

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

GOOGLE LLC,
Petitioner,

v.

SECURE COMMUNICATION TECHNOLOGIES, LLC,
Patent Owner.

Case No. IPR2025-01181
Patent No. 11,334,918

**PETITION FOR *INTER PARTES* REVIEW
UNDER 35 U.S.C. §§ 311-319 AND 37 C.F.R. § 42.1 et seq**

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	STANDING CERTIFICATION.....	6
III.	UNPATENTABILITY GROUNDS.....	6
IV.	'918 PATENT.....	7
	A. Background.....	7
	B. Prosecution History	9
	C. POSITA	9
V.	CLAIM INTERPRETATION	10
	A. “determining...proximity”	10
VI.	GROUND 1: EAGLE IN VIEW OF BEHRENS AND OLKKONEN RENDERS OBVIOUS CLAIMS 1-4, 8-20, 22-25, 27-28, AND 31	11
	A. Eagle	11
	B. Behrens	13
	C. Olkkonen	13
	D. Eagle in view of Behrens, in further view of Olkkonen.....	15
	1. Receiving different identifying information from the same device.....	17
	2. Filtering beacon service identifiers	20
	3. Networking applications	25
	4. Blacklists and friend lists	27
	5. Re-alerting a previously alerted device.....	30
	E. Mapping to Challenged Claims	32
	1. Claim 1	33
	a. [1.PRE] “A mobile wireless device comprising:”	33
	b. [1.A] “a first radio; a second radio;”.....	34
	c. [1.B] “one or more processors; 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:”	35
d. [1.D] “receiving, using the first radio, identifier related information associated with a proximity beacon service, from one or more servers;”	36
e. [1.E.I] “receiving, using the second radio, a plurality of short range transmissions, including a plurality of proximity beacon transmissions when the device is located within a detection range of one or more beacon transmitter devices associated with the proximity beacon service, each of the proximity beacon transmissions including”	39
f. [1.E.II] “a respective MAC address,”	41
g. [1.E.III] “a respective unique identifier, and”	43
h. [1.E.IV] “a Proximity Beacon Service Identifier (PBSI);”	44
i. [1.F.I] “determining if a particular short range transmission of the plurality of short range transmissions a) includes a MAC address, and”	44
j. [1.F.II] “b) includes the proximity beacon service identifier (PBSI) and if c) the PBSI indicates the particular short range transmission is a proximity beacon transmission associated with the proximity beacon service;”	45
k. [1.G] “then: determining if an entity or object associated with the proximity beacon service is in proximity to the mobile wireless device, by utilizing the identifier related information and the unique identifier.”	46
2. Claim 2: “[Claim 1], wherein the MAC address is a randomly generated 48 bit number matching a format of a Bluetooth BD_ADDR.”	50
3. Claim 3	51
a. [3.PRE] “The mobile wireless device of claim 1 wherein the one or more processors further execute the instructions to perform operations including:”	51

b.	[3.A] “receiving, by the second radio, a first proximity beacon transmission including a first MAC address and a first unique identifier at a first time; and”	52
c.	[3.B.I] “receiving, by the second radio, a second proximity beacon transmission including a second MAC address and a second unique identifier at a second time,”	52
d.	[3.B.II] “the second MAC address being different from the first MAC address and”	54
e.	[3.B.III] “the second unique identifier being different from the first unique identifier; and”	55
f.	[3.C] “associating the first and second unique identifier with a single beacon transmitter device.”	55
4.	Claim 4: “[Claim 1], wherein the one or more processors further execute the instructions to perform operations including: further determining that at least one beacon transmitter device associated with the proximity beacon service is in proximity to the mobile wireless device, by utilizing an action function including one or more previously downloaded unique identifiers.”	56
5.	Claims 8/31	58
a.	[8.PRE]/[31.PRE] “[Claim 1][Claim 3] wherein the one or more processors further execute the instructions to...”	58
a.	[8.A]/[31.A] “receiving, via a second radio, the plurality of proximity beacon transmissions further includes receiving a first unique identifier at a first time that is different from a second unique identifier received at a second time; and”	58
b.	[8.B]/[31.B] “associating the first and second unique identifier with a single beacon transmitter device.”	58
6.	Claim 9	59
a.	[9.PRE] “A method for facilitating use of proximity beacons, the method executing within a mobile device, and the method comprising:”	59
b.	[9.A] “communicating... identifier related information...;”	59

