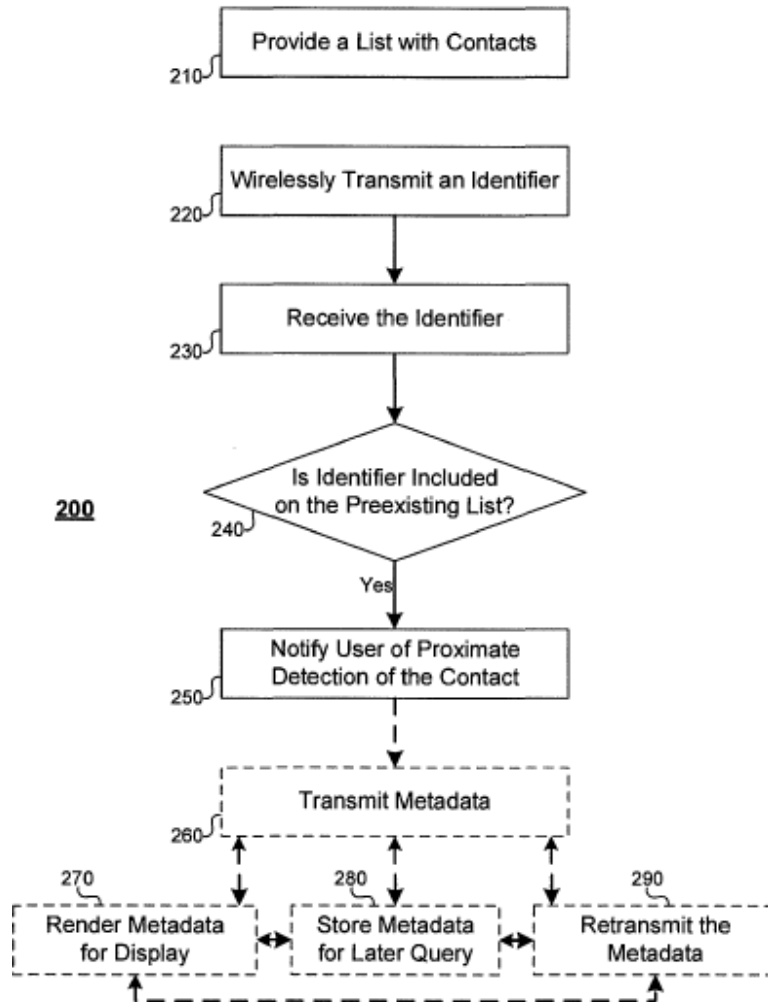


Fig. 2

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.” EX1009, ¶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.” EX1009, ¶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.” EX1009, ¶25.

30. As another example, U.S. Patent No. 7,000,001 to Lazaridis *et al.* (EX1027) 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.” EX1027, 2:3-10. “This transmission may be a continuous transmission, or may be configured to transmit at a periodic interval.” EX1027, 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.” EX1027, 3:59-65.

31. Similar methods and systems are also taught by U.S. Patent

Application Publication No. 2009/0239467 to Gulin *et al.* (EX1028). 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 near-field 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.” EX1028, Abstract. “Based on the information exchanged, the users can determine whether a relationship between the users exists or might be created.” EX1028, Abstract.

32. *See also* U.S. Patent Application Publication No. 2004/0248569 to Kondou *et al.* (EX1029), ¶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.”); U.S. Patent Application Publication No. 2005/0174975 to Mgrdechian (EX1010), ¶73 (“Referring again to FIG. 3A, the process may be initiated when an initiating user (e.g., User A) 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.”); EX1030, 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.”); EX1033, ¶¶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.” EX1009, ¶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 an

other 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." EX1009, ¶23, FIG. 3; *see also* EX1029, ¶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 U.S. Patent Application Publication No. 2005/0130634 to Godfrey (EX1031). 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.” EX1031, ¶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.” EX1031, ¶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.” EX1031, ¶55.

35. *See also* Wayne Jansen et al., “Proximity Beacons and Mobile Device Authentication,” NISTIR 7200 (June 2005) (EX1032), 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.”); EX1033, ¶38 (“the system suitably correlates the mobiles’ Bluetooth device ID’s with their wide-area addresses (phone nos.), for example by pre-registration”); U.S. Patent Application Publication No. 2008/0261526 to Suresh (EX1034), ¶¶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)."); EX1028, ¶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.”);

EX1010, ¶¶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, U.S. Patent Application Publication No. 2009/0059878 to Tamura (EX1035) 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.” EX1035, ¶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 sub-APs are virtually multiplexed to the AP 10 to perform actual communication with terminals 20, 22 and 24. The sub-AP1, sub-AP2 and sub-AP3 can perform encryption communication with encryption schemes independently selected for the respective sub-AP1, sub-AP2 and sub-AP3.” EX1035, ¶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.” EX1035, ¶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.” EX1035, ¶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.” EX1035,
¶173.

38. *See also* Sorte et al., “Service publishing to support an efficient network selection in an 802.11 multi-access environment,” January 2006 (EX1039), 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.”); U.S. Patent No. 8,411,662 to Saund et al. (EX1036, “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. A 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.”); U.S. Patent

Application Publication No. 2008/0045181 to Suzuki (EX1037), ¶¶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.”); International Patent Application Publication No. WO2006/028640 to Briancon et al. (EX1038), ¶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, 16₃, 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 1 12₁ (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 (VAP). The use of VAPs 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.” EX1009, Abstract, ¶4. “The method includes wirelessly transmitting, by a first device, an identifier associated with a user of the first device.” EX1009, ¶5. “The identifier can be a unique ID. The identifier can be a standardized ID.” EX1009, ¶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).” EX1009, ¶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.” EX1027, 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.” EX1027, 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 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.” EX1027, 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.” EX1027, 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.”

EX1010, ¶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.” EX1010, ¶14. U.S. Patent Application Publication No. 2005/0174975 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.”

EX1010, ¶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.” EX1010, ¶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.” EX1010, ¶28. “In another embodiment, a device may continuously or intermittently broadcast its ID and/or other information without having received an inquiry.” EX1010, ¶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.” EX1037, ¶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.” EX1037, ¶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.” EX1037, ¶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.” EX1037, ¶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.” EX1037, ¶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.” EX1037, ¶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.” EX1037, ¶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.” EX1037, ¶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.” EX1037, ¶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.” EX1037, ¶83, Figs. 10-11.

43. *See also* U.S. Patent No. 6,928,263 to Blake et al. (EX1040), 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.”); EX1033, ¶14 (“The system may comprise a plurality of second beacon devices, each arranged to receive identifiers from the first beacon.”); EX1030, ¶¶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”); EX1039, 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)) (hereinafter the “Bluetooth Specification,” EX1026) 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.” EX1026, 5, 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.” EX1026, 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.” EX1026, 132.

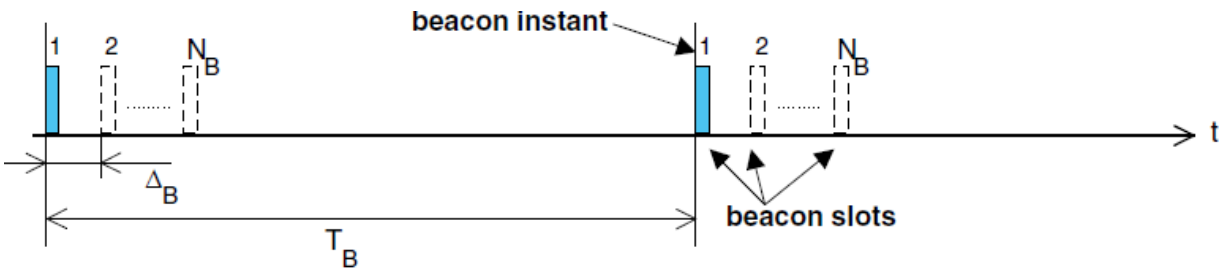


Figure 72—General beacon train format

EX1026, 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)) (EX1025, hereinafter the “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.” EX1025, 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.

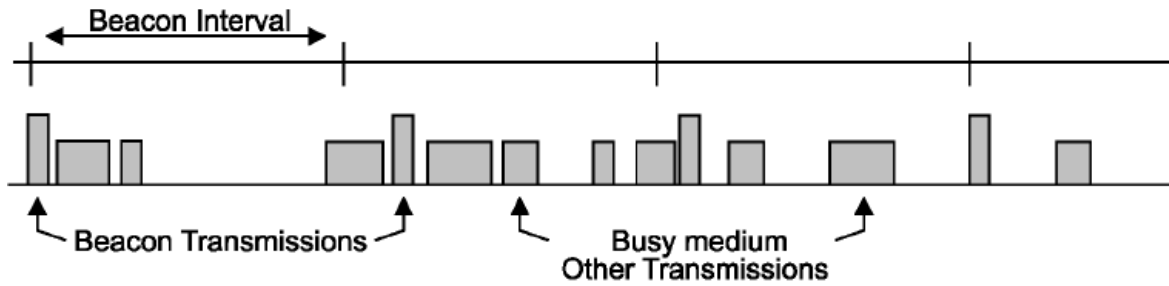


Figure 11-1—Beacon transmission on a busy network

EX1025, 420 (FIG. 11-1).

47. Details regarding the “Beacon frame format” are provided in Table 7-8 of the specification. EX1025, 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.” EX1009, ¶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. In 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).” EX1009, ¶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).”

EX1027, 2:11-23. “[B]ookmark beacon 12 could be used independently to communicate information, such as an advertisement, to a nearby wireless device 14.” EX1027, 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.” EX1027, 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.” EX1027, 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.” EX1010, ¶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.” EX1010, ¶20. “In one embodiment, the wireless device identifications and information are stored in a database accessible over the Internet.” EX1010, ¶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.” EX1010, ¶75.

51. *See also* EX1039, 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.”); EX1028, ¶¶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.”); EX1029, ¶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.” EX1031, ¶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.” EX1009, ¶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.” EX1009, ¶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).” EX1009, ¶26.

54. *See also* EX1032, 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.”); EX1031, ¶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 identify associated with the user of the second wireless device with a set of one or more predetermined identities; and notifying a user of the first wireless device that the user of a proximity of the user of the Second wireless device based on the comparison of the identity with the set of one or more predetermined identities.”).

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

55. Taking some sort of action if a match is determined to be present between stored information at the mobile device and information transmitted in a beacon transmission was known by 2008. For example, Krikorian teaches “notifying a user of the mobile first device, if the identifier is included on the preexisting list, that the user associated with the identifier is in proximity to the mobile first device.” EX1009, 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.” EX1009, ¶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.” EX1009, ¶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.” EX1009, ¶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.” EX1027, 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.” EX1027, 4:31-53; *see also* EX1027, 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* EX1039, 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).”); EX1040, 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.”); EX1010, ¶¶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 predefined 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. User’s [sic] 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.” EX1010, ¶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.” EX1010, ¶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.” EX1027 (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.” EX1027, 2:55-3:5.

60. *See also* EX1028, ¶¶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.).”); EX1040, 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.”); EX1033, ¶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.”); EX1009, ¶¶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.” EX1009, ¶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.” EX1009, ¶¶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.” EX1009, ¶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.

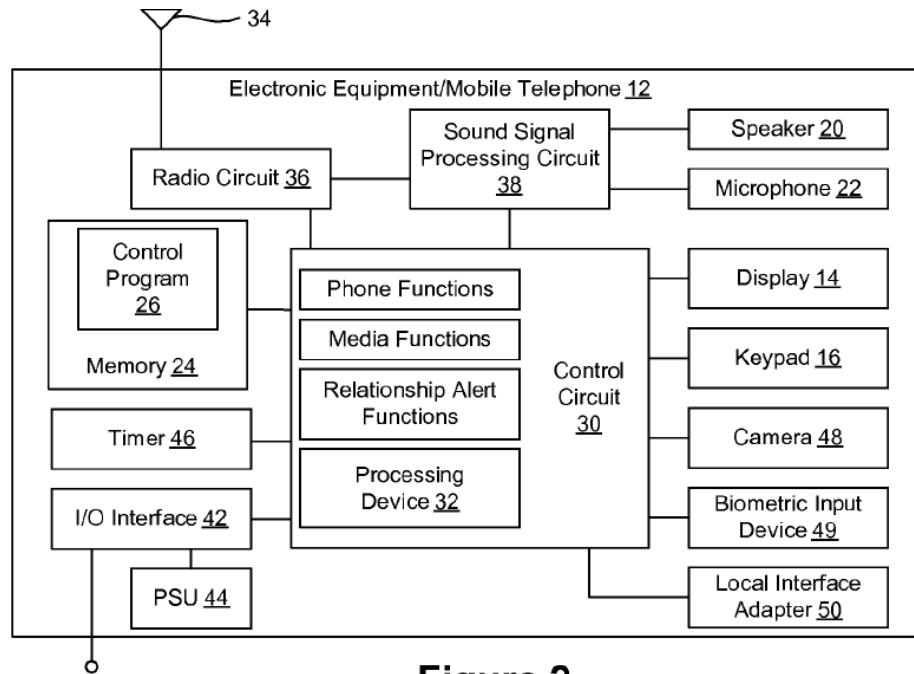


Figure 2

EX1028, FIG. 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.” EX1028, ¶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.” EX1028, ¶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.” EX1028, ¶80.

63. *See also* EX1029, ¶¶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 describes techniques for mobile wireless devices (e.g., cellular phones) in proximity with one another to exchange information utilizing both a short range, first wireless capability and a second wireless capability that allows the devices “to communicate with a central server via the internet.” EX1001, 1:49-63. The '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. EX1001, 1:11-36. In this manner, the '971 Patent indicated that conventional cellular phones supported “at least two wireless standards.” EX1001, 1:11-36. The

'971 patent describes using these two wireless capabilities to broker the exchange of information between two wireless devices. EX1001, 1:51-63.

65. As seen from Figure 1, which I have annotated 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. EX1001, 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). EX1001, 4:36-47.

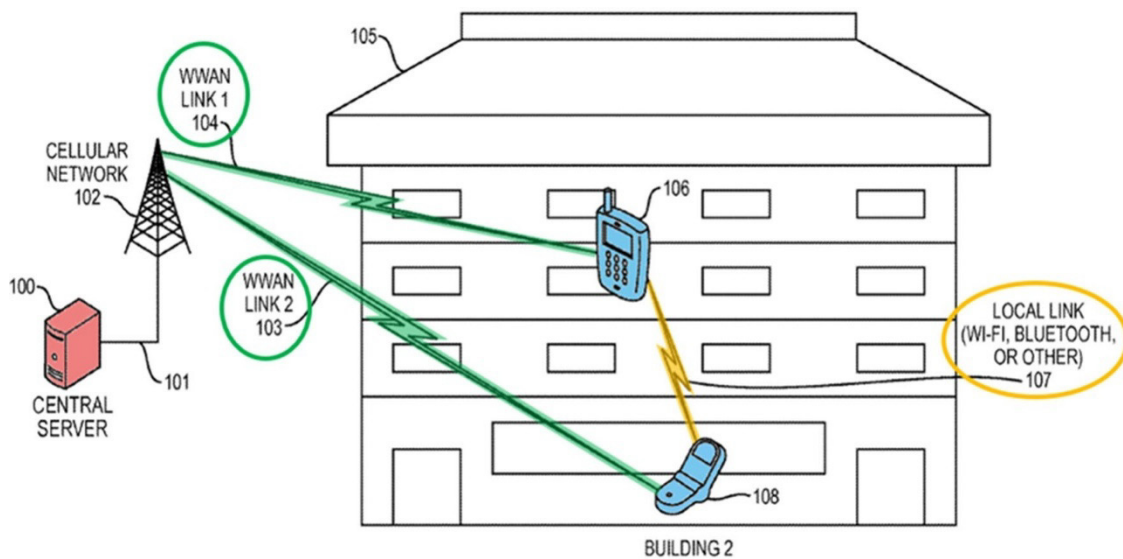


Figure 1

EX1001, FIG. 1 (annotated).

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

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. EX1001, Abstract, 1:49-67. As shown in Figure 6, the beacon transmissions include a MAC address (i.e., a hardware address/identifier) and a basic service set identifier (BSSID) or ad-hoc network name (SSID), where “one or both [of] the BSSID and the SSID may be used to indicate these particular beacons are associated with a [given] service.” EX1001, 8:25-38, FIG. 6 (annotated). I note that while Figure 6 provides an example of multiple identifiers, the '971 patent does not explicitly define the claim terms *beacon service identifier* or *unique identifier* that I discuss further in my declaration below.

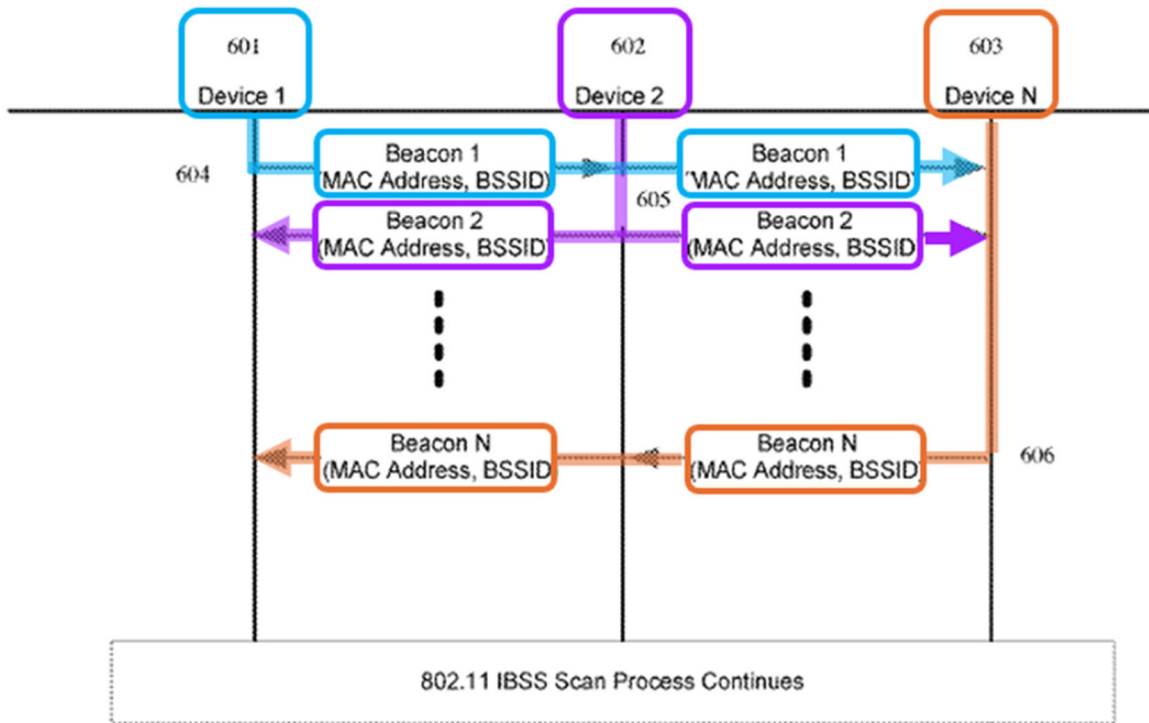


Figure 6 - 802.11 IBSS Beacon Process

EX1001, FIG. 6 (annotated).

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. EX1004, 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.’” EX1004, 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.” EX1004, 114. On April 24, 2023, the Examiner issued a Notice of Allowance without making any prior art rejections during prosecution. EX1004, 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.” EX1004, 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 1-83 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

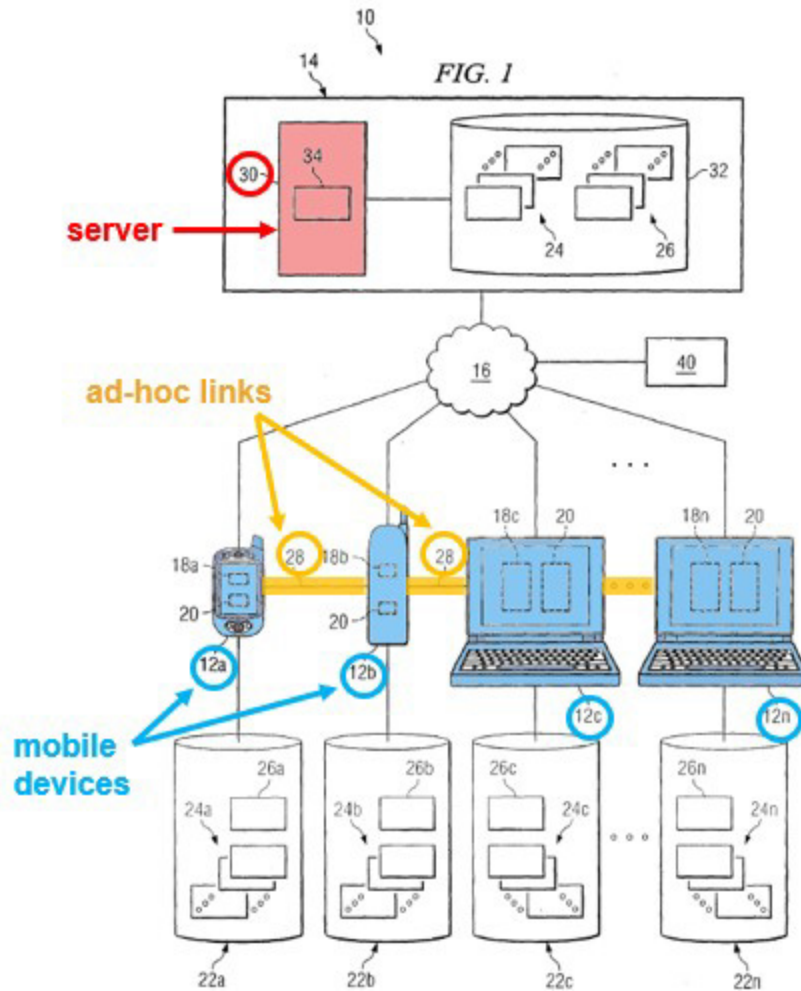
72. Each of the references that I discuss below (Watanabe, Ribaud, Behrens, and Nordman) are analogous to the '971 patent. Specifically, each of the references are in the same field of the '971 patent (facilitating the exchange of information between devices via short range and long range wireless communications), are reasonably pertinent to the problems described in the '971 patent (detecting wireless devices in close proximity to exchange information), or are both. *See* EX1001, 1:7-10, 1:37-2:11.