c.	[9.B] “receiving... a plurality of proximity beacon transmissions...;”	59
d.	[9.C] “...a particular short range transmission... includes a MAC address,”	59
e.	[9.D] “...(PBSI) is present, and c) determining that... the particular short range transmission is... associated with the proximity beacon service; and”	60
f.	[9.E] “...then... determining that an entity or object... is within proximity...”	60
7.	Claim 10	60
a.	[10.PRE] “The method of claim 9,”	60
b.	[10.A] “wherein a first one of the plurality of proximity beacon transmissions received at a first time includes a first unique identifier, and wherein a second one of the plurality of proximity beacon transmissions received at a second time includes a second unique identifier the second unique identifier being different from the first unique identifier; and”	60
c.	[10.B] “associating both the first unique identifier and the second unique identifier with a particular entity or object in proximity to the mobile device.”	60
8.	Claim 11: “[Claim 9] wherein the MAC address is selected from a group consisting of (a) a randomly generated 48 bit number matching a format of a MAC address and (b) a Bluetooth BD_ADDR.”	61
9.	Claim 12	61
a.	[12.PRE] “The method of claim 9”	61
b.	[12.A] “wherein a first one of the plurality of proximity beacon transmissions is received at a first time and includes a first unique identifier and first MAC address, and the Proximity Beacon Service Identifier (PBSI); and”	61
c.	[12.B] “wherein a second one of the plurality of proximity beacon transmissions received at a second time includes a second unique identifier different from the first unique identifier and a second MAC address different from the	

first MAC address, and the Proximity Beacon Service Identifier; and”	61
a. [12.C] “associating both the first unique identifier and the second unique identifier with the same entity or object in proximity to the mobile device.”	62
10. Claims 13/15: “[Claim 9, further comprising][Claim 1, wherein the instructions further comprise:] preventing the sending of the unique identifier, using the first radio, to the one or more servers, based upon previous detections of the respective unique identifier associated with the proximity beacon transmission.”	62
11. Claims 14/19: “[Claim 1, wherein the instructions further comprise:][Claim 9, additionally comprising:] sending the unique identifier, using the first radio, to at least one server of the one or more servers, and receiving further information relating to an object or entity associated with being within proximity to the mobile device.”	63
12. Claims 16/24: “[Claim 1, wherein the instructions further comprise:][Claim 9, additionally comprising:] controlling further communications between the mobile device and at least one device or server associated with an entity or object in proximity to the mobile device.”	64
13. Claim 17: “[Claim 9], further comprising: receiving, using the first radio, access code information by the mobile device from at least one of the servers; and utilizing the access code information to gain access to the entity or object determined to be in proximity to the mobile device.”	66
14. Claims 18/28: “[Claim 9][Claim 1], wherein [the] receiving [of] the identifier related information, using the first radio, is performed in response to [executing instructions for] sending at least the unique identifier to at least one of the one or more servers using the first radio.”	67
15. Claim 20: “[Claim 19] wherein the further information relates to... advertising content.”	67
16. Claim 22: “[Claim 19] wherein the further information relates to a nearby user of an application on another device, in common with an application on the mobile device.”	68

17. Claim 23: “[Claim 22] wherein the application is a multiuser game.”	70
18. Claims 25/27: “[Claim 9, wherein the step of determining that an entity or object is within proximity further comprises:][Claim 1, wherein... the one or more processors further execute the instructions... for determining that an entity or object is within proximity by further:] comparing the identifier related information with the unique identifier or information derived from the unique identifier.”	70
VII. GROUND 2: EAGLE IN VIEW OF BEHRENS, OLKKONEN, AND PERTTILA RENDERS OBVIOUS CLAIM 17	71
VIII. GROUND 3: EAGLE IN VIEW OF BEHRENS, OLKKONEN, AND JONES RENDERS OBVIOUS CLAIM 29	73
IX. CONCLUSION.....	75
1. APPENDIX A: U.S. PATENT NO. 11,334,918 CLAIM LISTING	76