A. Ribaud (EX1007)

73. Ribaud (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 Ribaud is §102(b) prior art to the '971 patent.

74. I note that Ribaudo describes mobile devices that detect other mobile devices in proximity using identifiers beacons using a short-range wireless protocol and communicate with a server using a long-range wireless protocol. EX1007, Abstract, ¶¶24-25, 57, 66-67, 79, FIG. 1. Ribaudo teaches “a system and method for providing communication services to mobile device users incorporating proximity determination” in order to facilitate social networking. EX1007, ¶¶2, 8, 29. Specifically, “when the user is in proximity to another user, the user’s mobile device detects the presence of the other user’s mobile device, receives an identifier associated with the detected other user, and compares the received identifier with the pre-processed match data stored on the user’s mobile device to determine whether the other user is one of the user’s predetermined matches.” EX1007, ¶¶6, 223 (“the present invention may connect users based on any desire, relation, affiliation, or other reason”).

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



EX1007, FIG. 1 (annotated).

76. As Ribaudo explains, “a user (e.g., of mobile device 12a) may be associated with one or more client IDs, which may identify the user publicly,” which “may be the unique MAC address[es] of the Wi-Fi NIC of the user’s mobile device[s] 12.” EX1007, ¶68. In operation, the mobile device “may beacon data such as the client ID of the user associated with [the] mobile device” (EX1007, ¶57) and an SSID of a proprietor of system 10. EX1007, ¶123. Moreover, “[t]he

unique MAC address of mobile device 12a may be beacons when the BLUETOOTH interface of mobile device 12a is active.” EX1007, ¶157.

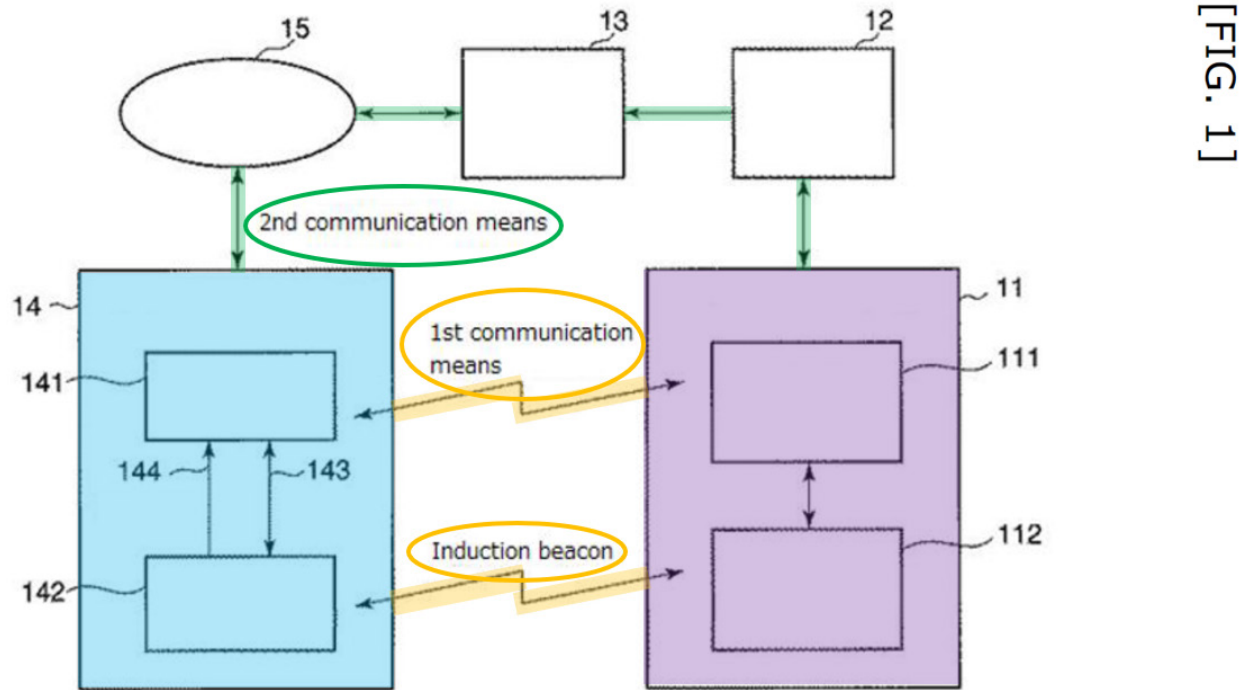
B. Watanabe (EX1005, EX1006)

77. 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 EX1005, which I understand is attached to the Petition as EX1006.

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

communication means” (green) “for communicating ... via the internet 15.”

EX1006, ¶26.

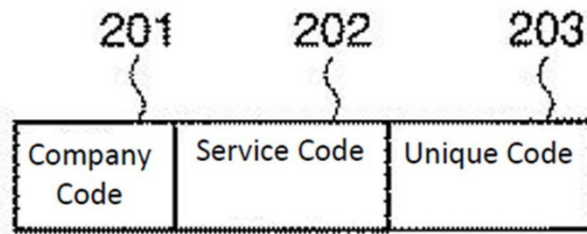


EX1006, FIG. 1 (annotated).

79. As Watanabe explains, “each access point 11 ... generates an induction *beacon* (power supply signal) to supply power ... via the first communication means” and reports “transmitter identification information.”

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

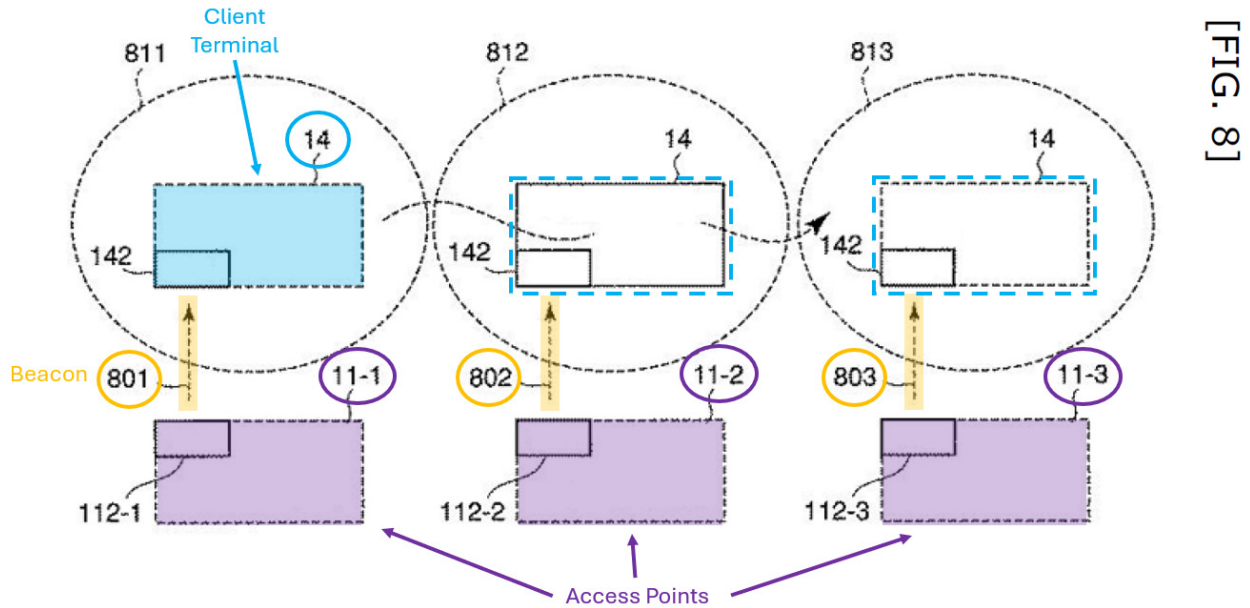
[FIG. 2]



EX1006, FIG. 2.

80. “When the electrical power induction receiver 142 in the client terminal 14 receives a beacon, it extracts the transmitter identification information in the beacon and compares this information with the pre-set filtering identification information,” and, “[i]f the comparison results match, the client main unit 141 is activated.” EX1006, ¶47.

81. 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 supply power to client terminal[] 14” (blue) “within [the] range” of the access point. EX1006, ¶49, FIG. 8.



EX1006, FIG. 8 (annotated).

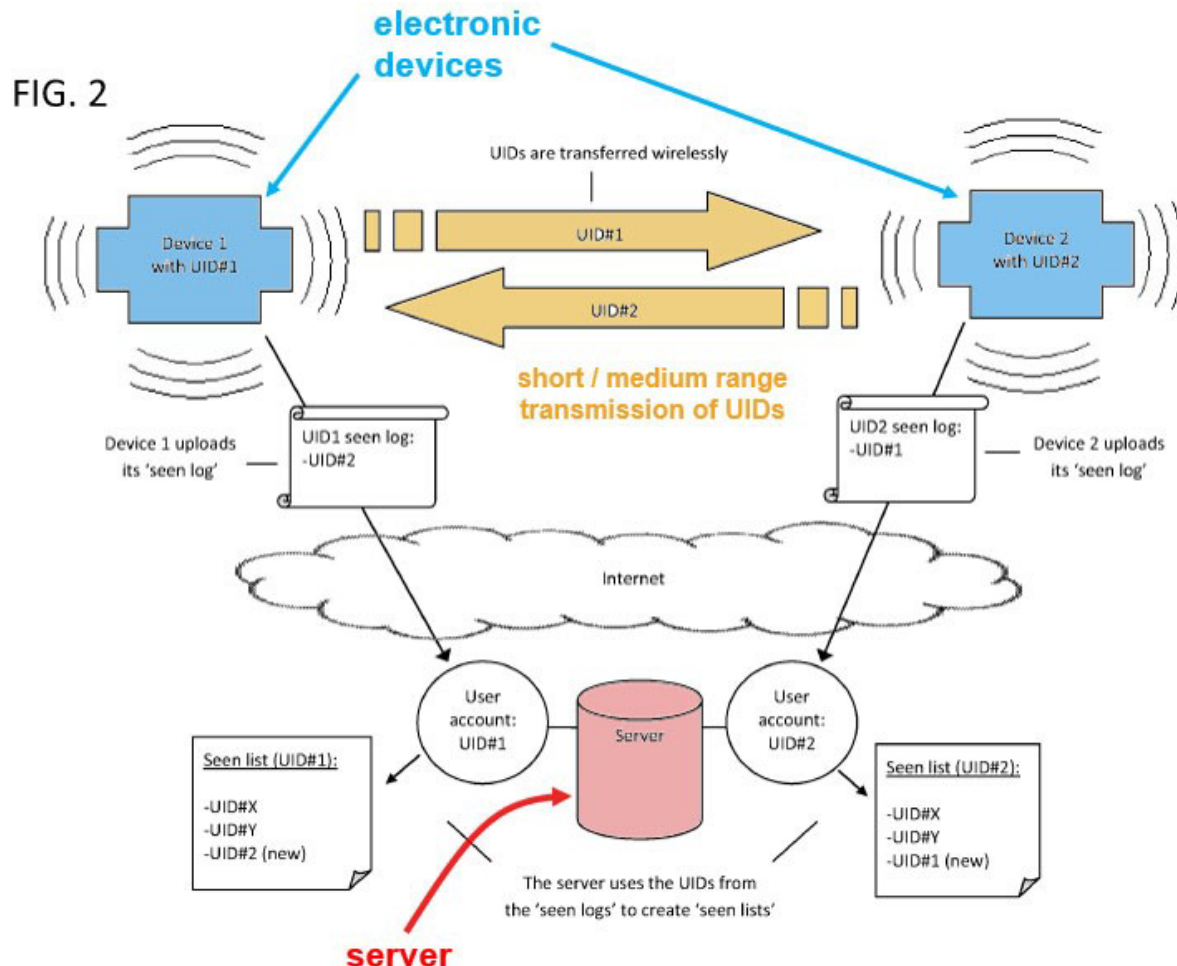
C. Behrens (EX1008)

82. 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.

83. 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. EX1008, Title, 11:1-5. The UID “contains information for identifying the device (and thus its user).” EX1008, 6:6-8. Specifically, the UID “may consist of or include a MAC (media access control) address, Bluetooth Device Address

(i.e. BD_ADDR), or other unique or quasi-unique identifier.” EX1008, 11:21-26.

Behrens also teaches 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. EX1008, 23:1-5. 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). EX1008, 32:21, FIG. 2.



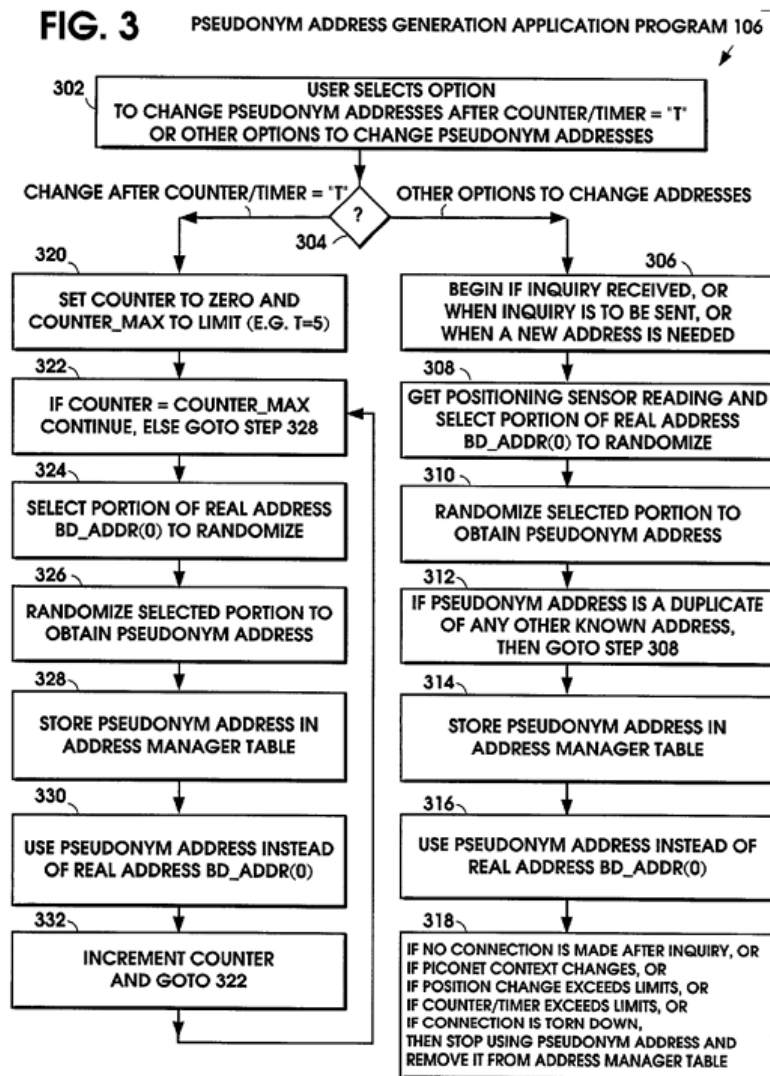
EX1008, FIG. 2 (annotated).

D. Nordman (EX1046)

84. Nordman (U.S. Patent Publication No. 2002/0174364), titled “Method for Protecting Privacy when Using a Bluetooth Device,” was published on November 21, 2002. I understand from Counsel that Nordman is §102(b) prior art to the ’971 patent.

85. Nordman describes a method for substituting a user’s Bluetooth Device Address (BD_ADDR) for a pseudonym address. EX1046, Abstract. Nordman’s “pseudonym address” is a “randomized version” of a Bluetooth Device Address (BD_ADDR). EX1046, Abstract, ¶6. Nordman describes that its “pseudonym address” can be “used in all the functions of the Bluetooth device that normally use the BD_ADDR.” EX1046, Abstract, ¶6. Various parameters may be used to generate the pseudonym address. For example, Nordman describes utilizing “various parameters [for an input] into the random number generator as initialization vectors to combine with the BD_ADDR.” EX1046, ¶8. The parameters may “change the random number sequence and thus thwart an eavesdropper's discovery of that sequence.” EX1046, ¶8; *see also* ¶¶12, 57. Nordman further describes providing a “privacy options menu” to allow a user to select different ways of randomizing the BD_ADDR. *See* EX1046, ¶¶34-42. For example, if the option to randomize the entire device address is selected, the user’s

Bluetooth device “randomizes the entire 48-bits of the user’s real BD_ADDR(0) to produce the pseudonym address.” EX1046, ¶¶40; *see also* ¶3. Nordman also describes performing pseudonym address operations via an application on a user’s Bluetooth-enabled device. EX1046, ¶58. As I have reproduced below, Figure 3 from Nordman is a flowchart that provides an overview of Nordman’s pseudonym address generation functionality:



EX1046, FIG. 3.

XI. DETAILED EXPLANATION OF THE UNPATENTABILITY GROUNDS

A. Ground 1: Claims 1, 11-13, 15, 20, 29-32, 34, 36, 50, 56, 61, 63-65, 67, 70, 73, and 80 are obvious over Ribaudo in view of Watanabe.

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

86. In addition to the reasons set forth below, a POSITA would have been motivated to combine the teachings of Ribaudo and Watanabe 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. EX1006, Abstract, ¶27; EX1007, Abstract, ¶18.

87. Ribaudo describes a beacon service identifier in the form of an SSID. In Ribaudo, a mobile device “may beacon an *SSID of ‘proprietor_name.net’* (e.g., where ‘proprietor_name’ corresponds to the name of a proprietor of system 10).” EX1007, ¶123. The “proprietor_name.net” may be associated with a particular service. For example, where the proprietor is an online dating platform, the SSID itself may be associated with, and therefore identify, one more services provided by such a proprietor (e.g., providing dating matches). *See, e.g.*, EX1007, ¶¶97-104, 138 (discussing “dating” related services). Ribaudo also describes filtering mechanisms, such as filtering based on “SSIDs,” and only notifying a user if a matching SSID is detected. EX1007, ¶61; *see also* ¶¶29, 55, 97-104, 123, 162, 223,

226. “Once a desirable SSID is detected... the two mobile devices 12a and 12b may establish a connection on the same network.” EX1007, ¶71. In this manner, Ribauda describes filtering beacon transmissions based on a particular beacon service identifier.

88. In view of this teaching, Ribauda describes using an identifier for a particular service as well as filtering based on such an identifier. To further enhance these capabilities and provide a more efficient manner to process and filter beacon transmissions, a POSITA would have been motivated to implement Watanabe’s beacon transmission structure, “service code,” and service code “filtering” techniques. For example, Watanabe describes a beacon transmission that includes multiple identifiers, including a “company code,” “unique code,” and “service code.” EX1006, FIG. 2, ¶¶14-15, 33, 49, 63. Watanabe describes filtering such beacon transmissions using the service code when determining whether a user has entered into a contract to receive services corresponding to the service code. EX1006, ¶¶41, 48-49, 51-52, 57, FIG. 8. Watanabe therefore teaches processing and filtering beacon transmissions based on “service codes” corresponding to a particular service. EX1006, ¶¶41, 48-49.

89. In the Ribauda-Watanabe combination, a POSITA would have found it obvious and would have been motivated to implement and beacon Watanabe’s service code together with beaconing a MAC address, client ID, and/or SSID in

Ribaudo's system to further enhance Ribaudo's processing of beacon transmissions and filtering capabilities. For example, Ribaudo's invention already "contemplates use of any other suitable identifiers ... according to particular needs." EX1007, ¶76. I note that filtering beacon transmissions via the received identifiers was well-known in the art. As described above, Godfrey explains that filtering processes "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." EX1031, ¶35. Krikorian describes a similar means of filtering beacon transmissions. EX1009, ¶26. In the present Ground, a POSITA would have included a service code corresponding to the type of match data beacons in Ribaudo. EX1007, ¶90 (describing "nine categories" of matching including "dating" and "employment"). A POSITA would have found it beneficial to include a service code corresponding to the type of match data beacons over Bluetooth between Ribaudo's mobile device. EX1007, ¶90. Including such a service code would allow the mobile device receiving the Bluetooth beacon to distinguish between different types of match data. This would allow mobile devices to identify desired service types. For example, the service code, as applied to Ribaudo, would identify beacon transmissions corresponding to a "dating" service, which would allow receiving mobile devices to more efficiently apply the filtering of beacon transmissions based on desired services as described in both Ribaudo and

Watanabe. For example, users may choose to be matched using one of Ribaudó's nine match categories, thereby setting a filtering criteria for beacon transmissions detected by a mobile device. The user's mobile device would then identify beacon transmissions including the service code that matches the user's set criteria. Thus, a POSITA would have been motivated to combine Ribaudó and Watanabe to further enhance Ribaudó's processing of beacon transmissions.

90. A POSITA would have had a reasonable expectation of success in combining the teachings of Ribaudó-Watanabe. Both describe mobile devices that receive beacon transmissions comprising identification information associated with a transmitting device, receive information relating to an entity associated with the identification information from a server using the Internet, compare the beacons identification information to preset identification information stored at the mobile device to determine if it matches, and take further action relating to the stored information if it matches. EX1006, ¶¶46-55; EX1007, ¶¶6-7.³

³ Moreover, as I explained in the Technological Background section, the use of MAC addresses, unique identifiers, and beacon service identifiers to identify devices and networks was known to a POSITA by 2008. *See, e.g.*, Section VII.B (citing, e.g., EX1009 (Krikorian), ¶¶21, 23, FIG. 3; EX1029 (Kondou), ¶35; EX1031 (Godfrey), ¶¶34, 54-55; EX1032 (Jansen), 23-24; EX1033

91. 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. 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. EX1006, ¶¶46-55; EX1007, ¶¶6-7. Further, Ribaud explains

(Langensteiner), ¶38; EX1034 (Suresh), ¶¶39, 58; EX1028 (Gulin), ¶69; EX1010 (Mgrdechian), ¶¶50, 91; EX1035 (Tamura), ¶¶47-48, 173, FIG. 4; EX1039 (Sorte), 4-5; EX1037 (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., EX1009 (Krikorian), Abstract, ¶¶4-5, 8, 22; EX1027 (Lazaridis), Abstract, 1:16-20, 2:37-45, 7:65-8:14; EX1010 (Mgrdechian) ¶¶13-14, 26-28, 42; EX1037 (Suzuki) ¶¶59, 63, 66, 68-70, 77-79, 83, FIGs. 6-7, 9-11).

“although MAC addresses and SSIDs are primarily described, [the] invention contemplates use of any other suitable identifiers ... according to particular needs.” EX1007, ¶76. Watanabe also explains that its “field configuration for this transmitter identification information is commonly used when using internet services.” EX1006, ¶¶15-16. A POSITA would thus have understood that these references disclose interrelated teachings based on well-understood technologies that would have been amenable to various well-understood and predictable combinations.

92. Additionally, a POSITA would have recognized that implementing Watanabe’s service code and filtering techniques based on that service code would have amounted to combining prior art elements according to known methods to yield predictable results, a simple substitution of one known element for another to obtain predictable results, and/or the use of known technique to improve similar devices (the mobile devices described in both Ribaud and Watanabe) in the same way. As I previously explained above, 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.

93. In summary, in the Ribaud-Watanabe combination, Ribaud teaches the system and functionality for sending and receiving beacon transmissions that

include several identifiers, and Watanabe describes certain information (including a specific identifier like a service code) that would have been obvious and within the skill of a POSITA to include in Ribaudó's beacon transmissions. A POSITA would not have viewed the type of information included in the claimed beacon transmission as inventive, particularly in view of Ribaudó's and Watanabe's teachings and as I further explain below.

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

94. In my opinion, Ribaudó in view of Watanabe ("Ribaudó-Watanabe") teaches⁵ the preamble, to the extent it is limiting. Both teach wireless devices

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. Any meaningful differences between the claims or elements are individually identified and discussed.

⁵ I understand from Counsel that the term "teaches" includes both express

configured to communicate with other devices in proximity. Ribaud teaches mobile devices 12 that “each have an associated memory module 22,” which includes “any suitable memory, database, or other data storage arrangement” (EX1007, ¶32), wherein “each include any suitable combination of hardware, software, and firmware to provide the functionality described” including “one or more applications 20 that are based on one or more programming languages” to “facilitate communication with other mobile devices 12” and the data center. EX1007, ¶19. This includes “magnetic media, optical media,” and “read-only memory (ROM).” EX1007, ¶32. This teaches non-volatile memory so that software or firmware program instructions are not lost when the device loses power.

95. And 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., EX1009, ¶¶6, 30-32; EX1028, ¶¶29, 79-80, FIG. 2; EX1029, ¶¶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**

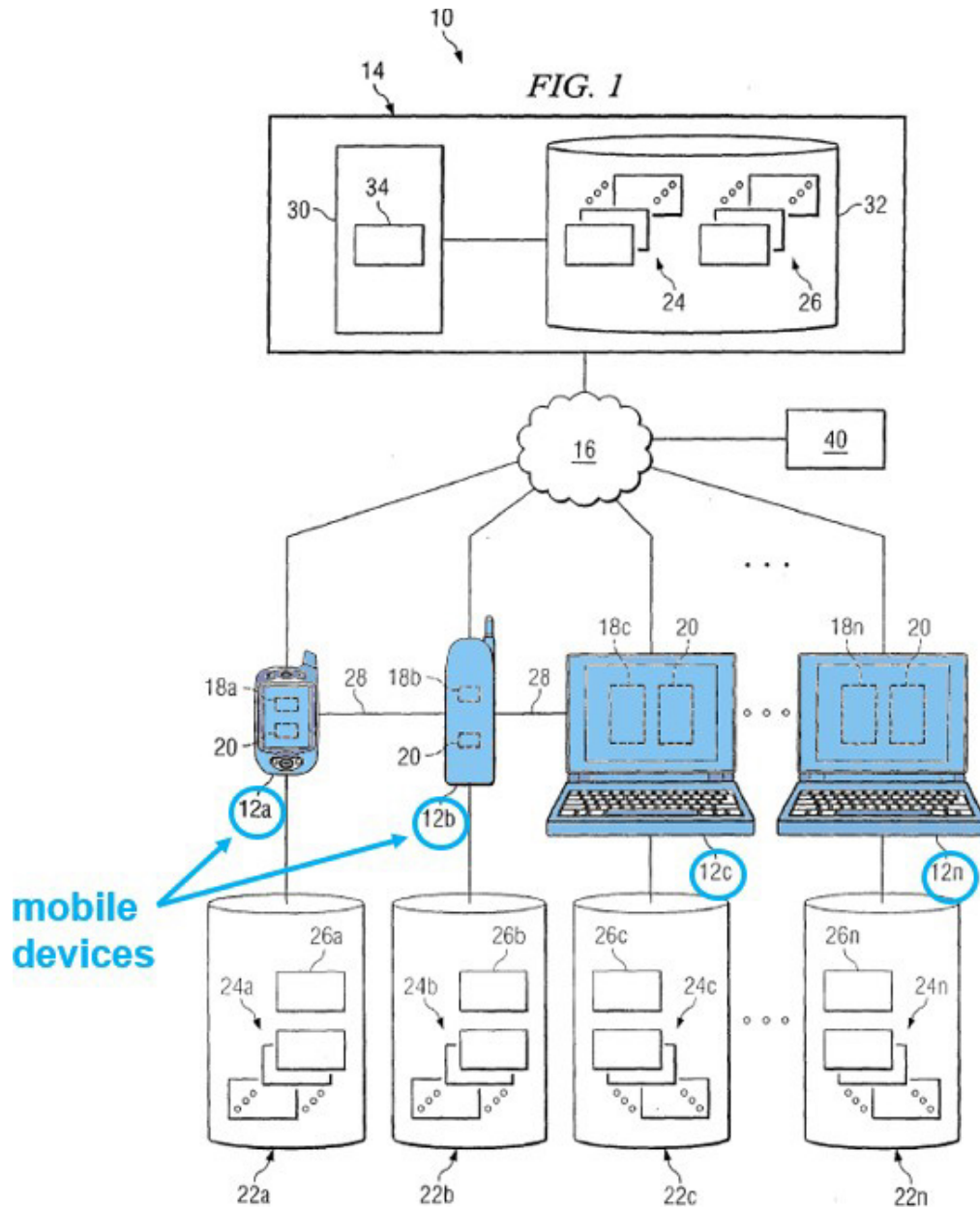
teachings and those fairly suggested to a person of ordinary skill in the art.

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;

96. In my opinion, Ribaud-Watanabe teaches Elements 1[a]/50[a].

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

97. Ribaud teaches mobile devices (*wireless device*) configured to receive beacon transmissions via a short-range protocol, such as Wi-Fi or Bluetooth. For instance, figure 1 of Ribaud includes “[m]obile devices 12” (blue), where each device (*e.g.*, 12a) “may include one or more suitable devices for wireless communication.” EX1007, ¶18; *see also* ¶15, FIG. 1.

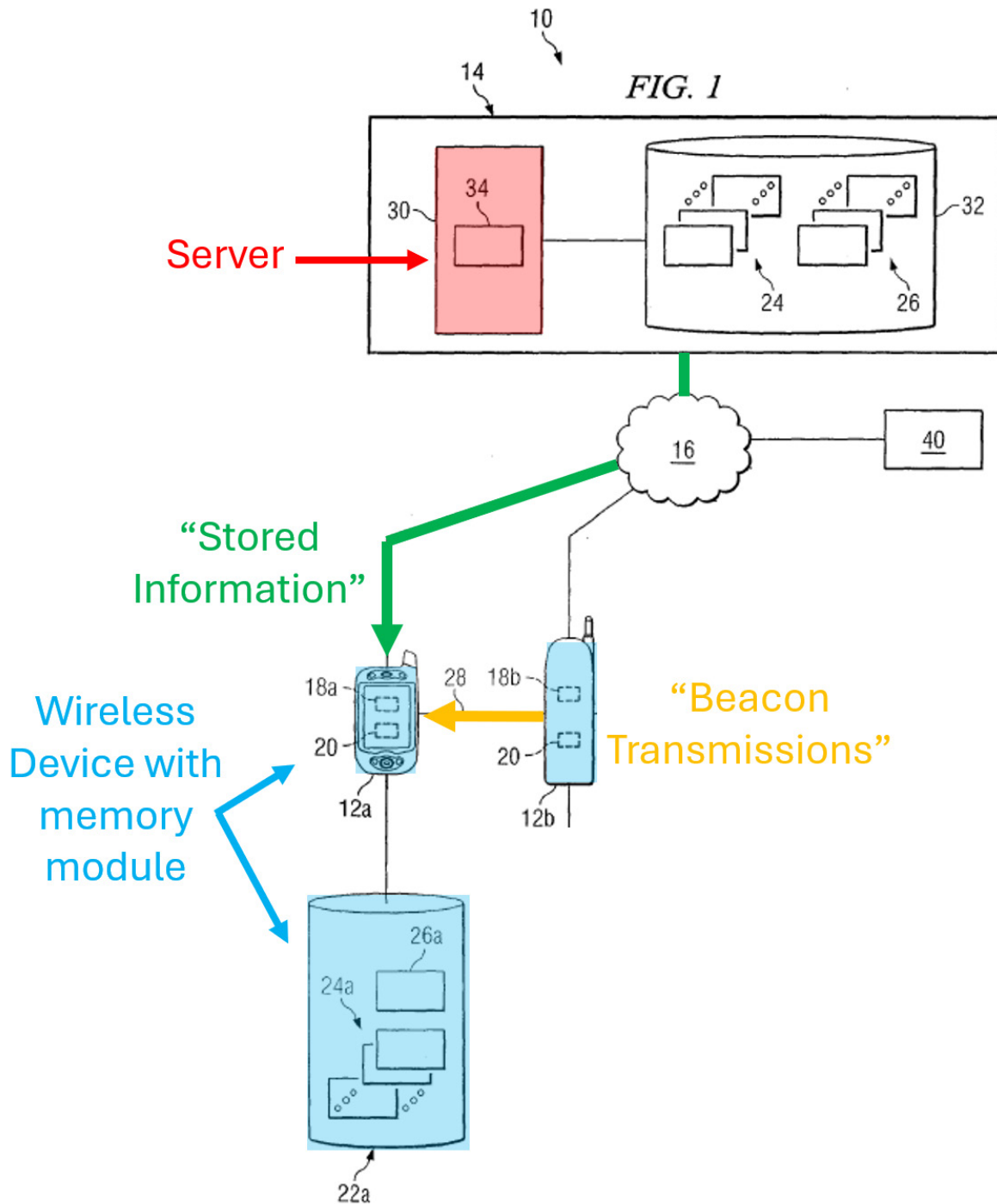


EX1007, FIG. 1 (annotated).

98. Ribaudo also indicates that “[e]ach mobile device 12 may include one or more suitable devices for wireless communication, such as one or more wireless fidelity (Wi-Fi) devices [or] one or more **BLUETOOTH** devices”—for example, Ribaudo’s “adaptor 18” may “facilitate communication with other mobile devices

12 (e.g., mobile devices 12b through 12n).” EX1007, ¶¶18-19, 21-22 (discussing NIC), 205, FIG. 1.

99. Ribaudó’s mobile devices receive a plurality of beacon transmissions from other mobile devices that are located within a detection range. Ribaudó explains that “mobile devices 12 are operable to *detect in proximity other mobile devices 12 that may be associated* with a user who is a potential match. ... Mobile device 12 may *beacon data* such as the client ID of the user associated with mobile device 12 (and possibly the user’s availability level and other identification information, such as trust score and status).” EX1007, ¶57. As depicted below, 12b may be an “other mobile device[]” in the detection range. The Bluetooth radio of mobile device 12a receives beacon transmissions from mobile device 12b, and such beaconing is performed using short-range transmissions. “In FIG. 1, links 28” (below, yellow) “illustrate example ad-hoc connections between mobile devices 12,” in which “*Wi-Fi technology* may be utilized to implement the detection process. ... Additionally or alternatively, ... mobile devices 12 may use *BLUETOOTH technology* to detect matches in proximity.” EX1007, ¶66, FIG. 1.



EX1007, FIG. 1 (annotated).

100. “This *beaconed data may be broadcast within any suitable range*, depending on the technology being employed.” EX1007, ¶57; *see also* ¶76 (“[A]lthough a 300-foot range is described as an example, a smaller or larger range is also contemplated for detecting other users in proximity.”). The proximity beacon transmissions, based on Wi-Fi or Bluetooth, are “short range,” when compared to cellular/WWAN transmissions.

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

102. Ribaudó also teaches receiving a plurality of beacons from more than one other mobile device. For example, Ribaudó explains that “John’s mobile

device 12 detects Steve’s mobile device 12 at a first time” and subsequently “detects Mary’s mobile device 12 at a second time,” EX1007, ¶148, which teaches that John’s device *receives a plurality* of short-range, proximity beacon transmissions.

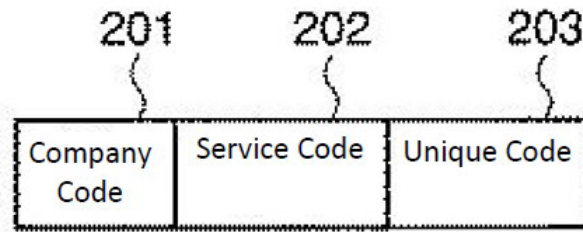
(ii) Overview of beacon transmission components

103. The Ribaud-Watanabe combination also teaches the claimed beacon transmission components. As I further discuss below, the combination of Ribaud and Watanabe further teaches that each of the plurality of beacon transmissions include a MAC address, a unique identifier that does not directly identify a location of a beacon transmitter, and a beacon service identifier that identifies a wireless beacon service, as follows:

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

104. Additionally, I note that the Ribaud-Watanabe combination teaches each beacon transmission including these three elements. For example, as seen from Watanabe’s Figure 2, Watanabe teaches a beacon transmission including multiple identifiers. EX1006, FIG. 2, ¶¶14-15, 33, 49, 63.

[FIG. 2]



EX1006, FIG. 2.

105. As seen from Watanabe’s Figure 2, Watanabe depicts a beacon transmission with three codes or identifiers. Watanabe describes a beacon transmission that includes a “unique code 203 specific to the ... transmitter,” which identifies a device transmitting the beacon. EX1006, ¶15. Watanabe’s “unique code” is similar to Ribaudó’s MAC address and the claimed MAC address, which also identifies the transmitting device. EX1007, ¶¶68-69, 157. Watanabe’s “company code 201 indicat[es] the service provider company.” EX1006, ¶15. Watanabe’s “company code” identifies a particular entity—such as a company rather than a device and is therefore similar to Ribaudó’s client ID and the claimed “unique identifier,” which also identifies a particular entity, such as a user. EX1007, ¶¶46, 84-85, 155-156. Watanabe’s “service code 202”—“indicating the type of service that can be provided —teaches the claimed “beacon service identifier.” EX1006, ¶15. In this manner, a POSITA would have recognized that

Ribaudo in view of Watanabe renders obvious a beacon transmission including each of the claimed identifiers.

106. As I explained in Section XI.A.1, Ribaudo teaches beaconing MAC addresses client IDs, and SSIDs. In view of Ribaudo's beaconing, a POSITA would have found it obvious to beacon such identifiers together as taught in Watanabe to enable more efficient processing and filtering of received beacon transmissions. Section XI.A.1.

(iii) MAC address

107. I note that Ribaudo describes MAC addresses and the ability for mobile devices to beacon and/or recognize MAC addresses. As Ribaudo explains, “[t]he adaptor 18 of a mobile device 12 that includes an NDIS-compliant and IEEE 802.11-compliant NIC may use the 802.11 frame or media access control (MAC) layer for detecting other mobile devices 12 in proximity.” EX1007, ¶21; *see also* ¶¶25 (“Mobile devices 12 may be identified on network 16 by a network address or combination of network addresses, such as a **MAC address** associated with the NIC, an IP address, a cell tower ID.”), 27, 68-69. Ribaudo further discloses that “[t]he **unique MAC address** of mobile device 12a **may be beacons** when the BLUETOOTH interface of mobile device 12a is active.” EX1007, ¶157. Although specifically referencing device 12a, a POSITA would understand Ribaudo as

teaching that each of the other mobile devices (12b, 12c, etc.), may likewise beacon its unique MAC address.

(iv) Unique identifier

108. Ribauda teaches “[m]obile device 12 may beacon data such as *the client ID of the user* associated with mobile device 12 (and possibly the user’s availability level and other identification information, such as trust score and status).” EX1007, ¶57; *see also* ¶84 (same). Ribauda describes the “client ID” as one of several “identifiers (IDs) for a user,” and explains that “[t]he client ID may include a public ID that may be broadcast from mobile device 12 and used by mobile devices 12 to detect a match in proximity[,]” or that it “may be used to shield the true identity of the user, for privacy purposes for example. Alternatively, the client ID may simply be the user ID of the user, which ... may reveal the true identity of the user.” EX1007, ¶¶45-46; *see also* ¶¶140 (listing identifiers of “another user” as including “an email address, telephone number, name, [etc.], or *other suitable information for identifying [a] user*”), 85. The client ID and potentially other suitable information included in Ribauda’s beacons that uniquely identifies a user, is thus a “*unique identifier*.” Because Ribauda’s client ID identifies a user, the client ID also *does not directly identify a location of a beacon transmitter* as recited in the claims. Rather, I note that Ribauda describes using

MAC addresses or SSIDs to identify locations instead of client IDs. EX1007, ¶¶78, 117, 213.

109. Additionally, the Ribaud-Watanabe combination teaches the *unique identifier*. For example, an example of the other suitable information described in Ribaud may include Watanabe's company code. EX1006, ¶15. Watanabe discloses a "company code 201 indicating the service provider company," which identifies a particular service-provider entity and thus serves as a unique identifier EX1006, ¶15. A POSITA would have been motivated to implement Watanabe's company code with Ribaud's beaconing to identify an entity associated with a beacon. A POSITA would have had a reasonable expectation of success because Ribaud already discloses transmitting and receiving beacons comprising multiple identifiers.

(v) Beacon service identifier

110. I note that the term "*beacon service identifier*" is not a term of art. Additionally, the '971 patent does not provide an explicit definition for "beacon service identifier." However, I note that the plain language of the words in the term indicate that it encompasses an identifier of a service using beacons. Based on this plain language of the claim in view of the specification, the Ribaud-Watanabe combination teaches the claimed *beacon service identifier*. Specifically, Watanabe discloses the transmission of beacons containing a plurality of fields, including a

“*service code 202* indicating the type of service that can be provided” via that device. *See* EX1006, ¶15. Such a service code 202 also teaches the claimed “*beacon service identifier*” because it identifies a type of service available via the beacon transmitter device. EX1006, ¶¶14-15, FIG. 2.

111. In the Ribaudó-Watanabe combination, I believe a POSITA would have found it obvious and would have been motivated to use a “service code” such as Watanabe’s “service code 202” to convey service information. EX1006, ¶15. For example, such a service code would be used when providing a user matching platform or an online data platform and providing dating matches to users within a given area as described in Ribaudó. EX1007, ¶¶97-104, 123. For example, such a service code would indicate that a particular beacon transmission corresponds to a “dating” service. Conveying Ribaudó’s service information using such a parameter would identify beacon transmissions received from other devices as relevant to the particular service (e.g., a user matching service or dating platform).

112. In my opinion, a POSITA would have been motivated to beacon a service code together with Ribaudó’s MAC addresses and client IDs to preserve processing costs by filtering out beacon transmissions that do not include a relevant service code. For example, this may include filtering for only beacon transmissions that include an identifier of a dating service. As I further describe with reference to claim elements 1[c]/50[c], including a service code would allow

mobile devices receiving beacon transmissions to more efficiently filter beacon transmissions as described in both Watanabe and Ribaudó. Sections XI.A.1, XI.A.2.d.

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

114. Additionally, a POSITA would have had a reasonable expectation of success in applying Watanabe's teachings to Ribaudó. Section XI.A.1. Both describe receiving beacon transmissions comprising identification information from a nearby device, via Bluetooth, receiving preset identification information relating to an entity from a server using the Internet, assessing the contents of the beacon transmissions, and determining whether the transmitting device is in proximity by utilizing the transmitted identification information and the preset identification information. EX1006, ¶¶46-55; EX1007, ¶¶6-7. A POSITA would thus have understood that these references disclose interrelated teachings based on well-understood technologies that would have been amenable to various combinations with predictable results.

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

115. The Ribaud-Watanabe combination teaches a *beacon service identifier* that *identifies the unique identifier is relevant to stored information associated with a wireless beacon service* by teaching conveying service information. For example, Watanabe explains that the “service code 202” can be used together with other unique identifiers (e.g., company code 201) to determine whether a unique identifier is relevant to stored information. EX1006, ¶¶15, 41-44. When implementing the service code, Watanabe associates the service (e.g., “S1”) with service providers (e.g., “C1,” “C2,” and/or “C3”). EX1006, ¶¶41-42. Watanabe’s service code therefore enables a mobile device to determine whether another unique identifier (e.g., a company code) is relevant when filtering beacon transmissions. EX1006, ¶¶41-42; *see also* ¶¶51-52 (explaining that both a service code and company code must match for services to be provided).

116. In the Ribaud-Watanabe combination, a POSITA would have used Watanabe’s service code with Ribaud’s client ID (i.e., claimed *unique identifier*) to signal whether a particular beacon transmission is relevant to the match data stored on Ribaud’s mobile device. When Watanabe’s service code (“*beacon service identifier*”) is included in Ribaud’s beacon along with Ribaud’s client ID (“*unique identifier*”) and other identifiers, the service code would identify that the

client ID is relevant to stored information associated with Ribaudo's matching service. As I previously discussed, Ribaudo describes several services like "dating" or "business networking." EX1007, ¶¶29, 58, 90, 223. In the dating context, the service code would identify that the client ID is relevant to dating service match data. This match data would be stored on the mobile device if previously downloaded or at the server if not yet downloaded. I will discuss this further in Section XI.A.2.c with respect to claim elements 1[b]/50[b]. In the business-networking context, the service code would identify that the client ID is relevant to match data associated with a conference or other networking function. EX1007, ¶¶55, 78, 96, 160, 163, 197. As I previously explained, a POSITA would have used Watanabe's service code to identify a service from Ribaudo together with Ribaudo's client ID to determine whether a matching user device is in proximity. Section XI.A.1. Thus, the Ribaudo-Watanabe combination teaches a *beacon service identifier that identifies the unique identifier is relevant to stored information associated with a wireless beacon service*.

2) Stored information is not otherwise accessible utilizing Bluetooth

117. 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. I understand that this phrase only appears in the claims. EX1001, 23:30-31, 26:59-60, 28:61-62, 29:35-36. Regardless, as I will

further explain with reference to claim elements 1[b]/50[b], Ribaudó's "user match data" teaches the claimed *stored information*. EX1007, ¶¶16, 33, 53. Ribaudó explains that the user match data includes "match identifiers and other information for the other users determined to be matches for the user." EX1007, ¶16.

118. In this manner, Ribaudó teaches the claimed *stored information*. Additionally, Ribaudó describes that the mobile device receives the match data via "wide area networks (WANs)" including the "Internet" or a "cellular connection." EX1007, ¶¶24-26, 204. In this manner, the match data that is delivered to Ribaudó's mobile device is delivered via a long-range protocol and is *not otherwise accessible* via a *short range protocol* or *Bluetooth*.⁶ Section XI.A.2.c (1[b]/50[b]).

119. In addition to Ribaudó-Watanabe'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. Furthermore, using protocols such as Bluetooth for

⁶ While I note that Ribaudó describes other "certain embodiments" that can communicate match data via Bluetooth or Wi-Fi, those embodiments are not relied upon here or when match data is delivered via, for example, a cellular connection. *See* EX1007, ¶166.

communications between mobile devices and servers was known. *See, e.g.*, Section VII.H.

120. 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.

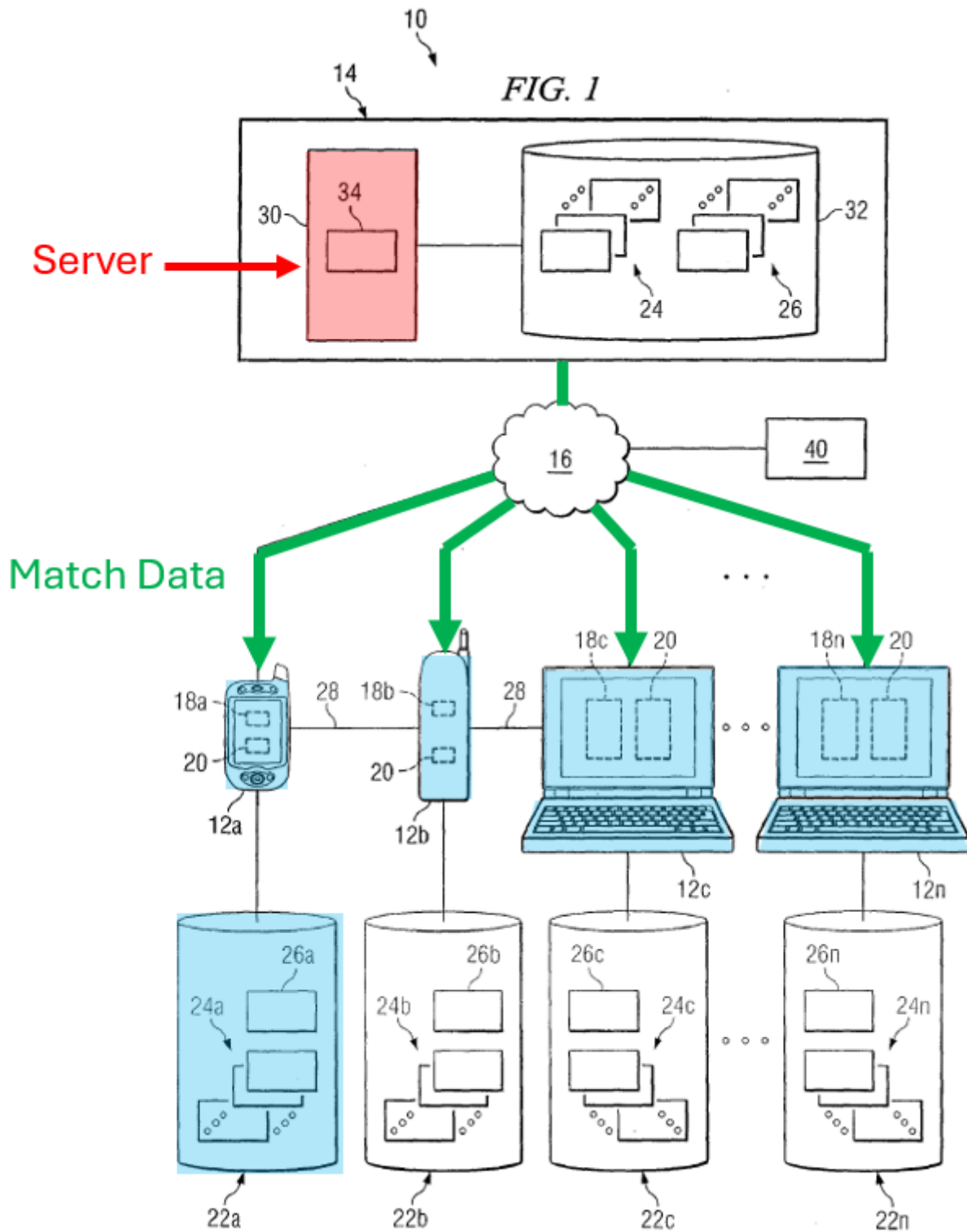
121. In sum, as shown in Figure 1, Ribaud-Watanabe teaches Elements 1[a]/50[a].

- (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;**

122. In my opinion, Ribaud-Watanabe teaches Elements 1[b]/50[b].

- (i) **Receiving at the wireless device stored information from a server**

123. I understand that Ribaud's "[d]ata center 14 includes a server system 30" (red), as depicted below in Figure 1. EX1007, ¶34, FIG. 1.

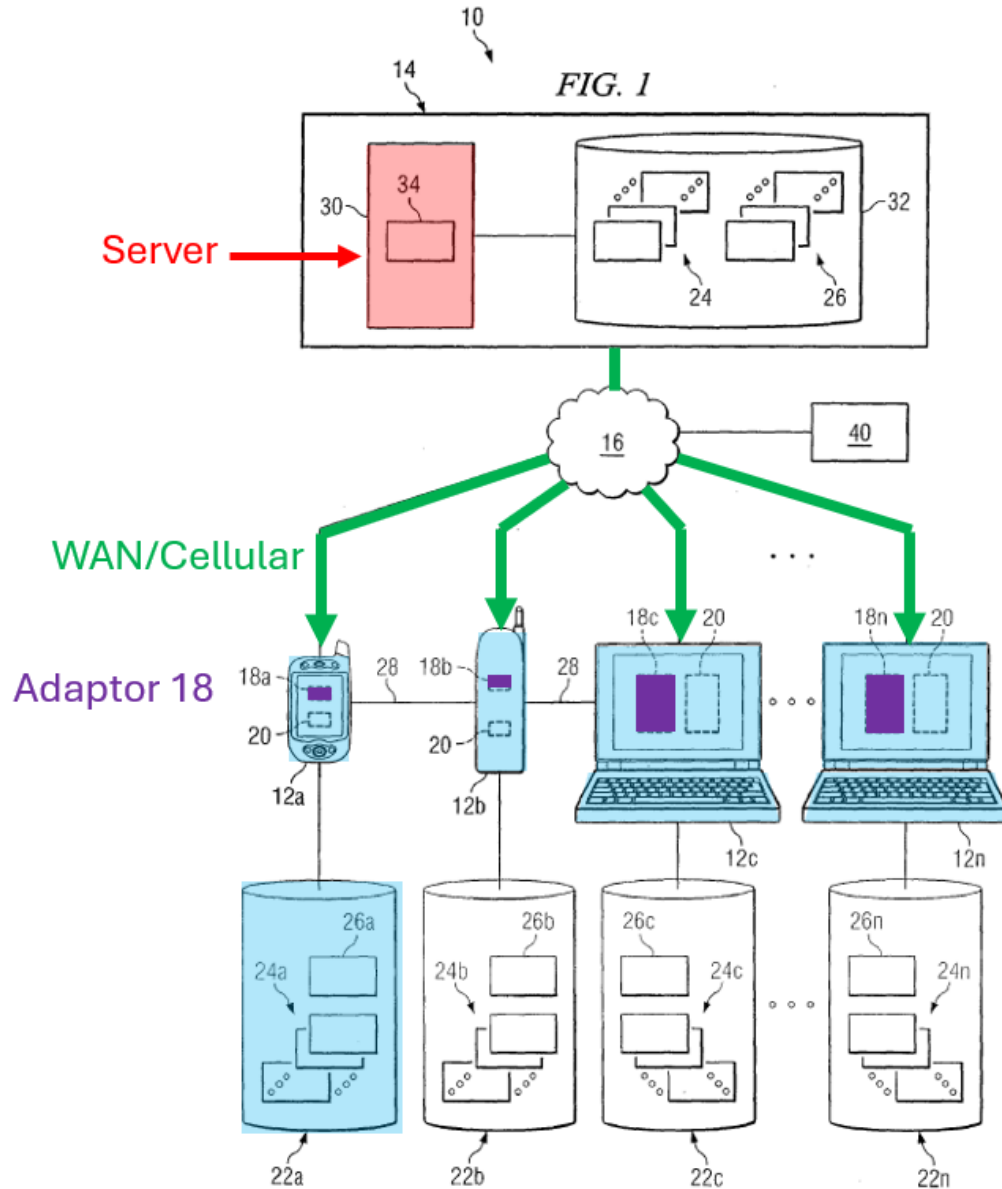


EX1007, FIG. 1 (annotated).

124. Ribaudo describes that its data center “*transmit[s] to each user match data* containing match identifiers and other information for the other users determined to be matches for the user. This *pre-processed match data* for the user is stored locally on the user’s mobile device 12.” EX1007, ¶16. Ribaudo also describes that its “memory module 22 may store match data 26 downloaded from data center 14 and identifying one or more predetermined matches for the user.” EX1007, ¶33; *see also* ¶¶53, 204-205 (also describing proximity detection before downloading match data from the server). Ribaudo’s match data is stored at the data center prior to transmission by server system 30 to a mobile device. EX1007, ¶¶26, 34, 53, 82-83. Accordingly, Ribaudo’s server system teaches the claimed *stored information from one or more servers* being transmitted and received at a wireless device as claimed.

(ii) Using a second wireless protocol different from Bluetooth

125. In my opinion, Ribaudo teaches the user’s mobile device receiving transmitted match data via a *second wireless protocol the is different from the short range wireless protocol*. For example, Ribaudo describes this transmission and reception occurring via a wide area network (WAN) or cellular protocol. EX1007, ¶24.



EX1007, FIG. 1 (annotated).

126. Ribaudo describes that its “[m]obile devices 12 may each include any suitable combination of hardware, software, and firmware to provide the functionality described herein.” EX1007, ¶¶18-19, 21-22 (discussing NIC), FIG. 1. Ribaudo indicates that “[e]ach mobile device 12 may include one or more suitable

devices for wireless communication,” including an “adaptor 18” that “may facilitate communication ... between mobile device 12 and data center 14.” EX1007, ¶¶18-19, FIG. 1. Further, Ribauda indicates that its “mobile devices 12 may each be coupled to data center 14 via network 16.” EX1007, ¶¶24-25. This includes “*wide area networks (WANs)*, [or] all or a portion of a global computer network such as the Internet.” EX1007, ¶¶24-25. Ribauda’s mobile devices may thus be coupled to the data center, via a WAN, using a “*wireless link*.” EX1007, ¶¶24-25. Ribauda’s system may also “employ[] a *cellular* connection ... to download from data center 14.” EX1007, ¶204. In this manner, Ribauda describes receiving the stored information using adaptor 18a’s cellular/WWAN radio protocol, which is different from a short-range or Bluetooth protocol. As I previously described, such functionality was known in systems existing prior to the ’971 patent’s priority date. *See* Section VII.H.

127. In addition to Ribauda-Watanabe’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. Additionally, storing information at servers and mobile devices communicating with servers to obtain stored information was known. *See, e.g.*, Section VII.E.

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

128. Ribaudó's match data also teaches the claimed *stored information relating to a particular entity or object associated with a first unique identifier*. Ribaudó's match data includes match IDs and client IDs that identify an entity such as a user. EX1007, ¶¶16, 40, 46, 53, 57, 82-85. Ribaudó further elaborates on what its described match data comprises. For instance. Ribaudó indicates that its "match data contain[s] match identifiers and other information for the other users determined to be matches for the user." EX1007, ¶6. Ribaudó also describes examples of match data and a match ID including a "client ID." EX1007, ¶¶49-51. Ribaudó further states that "[e]ach user may receive the other user's hash value from data center 14 as a part of the match data 26 downloaded to the user's mobile device 12." EX1007, ¶52. "This pre-processed match data for the user is stored locally on the user's mobile device." EX1007, ¶6. Then, when in proximity with another user, the user's mobile device "compares the received identifier with the pre-processed match data stored on the user's mobile device to determine whether the other user is one of the user's predetermined matches." EX1007, ¶¶6, 16, 40, 53, 57, 82-85.

129. Ribaudó further explains that "*using match data 26* (e.g., the match IDs) downloaded from data center 14, mobile devices 12 are operable to detect in proximity other *mobile devices 12 that may be associated with a user who is a*

potential match.” EX1007, ¶57. Ribauda further explains that a “[m]obile device 12 may *beacon data such as the client ID of the user associated with mobile device 12* (and possibly the user’s availability level and other identification information, such as trust score and status). This beacons data may be broadcast within any suitable range, depending on the technology being employed.” EX1007, ¶57; *see also* EX1007, ¶¶123, 157, 173 (further describing beaconing by mobile devices 12). The match data relates to “commonalities or other reasons for interacting” between two users of a given internet service (e.g., online dating) and therefore relates to a particular *entity* associated with a *unique identifier* as recited in the claims. *See* EX1007, ¶¶16, 29, 97-105; *see also* EX1007, ¶¶157-171 (describing various services, including “Closed Group Matching,” “Implied Proximity” matching, “External Web Service,” and “Use of Match Data in Cooperation with Third Parties”), 204-205, 221-223.

130. In addition to Ribauda-Watanabe’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.

- (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

131. In my opinion, Ribaud-Watanabe teaches Elements 1[c]/50[c].

(i) Filtering the beacon transmissions that include a particular beacon service identifier

132. The Ribaud-Watanabe combination teaches filtering beacon transmissions based on those that include a particular beacon service identifier.

133. For example, Watanabe describes filtering beacon transmissions based on a “service code.” Watanabe’s “filtering identification information notification unit 13 selects and combines the proper codes to generate filtering identification information for the client terminal 14.” EX1006, ¶41. One way of applying Watanabe’s filtering is to filter the beacon transmissions based on “service codes” corresponding to a particular service. EX1006, ¶¶41, 48-49.

134. Additionally, I note that Watanabe describes filtering beacon transmissions based on service codes when determining whether a user is to receive services corresponding to the service code. EX1006, ¶¶41, 51-52, 57, FIG. 8. For example, a mobile device receiving a service code “S2” included in a transmitted beacon may check the service code for filtering purposes and to determine whether the beacon is associated with a particular service. EX1006, ¶52; *see also* ¶15 (referring to a service code as a “filter” code). In view of this

disclosure, Watanabe teaches filtering beacon transmissions using a service code corresponding to a particular type of service.

135. In the Ribaudó-Watanabe combination, a POSITA would have found it obvious and would have been motivated to implement and beacon Watanabe's service code together with beaconing a MAC address, client ID, and/or SSID in Ribaudó's system to further enhance Ribaudó's processing of beacon transmissions and filtering capabilities.

136. For example, I note that Ribaudó teaches receiving, processing, and filtering identifiers received from other mobile devices. For example, Ribaudó explains determining if a mobile device received certain identifiers from another mobile device: "a first user's mobile device detects the presence of a second user's mobile device in proximity based on network *identifiers* communicated from the mobile devices of the first and second users." EX1007, ¶7; *see also* ¶6, cl. 1. This detection is achieved by processing the received identifiers. EX1007, ¶7; *see also* ¶6, cl. 1. Ribaudó also describes various filtering mechanisms as part of its identifier processing and matching process. EX1007, ¶¶58, 61, 64.

137. Ribaudó describes potentially filtering based on "SSIDs" and only notifying a user if a matching SSID is detected. EX1007, ¶61; *see also* ¶¶29, 55, 97-104, 123, 162, 223, 226. For instance, a "user desiring a work-related filter may specify instructions, as part of his or her user profile 24 that could be included in

the match ID, to instruct the adaptors 18 of other users to notify their users of a match only under certain circumstances, such as particular times of the day, days of the week, dates, SSIDs, or other suitable circumstances.” EX1007, ¶61 “Once a desirable SSID is detected... the two mobile devices 12a and 12b may establish a connection on the same network.” EX1007, ¶71. Indeed, Ribauda describes “[i]n ad-hoc mode ... application 20 may beacon an SSID of ‘proprietor_name.net’ (e.g., where ‘proprietor_name’ corresponds to the name of a proprietor of system 10). When a first user of a mobile device 12 who is in proximity of a second user of application 20 on another mobile device 12, the first user's mobile device 12 may perform an SSID scan to browse the list of available networks in proximity of the first user.” EX1007, ¶123. Additionally, Ribauda describes filtering based on “work” or “recreation” matches and the ability to “filter matches that are not primarily work-related matches.” EX1007, ¶61. This enables Ribauda’s system to filter beacon transmissions based on identifiers.

138. In view of these filtering teachings from Ribauda (e.g., based on work or recreation), a POSITA would have found it obvious and would have been motivated to combine Ribauda and Watanabe. As I explained above, a POSITA would have included a service code corresponding to the type of match data beacons in Ribauda. EX1007, ¶90 (describing “nine categories” of matching including “dating” and “employment”); *see also* ¶¶55, 97-104, 223. Ribauda

explains that “users may choose to be matched based on one or more of the following nine categories that may each be as granular as the user desires: (1) Background, (2) Hobbies/Interests, (3) Organizations, (4) Friends and Acquaintances, (5) Business Networking, (6) Dating, (7) Networking Goals, (8) Market (buy/sell items, free agent services), and (9) Employment.” EX1007, ¶90. A POSITA would have found it obvious to include Watanabe’s service code to identify a particular category a user in Ribaudó is seeking to match with other users, thereby improving the functionality of Ribaudó’s filtering techniques. Including such a service code would distinguish between different types of match data. For example, the service code would identify beacon transmissions corresponding to a “dating” service, which would allow receiving mobile devices to more efficiently apply the filtering of beacon transmissions described in both Watanabe and Ribaudó. Thus, the Ribaudó-Watanabe combination teaches the claimed “*filtering*” based on particular beacon service identifiers.

(ii) Selecting one or more unique identifiers from the beacon transmissions

139. In addition to filtering beacon transmissions based on beacon service identifiers, the Ribaudó-Watanabe combination also teaches selecting one or more unique identifiers based on this filtering. As I previously explained, Ribaudó selects a unique identifier (e.g., Ribaudó’s “client ID”) when extracting the client ID from a received beacon transmission to compare the client ID “with the pre-

processed match data stored on the user's mobile device" in order to identify and determine matches. EX1007, ¶¶6, 45-46, 65-68, 84-85; *see also* cl. 9. And "when mobile device 12a *detects another client ID (or other suitable identifier indicating a potential user of system 10)*, mobile device 12a may consult match data 26a to determine whether the user associated with the detected client ID is identified in the match data 26a for mobile device 12a." EX1007, ¶85. Based on this description, Ribauda teaches selecting one or more unique identifiers from beacon transmissions when identifying a received client ID to compare with stored match data as explained for 1[b]-1[c]/50[b]-50[c].

140. Additionally and as I previously explained, in the Ribauda-Watanabe combination, this selection would have occurred in response to filtering beacon transmissions based on a particular beacon service identifier. *See* Section XI.A.2.d (1[c]/50[c]). For example, this filtering may be performed based on Watanabe's service code as implemented with Ribauda to identify a particular service (e.g., work or dating). Performing this filtering based on a service identification would allow receiving mobile devices to more efficiently process beacon transmissions (as described in both Watanabe and Ribauda) and perform a unique identifier comparison only for beacon transmissions corresponding to a particular service (e.g., work or dating).

141. Thus, the Ribauda-Watanabe combination teaches this claim element.

142. In addition to Ribaud-Watanabe's teachings above, as I explained in the Technological Background section of my Declaration, identifying and selecting unique identifiers from beacon transmissions was known to a POSITA by 2008.

See, e.g., Section VII.F.

- (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.**

143. In my opinion, Ribaud-Watanabe teaches Elements 1[d]/50[d]. This is because the recited "*first further action*" relating to the stored information is a broad and generic claim term and one that at least Ribaud teaches. I note that dependent claims 7, 11-12, 20, and 29-30 additionally describe examples of "*first further actions*," and I address these claims further below.

144. For example, Ribaud teaches determining that a first unique identifier is present among the selected one or more unique identifiers when identifying matches using detected client IDs and previously stored match data. Such functionality was known to a POSITA by 2008, as I explained above. *See* Section VII.C (citing to Krikorian, Lazaridis, Mgredechian, and Suzuki) Ribaud explains that "when the user is in proximity to another user, the user's mobile device detects the presence of the other user's mobile device, *receives an identifier associated with the detected other user, and compares* the received identifier *with the pre-processed match data* stored on the user's mobile device to determine

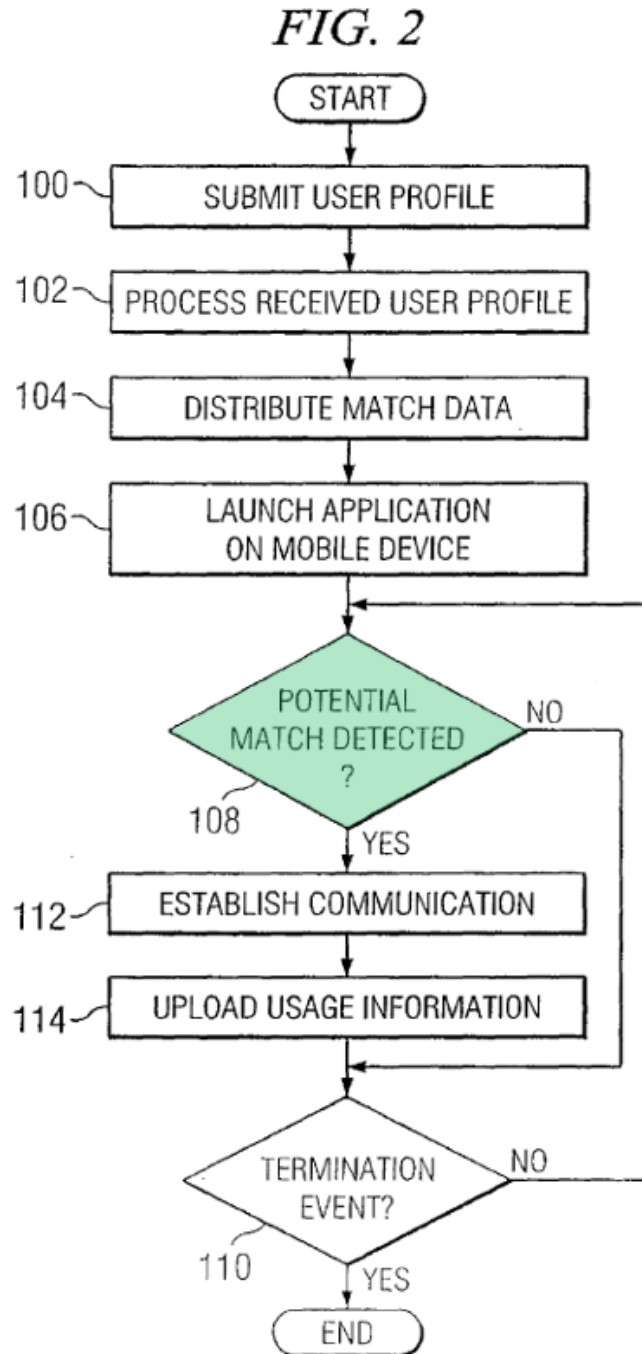
whether the other user is one of the user's predetermined matches. ... [T]his detection of another user in proximity and determination of whether another detected user is a match is performed locally on the user's mobile device."

EX1007, ¶6; *see also* ¶16 (describing the same).

145. In Ribaudó's Figure 2, "[a]t step 106, the user of mobile device 12a launches application 20[,]" which:

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

EX1007, ¶84; *see also* ¶¶80-83.



EX1007, FIG. 2 (annotated).

Then:

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

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

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

146. Based on these teachings from Ribaudó, Ribaudó's mobile device determines whether an entity (*e.g.*, user of another mobile device) associated with a proximity beacon service is in proximity, on the basis of pre-processed match data and identifiers received from the data center ("*first unique identifier*") and the user's client ID (the "one or more unique identifiers") detected from the beacon transmissions. Ribaudó's description of determining that another matching mobile device is in proximity provides and discloses an example of the claimed *first further action*.

147. As seen from Ribaudó's Figure 2, Ribaudó describes various additional examples of a *first further action* that may occur in response to a match determination. Ribaudó explains that if a match is detected at step 112, "communication between matched users of mobile devices 12 may be established." EX1007, ¶87. Similarly, "if a match is determined, then mobile device 12a may

notify its associated user of the match.” EX1007, ¶87. Additionally, “usage information may be uploaded to data center 14.” EX1007, ¶87. Ribaud also teaches retrieving content from a server as well as displaying a match value on a mobile device (e.g., displaying that both users have a “Harvard” match). EX1007, ¶¶17, 47, 78, 134. Based on these teachings, Ribaud describes several examples of a *first further action* that may occur related to the match data (i.e., “*stored information*”) in response to detecting that a *first unique identifier* is present among *one or more unique identifiers* detected from the beacon transmissions.

148. In addition to Ribaud-Watanabe’s 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.

149. Thus, the Ribaud-Watanabe combination renders obvious claims 1 and 50.

3. **Dependent Claims 11-13, 15, 20, 29-32, 34, 36, 56, 61, 63-65, 67, 70, 73, and 80**
 - (a) **Claims 11/32/63: The [method]/[computer program product] of claim [1]/[50] wherein the [taking] first further action [further comprises]/[additionally includes]: [causing the wireless device to] [determine]/[determining], based upon at least a portion of the stored information, that at least one**

beacon transmitter is associated with a predetermined location.

150. In my opinion, Ribaud-Watanabe teaches claim 11.

151. Ribaud teaches *determining, based upon at least a portion of the stored information, that at least one beacon transmitter is associated with a predetermined location* as claimed. In particular, Ribaud teaches “location” tag information that can associate detected matches with particular locations. EX1007, ¶¶117, 160-161, 166, 185-186, 202, 213, 216. For example, Ribaud indicates “a user may tag particular locations based on hardware signatures such as network identifiers (e.g., MAC addresses) associated with one or more networks at the location. For example, based on MAC addresses or other hardware signatures, particular locations can be tagged with useful information by users of mobile devices 12.” EX1007, ¶117. Tag information can be edited by a user to “include more useful information about the location, such as ‘CES-ConferenceRoom4,’ ‘MainStreetCafe,’ ‘DFWAirport-Terminal3,’ or other suitable keywords.” EX1007, ¶117. Ribaud explains that using this location tag information, mobile devices detecting matches (*based upon at least a portion of the stored information*) are then able to associate a detected matching mobile device with the predetermined location corresponding to the tag: “tagged information for a location may be shared with other users who use the location to *provide context for the other users’ detected matches at the location.*” EX1007, ¶117. In this manner,

Ribaudo's teaching of correlating a detected mobile device and a user match with a location tag teaches as a *first further action, determining that a beacon transmitter is associated with a predetermined location.*

152. Additionally, Ribaudo also describes matching users attending a particular event at a “particular location and/or time.” EX1007, ¶160. For example, “match data 26 may be sent to some or all users who are members of a particular group at a particular time or location.” EX1007, ¶¶163, 166. Ribaudo describes example locations like “a coffee shop, an airport, a university, a wedding, or any other suitable gathering of users that is known or scheduled in advance.” EX1007, ¶160. Users at these locations may detect and communicate with one another and “locate each other at the event” based on proximity. EX1007, ¶161.

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

154. Indeed, as I discuss above, performing an 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.

155. In this manner, Ribaudó's additional examples of location-based match detection and user detection also teach determining that a matching mobile device transmitting a beacon is also *associated with a predetermined location* as claimed.

(b) 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].

156. In my opinion, Ribaudó-Watanabe teaches claims 12 and 64.

157. At the outset, I note that Ribaudó describes a scenario where proximity detection occurs prior to a mobile device using a cellular radio to download match data (i.e., the claimed *stored information*) from the server. EX1007, ¶¶204-205. For example, Ribaudó describes a mobile device first detecting other users in proximity and then subsequently “download[ing] from data center 14 the individual match IDs for those users.” EX1007, ¶¶204-205. In view of this example and sequencing of data reception, Ribaudó teaches receiving match data (i.e., the claimed *stored information*) in response to sending a detected unique identifier to a server. EX1007, ¶¶65-68, 204-205. I also note that Ribaudó describes match data “synchronization” or downloading the “most current match data” based on the client ID, which are also examples of sending a unique

identifier and then receiving stored information, which may be in the form of updated match data. EX1007, ¶¶31, 40-42, 53.

158. Ribauda also teaches a mobile device that sends a client ID to a server when accessing another user's "personal URL," which may include the client ID (e.g., "www.proprietor_name.net/**clientid**_82740AF3RT432"). EX1007, ¶¶126-147, FIG. 3. Registered users may be assigned one or more personal URLs by data center 14. EX1007, ¶126. A mobile device may use the personal URL to connect to data center 14 and retrieve match data. EX1007, ¶¶128-130. Alternatively, a user may select a summary link showing the client IDs of nearby users to connect with the data center. EX1007, ¶139. A POSITA would have understood that accessing the personal URL or summary link transmits the client ID (a "*first unique identifier*") to the data center.

159. For instance, Ribauda discloses that a mobile device may use a personal URL to connect to data center 14 and (among other things) retrieve match data. EX1007, ¶¶128-130. Alternatively, a mobile device may allow a user to "click on a summary link that shows the client ID of all nearby users" in order to connect with data center 14. EX1007, ¶139. A POSITA would have understood that using or accessing the personal URL or the summary link sends the relevant client ID to the data center when the client ID is included in, or associated with, the personal URL or summary link. This is consistent with the well-known operation of URL-

based web requests, in which accessing a link or entering a URL causes a request, where the request includes the requested URL and any URL parameters, to be sent to a server. Thus, when a personal URL or summary link is accessed by a mobile device, the resulting URL-based request would have been understood to provide the server and/or data center with the URL information to identify the requested resource or associated client information. This demonstrates that the client ID is sent to the data center when the personal URL is accessed.

160. For example, U.S. Patent Application Publication No. 2002/0116494 to Kocol et al. (EX1012, “Kocol”), explains that when a “network user begins a communication session over the Internet, the user can request data files from an Internet-connected computer called a file server or Web server using the hypertext transfer protocol (HTTP). These data files comprise what are commonly referred to as Web pages” EX1012, ¶6. “A network user can request a Web site page by *clicking on a link* in the browser window or by *typing in a uniform resource locator (URL) network address* in the browser location toolbar.” EX1012, ¶7. When the request is made, “the user's browser *sends a request message* from the user's browser to the Web site server, *providing the Web site server with the URL of the requested page*. So-called Internet ‘cookies’ and *header information may also be sent* along with such a request.” EX1012, ¶7. Additionally, “[i]nformation may also be passed to the Web site server via parameters contained as part of the

Web page URL address. For example, the URL

http://www.URLAddress.com/x.cgi?account_no=123 is a URL containing the parameter ‘*account_no*’, with a value of *123*, *which is passed to the Web server as part of the URL request.*” EX1012, ¶¶9-11. Kocol further discloses that links are “generally coded with an anchor tag” that “specifies the URL address of the requested data file,” and that the anchor tag “specifies the domain name and page reference and thereby specifies the URL of the requested data file.” EX1012, ¶¶11-13.

161. Ribaudo teaches that the first further action is related to the first unique identifier for the reasons explained in Section XI.A.2.e (1[d]/50[d]). In the Ribaudo-Watanabe combination, taking a first further action additionally includes causing Ribaudo’s wireless device to send the first unique identifier or information derived from it to one or more servers (data center 14) and receive the stored information (match data) in response. Section XI.A.2.e; EX1007, ¶¶204-205.

- (c) **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 of]/[performing] the first further action.**

162. In my opinion, Ribaudo-Watanabe teaches claims 13 and 65 for the reasons I explained for claim 1. For example, the explanation that I provided for

claim 1 accounts for the Ribaud-Watanabe combination teaching the stored information being received prior to performing the first further action as recited in claims 13 and 65. EX1007, ¶¶6, 16, 80-85, 87, FIG. 2; Sections XI.A.2.c (1[b]/50[b]) (receiving stored information at the wireless device from the server relating to an entity/object with a first unique identifier), XI.A.2.d (1[c]/50[c]) (selecting a unique identifier(s) by filtering), and XI.A.2.e (1[d]/50[d]) (taking first further action relating to the stored information if the first unique identifier is present among the selected unique identifier(s)).

(d) 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].

163. In my opinion, Ribaud-Watanabe teaches claims 15, 36, 67, and 80 for the reasons I explained for claim elements 1[b]/50[b]-1[d]/50[d]. In particular, Ribaud teaches determining if a first unique identifier is present among the first selected one or more unique identifiers when comparing a received client ID with client IDs from downloaded match data. EX1007, ¶¶6, 16, 33, 83-85; Sections XI.A.2.c (1[b]/50[b]) (receiving stored information relating to an entity/object with a first unique identifier), XI.A.2.d (1[c]/50[c]) (selecting a unique identifier(s) by

filtering), and XI.A.2.e (1[d]/50[d]) (taking first further action relating to the stored information if the first unique identifier is present among the selected unique identifier(s)).

- (e) **Claim 20/73: The [method]/[computer program product] of claim [1]/[50] wherein the first further action [additionally] includes [causing the wireless device to determine]/[determining] an address or location associated with the wireless device based at least in part upon the first unique identifier being associated with a pre-determined location, and wherein the wireless device is located indoors where a GPS signal may not be available.**

164. In my opinion, Ribaud-Watanabe teaches claims 20/73.

165. Ribaud teaches *determining a location associated with the wireless device based on the first unique identifier being associated with a pre-determined location* as claimed. As described with reference to claims 11/32/63, Ribaud teaches a mobile device associating location tag information with a detected match. Section XI.A.3.a (claims 11/32/63); EX1007, ¶¶117, 160-161, 166, 185-186, 202, 213, 216. Ribaud explains that the location tags can be used “to provide context for ... detected matches at the location.” EX1007, ¶117. When associating a location tag with a detected match to provide this context, Ribaud teaches determining a location associated with the wireless device detecting matching beacon transmissions as well. EX1007, ¶117. For example, when a wireless device uses match data to detect a match in proximity that corresponds to a location like

“CES-ConferenceRoom4,” “MainStreetCafe,” or “DFWAirport-Terminal3,” the wireless device has also determined that the wireless device is present in that location as well. EX1007, ¶117. In this manner, the wireless device determines an associated location corresponding to its own location based on matches and corresponding location tags.

166. Ribaudo also teaches the wireless device being *located indoors where a GPS signal may not be available* as claimed. For example, Ribaudo describes several indoor locations where matching and location determination may occur: “a hotel, coffee shop, airport” or “ConferenceRoom.” EX1007, ¶¶117, 231 (describing functionality also occurring inside “airplanes” or “trains”).

Additionally, Ribaudo explains that its proximity and location detection may occur without needing to rely on GPS signals. EX1007, ¶¶185, 228. For example, Ribaudo explains that its proximity detection is “readily distinguishable from other potential solutions, which may ... use global position system (GPS) data to determine user location.” EX1007, ¶¶185, 228 (describing the detection of “matched users based on their proximity to one another rather than using triangulation or GPS data”). In view of these teachings, Ribaudo also teaches the claimed match detection and location determination features even when the wireless device is *located indoors where a GPS signal may not be available* as claimed.

- (f) **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.**

167. In my opinion, Ribaud-Watanabe teaches claims 29 and 56.

168. Ribaud teaches *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*. Ribaud 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.” EX1007, ¶215. Ribaud also indicates that match data includes “other information.” EX1007, ¶16. Ribaud also discloses that “advertisements, *personal advertisements*, and classified advertisements may be served on a per wireless access point basis (e.g., a per MAC address basis or per cell tower ID basis)” and “displayed on mobile devices 12 using application 20.” EX1007, ¶217. Ribaud also describes that these advertisements may be provided upon a match, by which its data center 14 enables the mobile device 12 to receive advertisement content “based on implied proximity.” EX1007, ¶¶215-217. . A POSITA would have

found such personalized advertising obvious in view of the Ribaudó's delivering of business-related communications (e.g., "sales," "facilitation of business transactions," "finding a doctor or other service," etc.) based on matching commonalities. EX1007, ¶¶140, 152, 223-224. For example, Ribaudó explains that matching commonalities between a customer and a salesperson may provide "rapport with a prospective client [and] may increase the likelihood of making a sale." EX1007, ¶140.

169. Therefore, the Ribaudó-Watanabe-Behrens combination teaches claims 29 and 56.

(g) 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.

170. In my opinion, Ribaudó-Watanabe teaches claim 30. Ribaudó teaches retrieving content from a server once a match between mobile devices 12 has been determined. *See* Section XI.A.2.e (1[d]/50[d]). I described one example of such content being advertisements with respect to claims 29 and 56. Section XI.A.3.f. Additionally, I note that Ribaudó's determination of a match using a client ID (*unique identifier*) is an example of *information derived from a first/second unique identifier* as recited in Claim 7. That is, the information that is derived is that a match has been determined or detected, and this information is derived using Ribaudó's client ID (*unique identifier*). Based on this match, Ribaudó describes

retrieving commonality information (i.e., the claimed *content*) from a server and displaying this commonality information on a mobile device. For example, Ribaudo 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.” EX1007, ¶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.” EX1007, ¶134. For example, when “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.” EX1007, ¶47; *see also* ¶78. The displayed commonality information corresponds to the claimed *content* received from a server. The mobile device receives this commonality information or *content* from the server for display based on the client ID match. EX1007, ¶¶130-131, 148-150. For example, Ribaudo describes data center 14 providing notifications with commonality information in response to detected matches. EX1007, ¶¶130-131, 148-150. In this manner, Ribaudo describes receiving content, such as commonality information, from a server based on the

determination of a match. These operations may occur to further establish and enable communications between matched mobile devices 12 (e.g., a *first further action*).

171. I also note that Ribaudó's "personal URL" is another example of *information derived from a first unique identifier*. EX1007, ¶¶126-147, FIG. 3. The "personal URL" is derived from a client ID (*unique identifier*) because it is constructed using a client ID. EX1007, ¶¶127-130. For example, Ribaudó provides the following example of a personal URL, which includes a client ID; "www.proprietor_name.net/**clientid**_82740AF3RT432". EX1007, ¶127.

Additionally, I note that Ribaudó explains that match data may include "any suitable information." EX1007, ¶¶49-51. A POSITA would have therefore found it obvious to include a personal URL in the match data. Using the personal URL, Ribaudó describes a mobile device retrieving content such as commonality information from data center 14. EX1007, ¶¶128, 130-132, 134, 138-144, 146-47. For example, in Figure 3, data center 14 receives the URL with the client ID via a "connection request" and then returns "commonalities or other suitable information" to the requesting mobile device. EX1007, ¶¶128, 130. Therefore, it would have also been obvious to use the personal URL in the match data to retrieve and receive content after detecting a match as well. This therefore teaches

receiving content from a server based upon information derived from the first unique identifier.

172. Thus, Ribaudo-Watanabe teaches claim 30.

(h) 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.

173. In my opinion, Ribaudo-Watanabe teaches claims 31 and 61.

174. Ribaudo teaches that a server associated with an account for a user of the wireless device performs a step of sending a message to an email address associated with the account for the user. 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.” EX1007, ¶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.” EX1007, ¶140. Ribaudo teaches that “sales people may use this capability to facilitate sales initiated by emails or other forms of communication.” EX1007, ¶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.” EX1007, ¶152; *see also* ¶¶151, 153. Ribaudo 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.” EX1007, ¶157; *see also* ¶¶30-31 (describing registered users and accounts).

175. Moreover, Ribaudo teaches that the first further action has already been performed. *See* Section XI.A.2.e (1[d]/50[d]). As I described with reference to claim elements 1[d]/50[d], an example of a *first further action* is determining that a match is in proximity. Section XI.A.2.e (1[d]/50[d]). Additionally, the user of mobile device 12a may be notified by data center 14, via email, that communication with mobile device 12b has been established. EX1007, ¶¶148, 157. Ribaudo also teaches that data center 14 may email the user of mobile device 12a in the event that communication between mobile devices was established (i.e., a match) yet no messages between the devices were exchanged (referred to as a “missed encounter”). EX1007, ¶¶151-153.

(i) 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.

176. In my opinion, Ribaud-Watanabe teaches claim 34.

177. Ribaud-Watanabe teaches that the first further action is related to an advertisement tied to a location for the reasons explained in Section XI.A.3.f (claims 29/56). Ribaud 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.” EX1007, ¶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.” EX1007, ¶217. A POSITA would have understood that an advertisement tied to a cell tower ID would be tied to a location. In Ribaud, 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.

(j) Claim 70: The computer program product of claim 50 wherein the first further action additionally includes causing the wireless device to display a current location, based at least in part upon a predetermined

location associated with the first unique identifier, or based at least in part upon information derived from the first unique identifier.

178. In my opinion, Ribaudo-Watanabe teaches claim 70.

179. In particular, Ribaudo teaches *causing the wireless device to display a current location, based at least in part upon a predetermined location associated with the first unique identifier*. As described with reference to claims 11/32/63 and 20/73, Ribaudo teaches a mobile device associating location tag information with a detected match in proximity. Sections XI.A.3.a (11/32/63), XI.A.3.e (20/73); EX1007, ¶¶117, 160-161, 166, 185-186, 202, 213, 216. As explained for claims 20/73, Ribaudo when a mobile device associates a particular location tag with a detected match in proximity, Ribaudo also teaches that mobile device determining its own current location—e.g., at “CES-ConferenceRoom4,” “MainStreetCafe,” or “DFWAirport-Terminal3.” EX1007, ¶117. This determination occurs based on the detected location tag, which provides a “relevant descriptor for the location.” EX1007, ¶117.

180. Ribaudo also indicates that detected location tag information may be displayed on a mobile device. Ribaudo explains that location tags can be “presented to a user on his associated mobile device 12, by application 20 for example.” EX1007, ¶117. Ribaudo further explains that users may view and interact with the displayed location tag information via application 20 and a web

browser. EX1007, ¶¶117-118; *see also* ¶¶78, 109-115 (describing additional tag displays and interactions). In this manner, when a match is detected in proximity, Ribaudó teaches displaying the location tag, which also indicates the detecting mobile device's *current location* based on a *predetermined location associated with the first unique identifier*. EX1007, ¶117.

B. Ground 2: Claims 2-10, 14, 16-19, 21-26, 28, 33, 35, 37-38, 40-49, 51-55, 57-60, 62, 66, 68-69, 71-72, 74-79, and 82-83 are obvious over Watanabe in view of Ribaudó and Behrens.

181. Independent claim 37 appears to take the limitations of independent claims 1 and 50 and recite them twice. Specifically, claim 37 recites the same first plurality of beacon transmissions as claims 1 and 50 and adds a second plurality of beacon transmissions (claim element 37[h]) that 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 (claim elements 37[i]-37[j]).

182. Claim 37 therefore 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 Ribaud-Watanabe's teachings with Behrens' teachings and would have had a reasonable expectation of success.

183. A POSITA would have been motivated to combine the teachings of Ribaud-Watanabe with Behrens to provide a mechanism for facilitating Ribaud's capability of allowing a user to selectively "shield" or "reveal" her true identity in different circumstances. EX1007, ¶¶45-46, 61-62, 68. In my opinion, a POSITA would have had a reasonable expectation of success in combining Ribaud, Watanabe, and Behrens because each relates to detecting nearby wireless devices and establishing communications. EX1007, Abstract, ¶18; EX1006, Abstract; EX1008, 1:6-9. *See supra* Sections XI.2.c-d.

184. As I explained for Ground 1 above, Ribaud and Watanabe teach a mobile device receiving a plurality of proximity beacon transmissions, each including a MAC address, unique identifier, and beacon service identifier. Section XI.A.2.b.

185. Behrens teaches electronic devices that "continuously/repeatedly transmit" "unique identifiers (UID) via non-directed wireless radio frequency transmission." EX1008, 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." EX1008, 11:21-26. Moreover, "[e]ven in the event that the device has a UIDs, the

software may allow use of a different UID.” EX1008, 22:28-29. Behrens teaches that “this may be beneficial to the user” because it “may even allow a user to have multiple or changing UIDs and, therefore, different online identities.” EX1008, 23:1-5. Behrens explicitly discusses that “MAC addresses” are a type of UID. *See* EX1008, 19:8-14. Based on these teachings, a POSITA would thus have understood that Behrens teaches that multiple unique identifiers and MAC addresses may be associated with the same user device, which is used to transmit beacons.

186. 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.” EX1007, ¶68. Ribauda explains that a single device with multiple distinct IDs is beneficial for shielding a true identity. EX1007, ¶46. For instance, Ribauda contemplates that “[t]he client ID may be used to shield the true identity of the user, for privacy purposes for example,” or, [a]lternatively, the client ID may simply be the user ID of the user, which in certain embodiments may reveal the true identity of the user.” EX1007, ¶46. Ribauda also teaches “time-slicing to join and bounce between several networks.” EX1007, ¶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).” EX1007, ¶72. Ribauda 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. Additionally, Ribauda teaches alternatively associating with one network for detecting users in proximity and another network for accessing internet resources). *See* EX1007, ¶72.

187. In view of Ribauda's teaching of using multiple client IDs, a POSITA would have been motivated to implement Behrens' teaching that *multiple unique identifiers* (which include MAC addresses or other unique IDs) may be associated with the same transmitting device or mobile device. Such functionality was known by the priority date of the '971 patent due to its implementation in similar systems such as ones described by Krikorian, Lazaridis, Mgrdechian, and Suzuki. *See* Section VII.C; EX1009; EX1010; EX1027; EX1037. Combining Behrens' teachings would have provided a mechanism for Ribauda to implement multiple client IDs and multiple MAC addresses, which are sent or received at different times. Such functionality was common at the time of the '971 patent's priority date. *See* Section VII.B; EX1009; EX1010; EX1027; EX1037. Additionally, Behrens explains that employing multiple identifiers would provide the benefit of a user having "different online identities" so that the user may, for example, "create a new online identity for an event or party he attends or has attended." EX1008, 23:2-4. This would provide a mechanism for enabling a user or mobile device to

associate multiple unique identifiers with the same entity/object (*i.e.*, the same mobile device user) to facilitate Ribaudó's teaching of using multiple client IDs. EX1007, ¶¶45-46, 61-62, 68. In the combination, the multiple unique identifiers would be included in beacon transmissions (e.g., via Bluetooth) from the same transmitting device, as taught by Behrens. EX1008, 4:21-24, 11:21-26, 18:21-28, 19:5-14, 25:22-25.

188. I also note that a POSITA would have had a reasonable expectation of success in combining Ribaudó-Watanabe with Behrens. For instance, all three describe similar proximity detection techniques in wireless systems that feature both short- range, Bluetooth communication as well as communication to a central server over the Internet. *See, e.g.*, EX1006, ¶¶46-55; EX1007, ¶¶6-7; EX1008, Abstract, 6:1-30, 19:5-14. And, as I discuss above, Ribaudó already contemplates a system that may assign multiple unique identifiers to a given user in order to “shield” or “reveal” her true identity in different circumstances. EX1007, ¶¶45, 68. A POSITA would thus have understood that applying Behrens' teachings to the Ribaudó-Watanabe system would have yielded predictable results. Indeed, as I have previously discussed, using identifiers to shield was well-known to the field prior to the priority date of the '971 patent. *See* Sections VII.B-C. Further, a POSITA would have understood that these references disclose interrelated

teachings based on well-understood technologies that would have been amenable to various well-understood and predictable combinations.

189. 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. 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.

190. 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. Moreover, including identifiers such as MAC addresses in beacon transmissions was known. *See, e.g.*, Section VII.C.

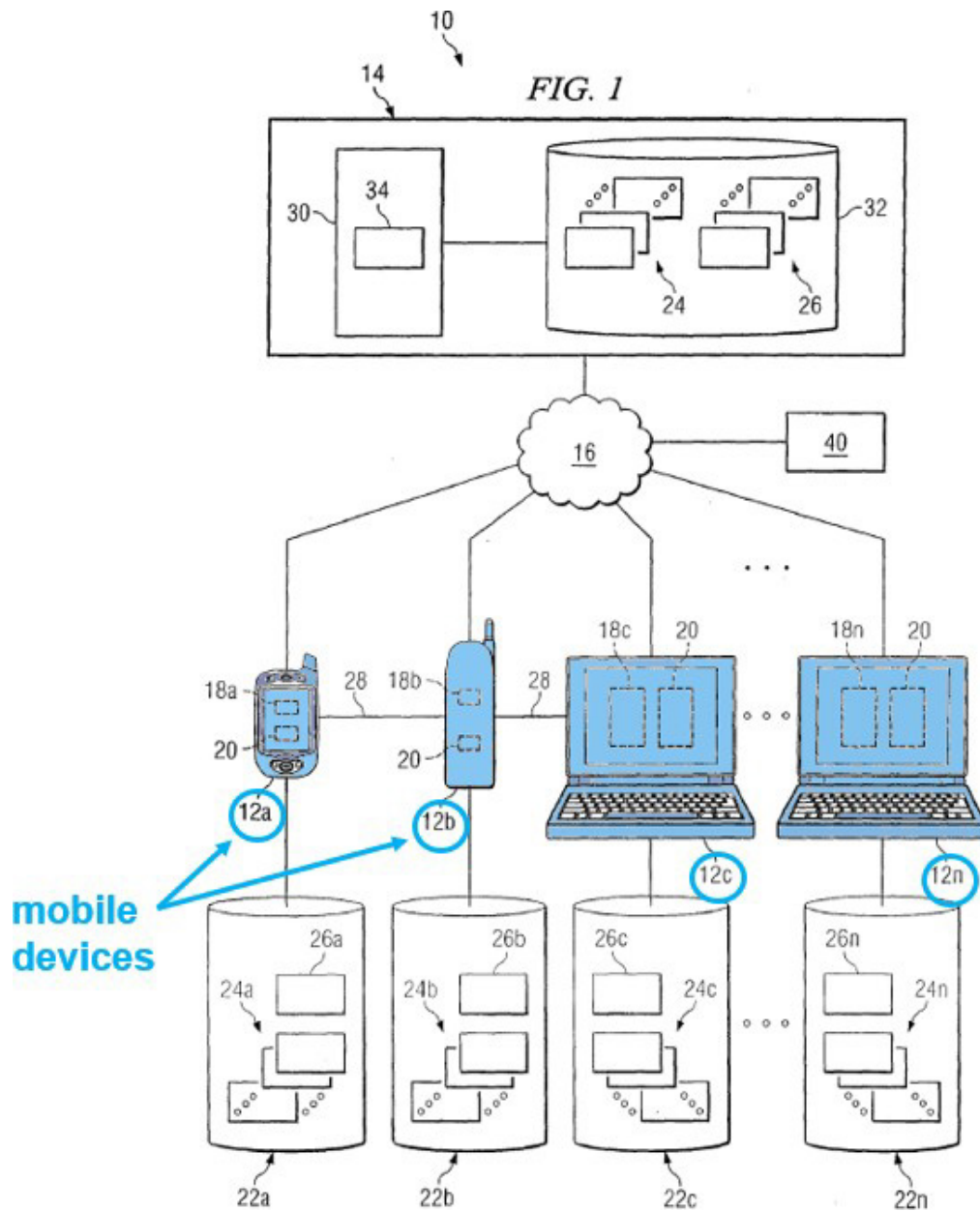
191. Therefore, based on the elements recited in the claims, the disclosures from the Ribaud-Watanabe-Behrens references, and the state of the art at the priority date of the '971 patent, a POSITA would have found it obvious to combine Behrens with Ribaud and Watanabe.

2. Independent Claim 37

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

192. In my opinion, Watanabe in view of Ribaud and Behrens (“Ribaud-Watanabe-Behrens”) teaches the preamble. *See* Section XI.A.2.a (1[pre]/50[pre]).

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



EX1007, FIG. 1 (annotated).

(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;**

193. In my opinion, Ribaud-Watanabe-Behrens teaches Element 37[a].

See Sections XI.A.2.b and XI.A.2.c (1[a]/50[a]–1[b]/50[b]).

194. Ribaud describes that its “[m]obile devices 12 may each include any suitable combination of hardware, software, and firmware to provide the functionality described herein,” and “[e]ach mobile device 12 may include *one or more suitable devices for wireless communication*,” including an “adaptor 18” that “may facilitate communication ... between mobile device 12 and data center 14.” EX1007, ¶¶18-19, FIG. 1. Ribaud explains that “the present invention contemplates any other suitable wireless platforms, including but not limited to BLUETOOTH, ZIGBEE, WiMax, RFID, UWB, GSM, CDMA, a proprietary platform, cell tower triangulation, and GPS.” EX1007, ¶76.

195. Ribaud describes its mobile devices having a radio for providing reception and transmission via a Bluetooth wireless protocol. For instance, Ribaud describes that “[e]ach mobile device 12 may include one or more suitable devices for wireless communication, such as one or more wireless fidelity (Wi-Fi) devices [or] one or more *BLUETOOTH* devices,” for example an “adaptor 18” that “may facilitate communication with other mobile devices 12 (e.g., mobile devices 12b through 12n).” EX1007, ¶¶18-19, 154, 157, 181-184, 205, FIG. 1.

Ribaudo also explains that “BLUETOOTH-enabled mobile devices 12 may use BLUETOOTH technology to detect matches in proximity.” EX1007, ¶¶66-67, 73. Adaptor 18a’s Bluetooth radio teaches the Bluetooth aspects of 37[a]. *See* EX1011 (Proctor Decl.), ¶¶73-89.

196. Ribaudo also describes additional radio functionality for a second wireless protocol, such as a cellular protocol among other wireless protocols. EX1007, ¶¶76, 79, 184. For example, “mobile devices 12 may each be coupled to data center 14 via network 16”—which may include “*wide area networks (WANs)*, [or] all or a portion of a global computer network such as the Internet”—and that the connection may be through a “*wireless link*.” EX1007, ¶¶24-25. Ribaudo’s system may “employ[] a *cellular* connection ... to download from data center 14.” EX1007, ¶204. Adaptor 18a’s cellular/WWAN radio therefore teaches the claimed *second wireless protocol*. *See* EX1011 (Proctor Decl.), ¶¶73-89.

197. Indeed, using short-range (i.e., Bluetooth) and long-range (i.e., cellular connections) for communications between different mobile devices and between a mobile device and a server was known prior to 2008. In addition to Ribaudo-Watanabe-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.

198. Therefore, in my opinion, Ribaud-Watanabe-Behrens teaches Element 37[a].

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

199. In my opinion, Ribaud-Watanabe-Behrens teaches Element 37[b].
See Section XI.A.2.a (1[pre]/50[pre]); EX1007, ¶19.

200. Ribaud teaches mobile devices 12 “may include, for example, ‘laptop’ computers, ‘palmtop’ computers, personal digital assistants, pagers, cellular telephones, game consoles, cameras, or any other suitable types of portable devices.” EX1007, ¶18. Ribaud’s mobile devices 12 also “each include any suitable combination of hardware, software, and firmware to provide the functionality described” including “one or more applications 20 that are based on one or more programming languages” to “facilitate communication with other mobile devices 12” and the data center. EX1007, ¶19.

201. Based on these devices, a POSITA would have recognized that Ribaud teaches 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. “802.11a

MAC layer: firmware/hardware co-design,” *Fourth International Conference on Information, Communications and Signal Processing, 2003* (EX1041) 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. EX1041, 1926-27.

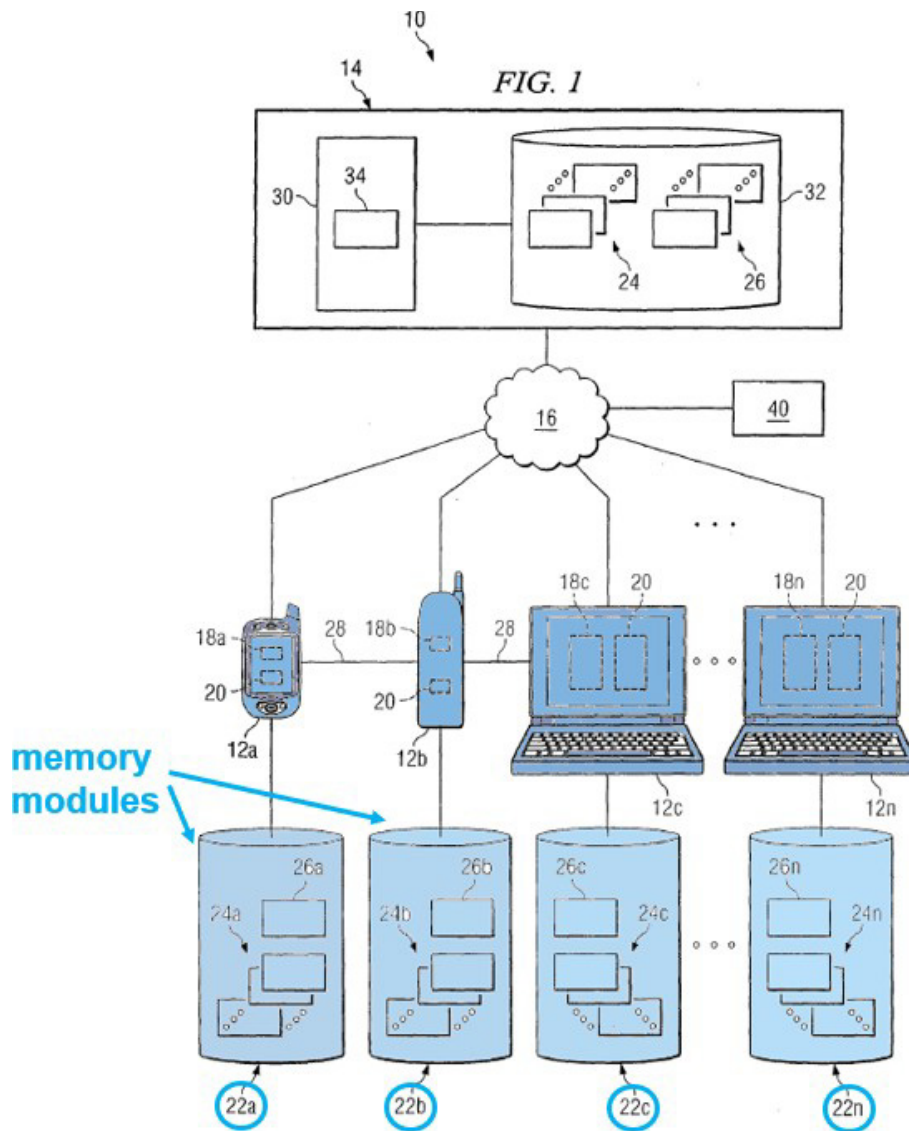
202. I note that Behrens also confirms this understanding and describes hardware used to implement mobile telephones or other “a small, battery-powered handheld device” such as a mobile phone, having “the components necessary for sending out, via short-range and/or medium-range radio frequency, at least one [unique identifier] UID” including “*at least one microprocessor* for managing the wireless radio transmissions as well as for processing and storing data.” EX1008, 20:31-21:15.

203. Moreover, in addition to Ribaud-Watanabe-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.

- (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:**

204. In my opinion, Ribaud-Watanabe-Behrens teaches Element 37[c].
See Section XI.A.2.a (1[pre]/50[pre]); EX1007, ¶¶19, 32. Ribaud explains that its “[m]obile devices 12 may each have an associated memory module 22”—or “any suitable number of memory modules 22 according to particular needs”—that may be “operable to store data as one or more compressed binary files.” EX1007, ¶32, FIG. 1.



EX1007, FIG. 1 (annotated).

205. Specifically, “[m]emory module 22 may store various data associated with the user of mobile device 12,” including “one or more user profiles 24 for the user of mobile device 12[,] ... match data 26 downloaded from data center 14 and identifying one or more predetermined matches for the user[, and] ... any other suitable information, according to particular needs.” EX1007, ¶33; *see also* ¶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. EX1007, 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 Ribaudó 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.

206. 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.” EX1008, 20:31-21:15.

207. Moreover, in addition to the teachings of the Ribaudó-Watanabe-Behrens combination described 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.

(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;

208. In my opinion, Ribaud-Watanabe-Behrens teaches Element 37[d].

See Section XI.A.2.b (1[a]/50[a]).

209. In addition to the reasons I provided above with respect to claim elements 1[a] and 50[a], Ribaud-Watanabe-Behrens teaches that the first plurality of beacon transmissions are received *during a first time period*. A POSITA would have understood that Ribaud’s wireless device receives beacon transmissions from different users, or even the same users, at different times, such as different times during the same day, on different days, etc. Ribaud provides several examples of this functionality. *See, e.g.*, EX1007, ¶¶45-46, 58, 60-61, 64, 68, 72 (describing “time-slicing”), 78, 148, 162-164, FIG. 2. Watanabe also describes similar functionality and confirms that this was well known. *See* EX1006, ¶¶14, 46, 49 (explaining that a plurality of beacons can be transmitted “continuously” or “periodically”).

210. Behrens also describes beacon transmissions transmitted over multiple time periods based on portable electronic devices that “continuously/repeatedly transmit” and scan for “unique identifiers (UID) via non-directed wireless radio frequency transmission” in order to establish social networks. EX1008, Title, 11:1-5. Additionally, Behrens explains that employing multiple identifiers would provide the benefit of a user having “different online identities” so that the user may “create a new online identity for an event or party he attends or has attended.” EX1008, 23:2-4. This further defines a mechanism for enabling a user or mobile device in Ribaudó’s system to associate multiple unique identifiers with the same entity/object (*i.e.*, the same mobile device user) to facilitate using multiple client IDs at different times. EX1007, ¶¶45-46, 68. In the combination, the multiple unique identifiers would be included in beacon transmissions (e.g., via Bluetooth) from the same transmitting device, as taught by Behrens. EX1008, 4:21-24, 11:21-26, 18:21-28, 19:5-14, 25:22-25.

211. As I will further describe with reference to claim elements 37[h]-37[k], the Ribaudó-Watanabe-Behrens combination also teaches changing unique identifiers and MAC addresses over different time periods. *See* Section VI.B; *infra* Sections XI.B.2.i-l (37[h]-37[k]).

212. In addition to Ribaudó-Watanabe-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. Furthermore, using protocols such as Bluetooth for communications between mobile devices and servers was known. *See, e.g.*, Section VII.H.

213. 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. Additionally, including identifiers in beacon transmissions was known. *See, e.g.*, Section VII.C. And continuously or periodically transmitting a beacon signal was also known to a POSITA by 2008. *See, e.g.*, Section VII.D.

(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;

214. In my opinion, Ribaud-Watanabe-Behrens teaches Element 37[e]. *See* Section XI.A.2.c (1[b]/50/[b]). The combination teaches Element 37[e] for the reasons I discussed with respect to Elements 1[b] and 50[b].

215. In addition to Ribaud-Watanabe-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.

- (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;**

216. In my opinion, Ribaud-Watanabe-Behrens teaches Element 37[f].
See Section XI.A.2.d (1[c]/50[c]). The combination teaches Element 37[f] for the reasons I discussed with respect to Elements 1[c] and 50[c].

217. In addition to Ribaud-Watanabe-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.

- (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;**

218. In my opinion, Ribaud-Watanabe-Behrens teaches Element 37[g].
See Section XI.A.2.e (1[d]/50[d]). The combination teaches Element 37[g] for the reasons I discussed with respect to Elements 1[d] and 50[d].

219. In addition to Ribaud-Watanabe-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.

- (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;**

220. In my opinion, Ribaud-Watanabe-Behrens teaches Element 37[h].

221. 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 I explained in Section XI.B.1 and XI.B.2.e (37[d]), a mobile device in the Ribaud-Watanabe-Behrens combination would receive a second plurality of beacon transmissions during the claimed “*second time period*” as well.

222. In addition to Ribaud’s context and framework, Behrens describes receiving unique identifiers (UIDs) that are beacons at different time periods. EX1008, 30:23-31:13. For example, Behrens describes a portable electronic device that scans “continuously/repeatedly for UIDs sent out by other devices” and

records these UUIDs in a log. EX1008, 10:24-11:9, 28:19-20, 31:6-13. “When such a device receives another device’s UUID, it records that UUID and measures the length of time during which it continues to receive that UUID. The device stores the received UUID, along with the time, date and duration of the reception.” EX1008, 11:11-17. Behrens further describes the mobile device determining that the UUID is no longer received but then subsequently detecting additional identifiers at a later time:

When the first device stops receiving the second device’s identifier (for a specified amount of time), it stores that event in its “seen log” along with a time and date stamp.

If the first device again receives the second device’s identifier, the first device again stores the event in its “seen log” with a time and date stamp. Optionally, **if the time between the last reception and the renewed reception of the same identifier** falls within a specified amount of time, the device may adjust the event and prolong the ‘seen’ session in the log.

EX1008, 30:27-31:4.

223. In this manner, Behrens describes the transmission of unique identifiers occurring at multiple time periods. Continuously or periodically transmitting a beacon signal, over different time periods, was known to a POSITA by 2008. *See, e.g.*, Section VII.D (citing, e.g., EX1026 (Bluetooth Specification), FIG. 72, 131-132; EX1025 (Wi-Fi Specification), 80-81, 419-420, FIG. 11-1;

EX1009 (Krikorian), ¶25; EX1027 (Lazaridis), 2:3-10, 3:44-46, 3:59-65). In the Ribaud-Watanabe-Behrens combination, this would include receiving a *second plurality of beacon transmissions* during a *second time period*, where each beacon transmissions would include a MAC address, a unique identifier, and a beacon service identifier as previously explained with reference to claim elements 1[a]/50[a]. Section XI.A.2.b (1[a]/50[a]).

224. In addition to Ribaud-Watanabe-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.

225. 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. Additionally, including identifiers in beacon transmissions was known. *See, e.g.*, Section VII.C.

- (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;

226. In my opinion, Ribaud-Watanabe-Behrens teaches Element 37[i] for the same reasons presented with reference to claim elements 1[c], 50[c], and 37[f]. *See* Sections XI.A.2.d (1[c]/50[c]), XI.B.2.g (37[f]).

227. For instance, the selection of unique identifiers based on filtering beacon transmissions based on a beacon service identifier occurs in the same way. Ribaud describes filtering while Watanabe describes filtering based on particular service codes. EX1007, ¶¶6-7, 58, 61, 64; EX1006, ¶¶41, 48-49, 51-52, 57. For instance, Ribaud describes “techniques for filtering matches detected in proximity,” the filtration depending on the particular service used by Ribaud’s mobile devices. EX1007, ¶64. In view of these teachings, a particular mobile device from Ribaud would have been configured to perform filtering for the *same particular beacon service identifier* regardless of whether the mobile device detected a first or second plurality of beacon transmissions. For example, when Ribaud’s mobile device identifies a beacon service identifier corresponding to matching service like a “dating” service, the mobile device would detect this “dating” service identifier (e.g., via Watanabe’s service code) in any plurality of beacon transmissions. EX1007, ¶¶55, 90, 97-104, 223. In Ribaud, a user “may choose to be matched based on one or more of the following nine categories that may each be as granular as the user desires: (1) Background, (2) Hobbies/Interests,

(3) Organizations, (4) Friends and Acquaintances, (5) Business Networking, (6) Dating, (7) Networking Goals, (8) Market (buy/sell items, free agent services), and (9) Employment.” EX1007, ¶90. Other systems before 2008, such as Krikorian, describe a similar filtration feature for identifying matches specific to an identifier and performing additional operations thereto. EX1009, ¶26. The selection of the unique identifier would also occur in the same manner and would be subsequently used to determine whether a match has been detected. *See* Sections XI.A.2.d (1[c]/50[c]), XI.B.2.g (37[f]). Thus, the Ribaud-Watanabe-Behrens combination teaches 37[i].

228. In addition to Ribaud-Watanabe-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., EX1031 (Godfrey) ¶¶11, 35; EX1009 (Krikorian) ¶¶4-5, 26; EX1032 (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**

229. In my opinion, Ribaud-Watanabe-Behrens teaches Element 37[j] for the reasons presented with reference to claim elements 1[d], 50[d], and 37[g] and as further explained below. *See* Sections XI.A.2.e (1[d]/50[d]), XI.B.2.h (37[g]).

**(i) 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**

230. In my opinion, the Ribaud-Watanabe-Behrens combination teaches taking the claimed *second further action*. As I explained with reference to claim elements 1[d]/50[d], both Ribaud and Watanabe teach performing further actions relating to the stored information based on the detection of a particular unique identifier. *See* Sections XI.A.2.e (1[d]/50[d]) and XI.B.2.h (37[g]). Thus, the Ribaud-Watanabe-Behrens combination teaches the claimed *second further action* for the same reasons presented for taking the *first further action*. *See* Sections XI.A.2.e (1[d]/50[d]) and XI.B.2.h (37[g]).

**(ii) 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**

231. In my opinion, the Ribaud-Watanabe-Behrens combination also teaches a *second unique identifier* being *associated with the same entity or object*

associated with a *first unique identifier*. The combination also teaches the *second unique identifier* as *not equal to the first unique identifier*.

232. Specifically, Ribaud and Behrens describe assigning multiple unique identifiers to a given transmitting device. For example, Ribaud discloses one or more client IDs to a particular mobile device. EX1007, ¶68. Behrens also discloses multiple or changing UIDs, to which Behrens also describes MAC addresses as UIDs. EX1008, 22:28-29, 23:1-5 (disclosing “***multiple or changing UIDs***”). This beneficially enhances privacy, by allowing “different online identities” as described in Behrens and/or the ability to “shield” or “reveal” one’s identity depending on context as described in Ribaud. EX1007, ¶¶46, 61-62; EX1008, 23:1-5.

233. Behrens teaches electronic devices that transmit unique identifiers (UIDs) that “may consist of or include a [WLAN] MAC (media access control) address, Bluetooth Device Address (i.e., BD_ADDR), or other unique or quasi-unique identifier.” EX1008, 11:21-26, 22:25-27. Behrens further teaches that its “software may instruct the device for sending out a UID via short or medium range wireless transmission” and may “obtain the device’s own UID(s)” or “assign (or allow the user to assign) a UID.” EX1008, 22:24-28. Moreover, in the event that a device has multiple UIDs, “the software may allow use of a different UID.” EX1008, 22:28-29. Behrens teaches that “this may be beneficial to the user”

because it “may even allow a user to have *multiple or changing UIDs* and, therefore, different online identities.” EX1008, 23:1-5. These changing UIDs “may also be linked to a single user account,” which allows a user to manage them. EX1008, 23:1-5.

234. In view of Behren’s teachings, a POSITA would have found it obvious for Ribaudó’s mobile devices to beacon different client IDs (i.e., claimed *unique identifiers*) at different times for at least masking or privacy purposes as well as for different contexts. *See* EX1007, ¶62 (describing using different user IDs with different masks), 46 (client ID may be user ID). Indeed, Ribaudó discusses the ability of a mobile device to include different user IDs or client IDs and use different IDs at different occasions or times. EX1007, ¶¶61-62.

235. In this manner, Ribaudó and Behrens describe a *second unique identifier* that is *associated with the same entity or object* as the *first unique identifier* and that the second and first identifiers are *not equal* as claimed.

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

236. The Ribaudó-Watanabe-Behrens combination also teaches that the received beacon transmissions including the first and second unique identifiers are received from the same transmitting device. For example, as I previously explained, Ribaudó describes assigning multiple IDs to a mobile device. EX1007,

¶¶45-46, 68, 72, 84-85. Ribaud describes generating “one or more identifiers (IDs) for a user” as well as assigning at least two types of client IDs to a mobile device: a public client ID and a user ID that “may reveal the true identity of the user.” EX1007, ¶¶45-46. In this manner, it is my opinion that Ribaud teaches the ability for a particular mobile device to transmit beacons using different identifiers.

237. Behrens confirms this understanding. Behrens describes assigning “*multiple or changing UIDs*” to a mobile device where each UID may be linked to a single user account. EX1008, 23:1-5. Behrens also describes the mobile device transmitting a particular UID “via short or medium range wireless transmission.” EX1008, 22:24-25, 23:7-24:5. Indeed, when a device has multiple or changing UIDs, the mobile device may select one or more of them to transmit. EX1008, 22:24-29 (“The software may instruct the device for sending out a UID via short or medium range wireless transmission. The software may obtain the device’s own UID(s), such as the device’s Bluetooth Device Address or WLAN MAC address, for example. The software may also, however, assign (or allow the user to assign) a UID. Even in the event that the device has a UIDs, the software may allow use of a different UID.”).

238. Therefore, the Ribaud-Watanabe-Behrens combination teaches a mobile device (i.e., the same mobile device or the *same transmitting device*) being capable of sending beacon transmissions using different unique identifiers.

239. In addition to Ribaud-Watanabe-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.

- (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.**

240. In my opinion, Ribaud-Watanabe-Behrens teaches Element 37[k].

- (i) **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**

241. As I previously explained, Behrens teaches multiple or changing MAC addresses. Behrens teaches that UIDs—such as MAC addresses—can change.⁷ EX1008, 11:21-26, 19:8-14, 22:25-27, 23:1-5. For example, as I explain above with reference to claim element 37[j], Behrens describes the use of “*multiple or changing UIDs*.” EX1008, 23:1-5. Behrens further explains that UIDs “may consist of or include a MAC (media access control) address, Bluetooth

⁷ As I explained for 1[a]/50[a] and 37[j] and for clarity here, Ribaud's client IDs teach the claimed “*unique identifiers*.” Ribaud in view of Behrens (and Watanabe) renders obvious client IDs changing over time.

Device Address (i.e., BD_ADDR), or other unique or quasi-unique identifier.”

EX1008, 11:21-26, 22:25-27. In this manner, Behrens teaches “MAC addresses” as a type of UID. EX1008, 19:5-14 (“According to a preferred embodiment of the third aspect of the invention, portable electronic devices send out via non-directional, short-range and/or medium-range radio frequency transmission, at least one unique identifier (UID) continuously or repeatedly, generally at a variable interval. This UID may consist of any unique or quasi-unique code, number, address, symbol, or a combination thereof, which uniquely identifies a device, and, by association, the owner of the device. Furthermore, existing networking addresses, such as media access control addresses (MAC addresses) or Bluetooth Device Addresses may be used. In 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.”). For example, Behrens describes using “a combination of different types of UIDs” which may include “Bluetooth Device Addresses, WLAN *MAC addresses and other types of UIDS*” when providing beacon transmissions. EX1008, 25:22-25. Accordingly, Behrens describes multiple or changing MAC addresses that may be used in beacon transmissions. This is further reinforced by the notion that other systems existing before the 2008 priority date of the ’971 patent commonly used MAC addresses in beacon transmissions. *See* Section VII.B. In view of this, it is my opinion that Behrens teaches that

multiple MAC addresses and unique identifiers may be associated with the same user and/or mobile device that transmits beacons. In view of Behrens's teachings, a POSITA would have found it obvious for Ribaudó's mobile devices to beacon different MAC addresses at different times for the reasons that I previously presented. *See* Section XI.B.1.

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

242. As I explained with reference to claim element 37[i] as well as elements 1[c]/50[c], and 37[f], the Ribaudó-Watanabe-Behrens combination teaches multiple beacon transmissions including the same particular beacon service identifier. *See* Sections XI.A.2.d (1[c]/50[c]), XI.B.2.g (37[f]), XI.B.2.j (37[i]). Taken with Behrens's teaching of multiple changing unique identifiers and/or MAC addresses, the Ribaudó-Watanabe-Behrens combination still teaches the beacon transmissions maintaining the same particular beacon service identifier (e.g., a particular service code from Watanabe). *See* Sections XI.A.2.d (1[c]/50[c]), XI.B.2.g (37[f]), XI.B.2.j (37[i]); EX1008, 11:21-26, 22:25-27, 23:1-5. For example, if the particular service is a "dating" service or a business networking service, as described in Ribaudó, the beacon transmissions in the combination would still include an identification of this service even when unique identifiers and/or MAC addresses are changing. Sections XI.A.1, XI.A.2.d (1[c]/50[c]), XI.B.2.g (37[f]), XI.B.2.j (37[i]) (explaining the beacon transmission filtering

provided by Watanabe based on a type of service). Thus, the Ribaud-Watanabe-Behrens combination teaches each beacon transmissions to include *the same particular beacon service identifier*.

243. In addition to Ribaud-Watanabe-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 and SSID identifiers could be used to identify a single device and/or network by 2008. *See, e.g.,* Section VII.B.

3. Dependent Claims 2-10, 14, 16-19, 21-26, 28, 33, 35, 38, 40-49, 51-55, 57-60, 62, 66, 68-69, 71-72, 74-79, and 82-83

(a) Claims 2 and 51

(i) 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

244. In my opinion, Ribaud-Watanabe-Behrens teaches the preamble, to the extent it is limiting. *See* Section XI.B.2.e (37[d]).

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

245. In my opinion, Ribaud-Watanabe-Behrens teaches Elements 2[a]/51[a]. *See* Section XI.B.2.i (37[h]).

- (iii) **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;**

246. In my opinion, Ribaud-Watanabe-Behrens teaches Elements 2[b]/51[b]. *See* Section XI.B.2.i (37[h]).

- (iv) **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

247. In my opinion, Ribaud-Watanabe-Behrens teaches Elements 2[c]/51[c]. *See* Section XI.B.2.j (37[i]).

- (v) **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.**

248. In my opinion, Ribaud-Watanabe-Behrens teaches Elements 2[d]/51[d]. *See* Section XI.B.2.k (37[j]).

- (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.

249. In my opinion, Ribaud-Watanabe-Behrens teaches claims 3 and 52.

See Section XI.B.2.e (37[d]), XI.B.2.1 (37[k]).

- (i) 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**

250. Ribaud-Watanabe-Behrens teaches this limitation for the reasons explained in Section XI.B.2.1 (37[k]).

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

251. As explained in Sections XI.A.2.b (1[a]/50[a]), XI.B.2.e (37[d]), XI.B.2.g (37[f]), and XI.B.2.1 (37[k]), the Ribaud-Watanabe-Behrens combination describes the first plurality of beacon transmissions received during the first time period including a particular service identifier and a first unique identifier. *See also* EX1007, ¶72 (teaching “time-slicing to join and bounce between several networks.”).

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

252. As I explained in Section XI.B.2.i (37[h]), the plurality of beacon transmissions sent during the *second* time period would include the same service identifier and the second unique identifier based on Behrens's teachings of changing UIDs. For example, the Ribaud-Watanabe-Behrens combination teaches beacon transmissions in the first time period having a particular service identifier as well as a unique identifier and a MAC address. *See* Section XI.B.2.e. (37[d]). The combination also teaches beacon transmissions in the second time period including the same service identifier but different unique identifiers and MAC addresses. Sections XI.B.2.k-1 (37[j]-37[k]). A POSITA would have recognized and found it obvious that based on these teachings, no transmissions during the first time period would have included both a second unique identifier and the same service identifier.

(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.

253. In my opinion, Ribaud-Watanabe-Behrens teaches claims 4, 40, and 53 because, as I explained in Sections XI.A.2.e (1[d]/50[d]), XI.B.2.i (37[h]), and XI.B.2.k (37[j]), Ribaud's mobile device determines whether an entity associated

with a proximity beacon service (any of Ribaudo's "nine categories" for providing a matching service, such as a "dating" service or "business networking" service) is in proximity based on a beacon service identifier such as Watanabe's service code. EX1007, ¶90. Ribaudo describes performing various actions (e.g., a *second further action*) in response to this determination. *See also* Section VII.G (where I described actions taken if a match is determined in comparable systems before the 2008 priority date). These actions include establishing communication between users of mobile devices 12, notifying a mobile device 12 of a match, uploading match data to data center 14, and retrieving content from data center 14 to display a match value on the mobile device 12. EX1007, ¶¶17, 47, 78, 87, 134. Further, Ribaudo also describes an "application" that has been launched on the mobile device to provide such functionality. EX1007, ¶¶84-85, 120-125, 141. Therefore, Ribaudo teaches a second further action based upon a function currently being performed on a device (e.g., operating a matching or dating application).

(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.

254. In my opinion, Ribaudo-Watanabe-Behrens teaches claims 5, 41, and 54.

255. Ribaudo teaches that the function is related to a shared application.

For example, 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.” EX1007, ¶120; *see also* ¶¶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. EX1007, ¶¶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"). I also note that Figure 1 depicts application 20 on multiple devices. Ribaud also 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." EX1007, ¶120; *see also* ¶¶123, 139 (second user may "acquire application 20 from another user ... to engage in messaging"), 220.

- (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.**

256. In my opinion, Ribaud-Watanabe-Behrens teaches claims 6 and 55. *See* Sections XI.A.2.e (1[d]/50[d]), XI.B.3.a.v (2[d]/51[d]), and XI.A.3.f (claims 29/56).

- (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.

257. In my opinion, Ribaud-Watanabe-Behrens teaches claims 7, 42, and 57. *See* Sections XI.A.2.e (1[d]/50[d]), XI.B.3.a.5 (claims 2 and 51), and XI.A.3.g (claim 30).

(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].

258. In my opinion, Ribaud-Watanabe-Behrens teaches claims 8, 43, and 59.

259. Ribaud teaches *sending a message to another device associated with an account* related to the first or second unique identifiers. Ribaud 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.” EX1007, ¶79. Ribaud 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.” EX1007, ¶79. Moreover, Ribaudo teaches that “each message that a user receives containing match data 26 identifying a match may include instructions for replying to the message” and “[i]f a user replies to the message, the message may be sent anonymously to the identified match using, for example, an SMS message routed through data center 14 or another suitable location.” EX1007, ¶164. Ribaudo indicates that messages between mobile devices 12 are related to the first and second unique identifiers received by the mobile device 12a and the users may be registered users who have user accounts. *See* EX1007, ¶¶30-31; Section XI.A.2.e (1[d]/50[d]).

- (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.**

260. In my opinion, Ribaudo-Watanabe-Behrens teaches claim 9. *See* Sections XI.A.2.e (1[d]/50[d]), XI.B.3.a.5 (2[d]/51[d]), and XI.A.3.h (31/61). In addition to the reasons I previously explained, I also note that Ribaudo’s email corresponds to the detected mobile device or a user corresponding to the detected mobile device and therefore relates to a “*particular entity or object*” as stated in

claim 9. EX1007, ¶¶151-153; Sections XI.A.2.e (1[d]/50[d]), XI.B.3.a.5
(2[d]/51[d]), XI.A.3.h (31/61).

- (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.**

261. In my opinion, Ribaud-Watanabe-Behrens teaches claims 10, 44, and 62. At the outset, I note that the '971 patent only appears to mention “preventing sending” one time in the specification. EX1001, 2:54-56. This language tracks the claim language and does not further describe what “preventing” entails, requires, or how it should be implemented. This lack of additional detail would have suggested to a POSITA that the claimed “preventing” would have been obvious.

262. For example, Ribaud teaches blocking actions, which are examples of the claimed “preventing” recited in claim 10. EX1007, ¶¶ 44, 99, 101-102. For example, “blocking a user may prevent a match from occurring with respect to the blocked user[.]” EX1007, ¶101. Additionally, Ribaud teaches that a user may filter matches based on time or location, thus preventing certain types of matches for a certain time. EX1007, ¶¶55, 58, 61, 229. For example, “at a bar the user may be interested in being notified of business networking matches only on a particular occasion, but at a later time, the user may also be open to being notified of

romantic matches.” EX1007, ¶58. Further, as discussed in detail below, Behrens teaches the concept of blocking and blacklisting users, which involves ignoring certain user IDs. EX1008, 6:13-17, 10:20-22, 20:10-20, 26:1-8. A POSITA would have understood or found obvious that a blocked or blacklisted client ID would be ignored and prevented from being sent to the server. A POSITA would have found it obvious to prevent sending a client ID to the server to save time and transmission bandwidth, power, etc., for the mobile device. This would have reduced wasting computing resources.

263. Ribaudó also teaches preventing the sending of a unique identifier to a server when determining whether a detected identifier matches a client ID that has already been downloaded to a mobile device as “pre-processed match data.” EX1007, ¶¶6-7 (describing match determination “*without consulting the data center*”); *see also* Abstract, ¶¶16, 48-51, cl. 9; Sections XI.A.2.c-XI.A.2.d (1[b]/50[b]-1[c]/50[c]). When no additional information is needed from the server to determine that the detected mobile device is in proximity, the mobile device will not send a unique identifier to a server. Specifically, Ribaudó states that its mobile devices are able to identify matches “without consulting the data” which includes one or more servers. EX1007, ¶¶6-7, 34-35. Ribaudó’s description of identifying matches without consulting data center 14 is contrasted with Ribaudó’s other example where **not** all match IDs are pre-synchronized to a mobile device to

conserve storage space. EX1007, ¶204. In this case, “a user may detect other users in proximity using a BLUETOOTH device, but *then perform a lookup of the detected user* in proximity” to identify matches. EX1007, ¶205. In view of these contrasting examples, Ribauda teaches preventing the sending of a unique identifier when pre-processed match data has already been downloaded and matches can be identified without needing to transmit the unique identifier to a server. A POSITA would have found it obvious to prevent sending a client ID to the server to save time and transmission bandwidth, power, etc., for the mobile device. This would have reduced wasting computing resources.

264. Additionally, Behrens also teaches preventing sending of the second unique identifier or information derived from it by the wireless device to the server(s). Behrens teaches that a user may “instruct the server to ignore specific UIDs,” “tell the server to block specific UIDs, or to have the server instruct his portable device to ignore specific UIDs and vice versa.” EX1008, 20:10-15. Behrens also teaches that “blacklists containing specific UIDs may be used to eliminate these UIDs from being associated with others.” EX1008, 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.” EX1008, 26:2-3. In combination with Ribauda’s discussion of detecting and identifying matches without the need to consult a server, a POSITA would have found it obvious to additionally instruct

the wireless device not to send specific UUIDs rather than send them and have them ignored because it would achieve the same result but reduce use of transmission bandwidth and power. These would have been benefits that a POSITA would have known to implement. Indeed, at the time of the '971 patent's priority date, systems had monitored power consumption for unneeded beacon transmissions. EX1009, ¶25 ("Wireless 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.").

265. Ribaudo teaches that the second further action is related to the second unique identifier for the reasons that I explained in Sections XI.B.2.k (37[j]) and XI.B.3.a.v (2[d]/51[d]). In the Ribaudo-Watanabe-Behrens combination, the second further action involving the second unique identifier, as taught by Ribaudo and Behrens, 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. Sections XI.B.2.k (37[j]) and XI.B.3.a.v (2[d]/51[d]).

- (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.

266. In my opinion, Ribaud-Watanabe teaches claims 14 and 66 for the reasons explained in Sections XI.B.2.f, XI.B.2.i, XI.B.3.a.iii, (37[e], 37[h], 2[b]/51[b]) (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.2.j, XI.B.3.a.iv (37[i], 2[c]/51[c]) (selecting a unique identifier(s) by filtering), and XI.B.2.k, XI.B.3.a.v (37[j], 2[d]/51[d]) (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.c (claims 13/65). This operation and sequence described with reference to claims 2/51 teaches stored information being received prior to performing the first further action.

(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.

267. In my opinion, Ribaud-Watanabe-Behrens teaches claims 16 and 68. *See* Section XI.A.2.b (1[a]/50[a]). For example, Watanabe teaches using a particular service code to identify a service that is usable by multiple beacon transmitter devices.

268. Watanabe indicates that “AP managing unit 11-1 manages services S1, S2, and S3,” “AP managing unit 11-2 manages services S2 and S3,” and “AP

managing unit 11-3 manages service S3.” EX1006, ¶40. This teaches multiple beacon transmitter devices capable of transmitting the same particular beacon service identifier. In the Ribaudo-Watanabe-Behrens combination, Ribaudo’s mobile device 12 would beacon one of Watanabe’s service identifiers (e.g., “S3”) based on the type of matching service used by the mobile device 12 (e.g., a dating service).

269. In the Ribaudo-Watanabe-Behrens combination, a POSITA would have found it obvious and would have been motivated to use the same “service code 202” described in Watanabe for all mobile devices participating in Ribaudo’s matching service to convey participation. EX1007, ¶¶97-104, 123. I explained the motivation for this combination in Section XI.A.1. In the combination, all users within a given area would use the same service code to identify the matching service and to identify beacon transmissions from other participants of the same matching service. The same service code would indicate that all beacon transmissions including that service code would be associated with the same service, such as Ribaudo’s online matching platform and/or dating service. Section XI.A.1. As I explained above, using beacon service identifiers to identify devices, networks, and/or services was also known by 2008. Section VII.A.

- (I) Claims 17/33/45/69: The [method]/[computer program product]/[mobile wireless device] of claim [2/37/51] wherein [at least one of] the [first or] second further action comprises: determining[, based upon at**

least a portion of the stored information,] that the beacon transmitter is associated with a predetermined location.

270. Ribaudo-Watanabe-Behrens teaches claims 17/33/45/69 for the reasons presented for claims 11/32/63. *See* Section XI.A.3.a (11/32/63).

(m) 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.

271. In my opinion, Ribaudo-Watanabe-Behrens teaches claim 18.

272. Ribaudo teaches that the *steps performed at the wireless device are performed as a result of an application program executing on the wireless device.*

Ribaudo teaches that “the user of mobile device 12a launches application 20 on mobile device 12a,” which “may attempt to detect other mobile devices 12 in proximity to mobile device 12a” by using match data “(e.g., the match IDs) downloaded from data center 14” and beaconing “data such as the client ID of the user associated with mobile device 12a.” EX1007, ¶84; *see also* ¶¶120 (“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’”), FIG. 1 (application 20). In the Ribaudo-Watanabe-Behrens combination, Ribaudo’s application would be installed and executed on Watanabe’s wireless device to perform the recited steps.

- (n) **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.**

273. In my opinion, Ribaud-Watanabe-Behrens teaches claims 19 and 72.

See Sections XI.A.3.i (34) and XI.B.3.a.5 (2[d]/51[d]).

- (o) **Claims 21/47/74: The [method]/[mobile wireless device]/[computer program product] of claim [2]/[37]/[51] wherein the second further action includes [causing the wireless device to determine]/[determining] an address or location associated with the wireless device based at least in part upon the second unique identifier being associated with a pre-determined location, wherein the wireless device is located indoors where a GPS signal may not be available.**

274. In my opinion, Ribaud-Watanabe-Behrens teaches claims 21/47/74

for the same reasons I discussed with respect to claims 20/73. *See* Sections

XI.B.3.e (20/73).

- (p) **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.**

275. In my opinion, Ribaud-Watanabe-Behrens teaches claims 22, 48, and 75.

276. Ribaud teaches that “[m]obile device 12 may notify its user if such a match is detected in proximity, allowing the user to initiate an interaction with the

detected match if desired.” EX1007, ¶26; *see also* EX1007, ¶79 (describing that mobile devices “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.”). Once an interaction is initiated, mobile devices may exchange messages amongst each other and access user profile information present on a respective mobile device. EX1007, ¶¶78-79, 81-83, 137, 151-153 (describing delayed communication in which a user has a fixed period of time to communication and notification may be provided by access via a website). For instance, Ribauda describes data communications between two mobile devices in a manner that allows one mobile device to access “user profile 24” which is stored on a second mobile device. EX1007, ¶137. Thus, a first mobile device is allowed to *access* a second mobile device (*i.e., device associated with the wireless beacon service*) to perform further communications or access user profile information.

277. As I described for claim 19, the user is also provided access to an advertisement. EX1007, ¶215; Section XI.B.3.n. Therefore, Ribauda also teaches allowing a user associated with the wireless device access to an object (e.g., advertisement) associated with the wireless beacon service.

(q) 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].

278. Ribaud-Watanabe-Behrens teaches claim 23. *See* Sections XI.A.2.e (1[d]/50[d]), XI.B.3.a (2[c]/51[c]) and XI.A.2.k. (37[j]).

279. Ribaud teaches *controlling further communications between the mobile device and at least one device or server associated with an entity or object in proximity* with the mobile device via, for example, enabling communications between mobile devices, controlling advertising, and/or blocking communications. For example, I discussed with regards to claims 22, 48, and 75, when a proximity match is detected, Ribaud's mobile devices may exchange messages and access user profile information present on a respective mobile device. EX1007, ¶¶78-79, 81-83, 137, 151-153 (delayed communications with fixed period to communicate); Section XI.B.3.p (claims 22/48/75). This enablement of communications is an example of controlling communications between two wireless devices associated with an entity in proximity to the wireless device (e.g., the user or owner of the other device). I also note that Ribaud's description of a determination of a match using a unique identifier also discloses an example of *information derived from a first/second unique identifier* for the reasons I presented for claim 30. Section XI.A.3.g (claim 30). As I previously explained, the use of a personal URL that was received from another mobile device in proximity to establish communications

also teaches the claimed *information derived* based on the inclusion of a client ID in the personal URL. Section XI.A.3.g (claim 30).

280. For instance, Ribaudo further describes controlling the types of communications (e.g., advertisements) sent to a wireless device based on the wireless device's proximity to a location, such as a wireless access point or cell tower. *See, e.g.*, EX1007, ¶140, ¶217 (“[A]dvertisements, personal advertisements, and classified advertisements may be served on a per wireless access point basis (e.g., a per MAC address basis or per cell tower ID basis). ... Data center 14 or another suitable component of system 10 may create a feedback loop similar to a cookie, which may be used to attach a user's preferences, purchasing patterns, destinations, and other personalized information to suitable wireless access points (e.g., MAC addresses or cell tower IDs).”).

281. Ribaudo also discloses “controlling further communications” by facilitating or stymying communications (e.g., a “match”) based on user preferences (e.g., “blocking”), *see, e.g.*, EX1007, ¶¶47, 101, or based on location or time. *See, e.g.*, EX1007, ¶¶117, 160, 163.

(r) 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.**

282. In my opinion, Ribaud-Watanabe-Behrens teaches claims 24, 82, and 77.

283. Ribaud teaches receiving, at the wireless device, timing notification information for coordination of active times for beacon transmissions. Ribaud teaches data center 14 distributing match data to mobile devices for beacon detection “at a particular location and/or time” and also allowing match detection to be “scheduled in advance,” which teaches the claimed *timing notification information*. EX1007, ¶¶160-162; *see also* ¶¶84-85. Ribaud teaches that “matches may be filtered by time of the detected match in proximity.” EX1007, ¶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).” EX1007, ¶64. Ribaud 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.” EX1007, ¶78; *see also* ¶¶152, 229 (describing match “availability settings” based on time of day). Additionally, match data “may be sent to some or all users who are members of a particular group at a particular time or location.” EX1007, ¶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.” EX1007, ¶163. Match data “may be sent to users during these breaks to facilitate discussions between certain attendees.” EX1007, ¶163.

- (s) 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.**

284. In my opinion, Ribaud-Watanabe-Behrens teaches claim 25 for the reasons explained in Section XI.B.3.r (claims 24/82/77).

285. Furthermore, Ribaud teaches that the wireless device’s receipt of the timing notification information is not directly from the beacon transmitter. Rather, Ribaud teaches that data center 14—not another mobile device—provides timing notification information when distributing match data. EX1007, ¶¶82-83 (data center 14 distributing match data), 162-163 (match data distributed at “specified times” or according to a “schedule”), 201.

- (t) 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.

286. In my opinion, Ribaud-Watanabe-Behrens teaches claims 26, 38, and 79. Sections XI.B.3.a.iii-XI.B.3.a.v (2[b]/51[b]-2[d]/51[d]) and XI.B.2.i-XI.B.2.k (37[h]-37[j]); EX1007, ¶85.

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

287. In my opinion, Ribaud-Watanabe-Behrens teaches claim 28 for the reasons I discussed with respect to claim elements 1[a]/50[a]. Section XI.A.2.b (1[a]/50[a]); EX1007, ¶¶18-19; EX1006 ¶27.

(v) 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.

288. In my opinion, Ribaud-Watanabe-Behrens teaches claim 46 for the reasons I discussed with respect to claim elements 1[b]/50[b]-1[d]/50[d]. Sections XI.A.2.c-e (1[b]/50[b]-1[d]/50[d]); EX1007, ¶85.

(w) 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.

289. In my opinion, Ribaud-Watanabe-Behrens teaches claim 58 for the reasons I discussed with respect to claims 7/42/57. *See* Section XI.B.3.f (7/42/57).

- (x) **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.**

290. In my opinion, Ribaud-Watanabe-Behrens teaches claim 60 for the reasons I discussed with respect to claims 31/61 and 9. *See* Sections XI.A.3.h (31/61) and XI.B.3.h (9).

- (y) **Claim 71: The computer program product of claim 51 wherein the second further action additionally includes causing the wireless device to display a current location on the wireless device, based at least in part upon a predetermined location associated with the second unique identifier, or based at least in part upon information derived from the second unique identifier.**

291. In my opinion, Ribaud-Watanabe-Behrens teaches claim 71 for the same reasons discussed with respect to claims 70. *See* Section XI.A.3.j (70).

C. Ground 3: Ribaud-Watanabe-Behrens-Nordman Renders Obvious Claims 27, 39, and 81

292. In my opinion, the combination of Ribaud, Watanabe, Behrens, and Nordman teaches claims 27, 39, and 81. Claims 27, 39, and 81 recite: “*The [method]/[mobile wireless device]/[computer program product] of claim [1]/[37]/[50] wherein the MAC address [or a respective beacon] is a randomly generated 48 bit number matching a format of a Bluetooth BD_ADDR.*”

293. 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.” EX1007, ¶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)*.” EX1021, 232 (describing Bluetooth addresses as a device specific identifier for Bluetooth form communications). Behrens confirms this understanding and explains that MAC addresses and Bluetooth devices are interchangeable as identifiers: “a UID may consist of or include a MAC (media access control) address, *Bluetooth Device Address (i.e. BD_ADDR)*, or other unique or quasi-unique identifier.” EX1008, 11:21-26, 25:22-25 (“a combination of different types of UIDs may be used” include “Bluetooth Device Addresses, WLAN MAC addresses and other types of UID[s]”). Behrens further teaches that “[i]n the case of Bluetooth, various address parts and lengths (e.g., *48-bit BD_ADDR*, 24-bit LAP, etc.), Friendly Names, as well as a combination thereof may be used.” EX1008, 19:12-14.

294. Nordman teaches the use of a “pseudonym address, which is a “randomized version” of a Bluetooth Device Address (BD_ADDR). EX1046, Abstract, ¶6. Nordman specifies “[t]he pseudonym address is used in all the functions of the Bluetooth device that normally use the BD_ADDR.” EX1046, Abstract, ¶6. A “user can select introducing various parameters into the random

number generator as initialization vectors to combine with the BD_ADDR ... to change the random number sequence and thus thwart an eavesdropper's discovery of that sequence.” EX1046, ¶8; *see also* ¶¶12, 57. Nordman further describes providing a “privacy options menu” to allow a user to select different ways of randomizing the BD_ADDR. *See* EX1046, ¶¶34-42. For example, if the option to randomize the entire device address is selected, the user’s Bluetooth device “randomizes the entire 48-bits of the user’s real BD_ADDR(0) to produce the pseudonym address.” EX1046, ¶40; *see also* ¶3.

295. In view of this teaching, Nordman’s pseudonym address teaches *a randomly generated 48 bit number matching a format of a Bluetooth BD_ADDR* and the Ribaud-Watanabe-Behrens-Nordman teaches the use of such an address as a MAC address for Bluetooth devices. Indeed, upon selection of a pseudonym address option, Nordman describes trigger configurations by which a user may choose to randomly generate their BD_ADDR. *See, e.g.*, EX1046, ¶¶34-49.

Further, Nordman’s process creates a randomly generated 48-bit number because the pseudonym address is a randomization of the “entire 48-bits of the user’s real BD_ADDR(0),” which amounts to a randomly generated number. EX1046, ¶¶40; *see also* ¶3.

296. A POSITA would have recognized the benefits provided by masking or randomizing addresses and would have been motivated to implement randomly

generated Bluetooth addresses as MAC addresses to advance Ribaudó's objective of enhancing privacy for Bluetooth device users. EX1007, ¶¶46, 78, 225-227 (describing "privacy" as an important user consideration); EX1046, Abstract, ¶¶4-5, 13, 96 (protecting user privacy using pseudonym addresses). For example, Nordman explains that using pseudonym addresses protects a user's privacy "by preventing the user's identity, routes, and activities from being correlated with his/her device's address." EX1046, Abstract, ¶¶5, 13, 95-96. This confers "anonymity upon the user." EX1046, ¶13; *see also* ¶¶8, 12, 52. And Ribaudó explains that "[s]ome users may desire substantial privacy" and "locations visited by a user are tracked (e.g., based on network identifiers or other information reported by a user), while in other embodiments, such locations are not tracked." EX1007, ¶225. Thus, a POSITA would have been motivated to combine Nordman with Ribaudó-Watanabe-Behrens to provide additional privacy protections for transmitted device identifiers like MAC addresses. *See also* Huang, L. et al., *Enhancing wireless location privacy using silent period*, IEEE WIRELESS COMMUNICATIONS AND NETWORKING CONFERENCE, (Vol. 2, pp. 1187-1192) (March 2005) (EX1042, "Huang") (describing randomly generated addresses that change periodically for improved privacy).

297. A POSITA would have had a reasonable expectation of successfully implementing Nordman's pseudonym addresses because Ribaudó, Watanabe, and

Behrens all describe Bluetooth communications and identifiers. EX1007, ¶¶18, 66-67, 73, 76-77, 154, 157, 181-184, 191; EX1006, ¶¶1-2, 27; EX1008, 4:21-24, 11:21-26, 18:21-28, 19:5-14, 25:22-25. Further, Behrens describes using a BD_ADDR interchangeably with a MAC address as implemented in Ribaud. EX1008, 11:21-26, 25:22-25. Therefore, implementing Nordman's pseudonym address in the combination would have been simple given that the pseudonym address functions as a BD_ADDR. Indeed, Nordman's disclosures operate on Bluetooth devices that may share substantial or identical architectural similarities. EX1046, ¶¶53-57. A POSITA would have therefore understood that applying Nordman's teachings would have yielded predictable results. Further, a POSITA would have understood that these references disclose interrelated teachings based on well-understood technologies that would have been amenable to various well-understood and predictable combinations.

XII. CONCLUSION

For the reasons above, it is my opinion that claims 1-83 of the '971 Patent are obvious based on each of the grounds specified in my Declaration.

In signing this declaration, I recognize that the declaration will be filed as evidence in an *inter partes* review before the Patent Trial and Appeal Board of the United States Patent and Trademark Office. I also recognize that I may be subject to cross-examination in the case and that cross-examination will take place within the United States. If cross-examination is required, I will appear for cross-examination within the United States during the time allotted.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true, and further 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.

Executed on this 24th day of August 2026, in New York City, New York.



Sundeep Rangan, Ph.D.