TABLE OF AUTHORITIES

CASES

KSR Int’l v. Teleflex,
550 U.S. 398 (2007)..... passim

Ohio Willow Wood Co. v. Alps South, LLC,
735 F.3d 1333 (Fed. Cir. 2013) 5

OTHER AUTHORITIES

MPEP §2111.05 73

EXHIBIT LIST

Exhibit	Description
1001	U.S. Patent No. 11,334,918
1002	Prosecution History of U.S. Patent No. 11,334,918
1003	Declaration of Mark Lanning
1004	Curriculum Vitae of Mark Lanning
1005	U.S. Patent Application No. 2005/0250552 (“Eagle”)
1006	U.S. Patent Application Publication No. 2010/0138481 (“Behrens”)
1007	U.S. Patent No. 7,590,086 (“Olkkonen”)
1008	Bluetooth Special Interest Group, Bluetooth Core Specification Version 2.1 + EDR (July 26, 2007)
1009	Bluetooth Special Interest Group, Assigned Numbers (December 14, 2002) (https://web.archive.org/web/20021214114356/http://www.bluetooth.org/assigned-numbers/baseband.htm)
1010	U.S. Patent Application Publication No. 2002/0131445
1011	U.S. Patent Application Publication No. 2002/0174364
1012	U.S. Patent Application Publication No. 2005/0164717
1013	U.S. Patent Application Publication No. 2006/0165100
1014	<i>Target Corporation v. Proxicom Wireless, LLC</i> , IPR2020-00903, Paper 2 (Petition for <i>Inter Partes</i> Review) (P.T.A.B May 8, 2020)
1015	<i>Target Corporation v. Proxicom Wireless, LLC</i> , IPR2020-00903, Paper 31 (Final Written Decision) (P.T.A.B Nov. 8, 2021)
1016	<i>Target Corporation v. Proxicom Wireless, LLC</i> , IPR2020-00904, Paper 2 (Petition for <i>Inter Partes</i> Review) (P.T.A.B May 8, 2020)
1017	<i>Target Corporation v. Proxicom Wireless, LLC</i> , IPR2020-00904, Paper 30 (Final Written Decision) (P.T.A.B Nov. 8, 2021)
1018	<i>Target Corporation v. Proxicom Wireless, LLC</i> , IPR2020-00931, Paper 2 (Petition for <i>Inter Partes</i> Review) (P.T.A.B May 15, 2020)
1019	<i>Target Corporation v. Proxicom Wireless, LLC</i> , IPR2020-00931, Paper 30 (Final Written Decision) (P.T.A.B Nov. 8, 2021)
1020	<i>Target Corporation v. Proxicom Wireless, LLC</i> , IPR2020-00932, Paper 2 (Petition for <i>Inter Partes</i> Review) (P.T.A.B May 15, 2020)
1021	<i>Target Corporation v. Proxicom Wireless, LLC</i> , IPR2020-00932, Paper 30 (Final Written Decision) (P.T.A.B Nov. 8, 2021)
1022	<i>Target Corporation v. Proxicom Wireless, LLC</i> , IPR2020-00933, Paper 2 (Petition for <i>Inter Partes</i> Review) (P.T.A.B May 15, 2020)

Exhibit	Description
1023	<i>Target Corporation v. Proxicom Wireless, LLC</i> , IPR2020-00933, Paper 30 (Final Written Decision) (P.T.A.B Nov. 8, 2021)
1024	<i>Target Corporation v. Proxicom Wireless, LLC</i> , IPR2020-00934, Paper 2 (Petition for <i>Inter Partes</i> Review) (P.T.A.B May 27, 2020)
1025	<i>Target Corporation v. Proxicom Wireless, LLC</i> , IPR2020-00934, Paper 31 (Final Written Decision) (P.T.A.B Nov. 30, 2021)
1026	<i>Target Corporation v. Proxicom Wireless, LLC</i> , IPR2020-00977, Paper 2 (Petition for <i>Inter Partes</i> Review) (P.T.A.B May 27, 2020)
1027	<i>Target Corporation v. Proxicom Wireless, LLC</i> , IPR2020-00977, Paper 31 (Final Written Decision) (P.T.A.B Nov. 30, 2021)
1028	<i>Target Corporation v. Proxicom Wireless, LLC</i> , IPR2020-00978, Paper 2 (Petition for <i>Inter Partes</i> Review) (P.T.A.B. June 1, 2020)
1029	<i>Target Corporation v. Proxicom Wireless, LLC</i> , IPR2020-00978, Paper 10 (Decision Denying Institution) (P.T.A.B. Dec. 4, 2020)
1030	<i>Target Corporation v. Proxicom Wireless, LLC</i> , IPR2020-00979, Paper 2 (Petition for <i>Inter Partes</i> Review) (P.T.A.B. June 1, 2020)
1031	<i>Target Corporation v. Proxicom Wireless, LLC</i> , IPR2020-00979, Paper 33 (Final Written Decision) (P.T.A.B Nov. 30, 2021)
1032	<i>Target Corporation v. Proxicom Wireless, LLC</i> , IPR2020-00980, Paper 2 (Petition for <i>Inter Partes</i> Review) (P.T.A.B June 1, 2020)
1033	<i>Target Corporation v. Proxicom Wireless, LLC</i> , IPR2020-00980, Paper 32 (Final Written Decision) (P.T.A.B Nov. 30, 2021)
1034	<i>Target Corporation v. Proxicom Wireless, LLC</i> , Nos. 2022-1282, 2022-1283, 2022-1338, 2022-1339, 2023 U.S. App. LEXIS 24861 (Fed. Cir. Sep. 20, 2023) (nonprecedential)
1035	Apple Inc., iPhone 3G Technical Specifications (https://web.archive.org/web/20080725084414/http://www.apple.com/iphone/specs.html)
1036	Apple Inc., iPhone User Guide for iPhone OS 3.1 Software (https://cdsassets.apple.com/live/6GJYWVAV/user/ma616_iphone_ios3_1_user_guide.pdf)
1037	U.S. Patent Application Publication No. 2004/0243519 (“Perttila”)
1038	U.S. Patent Application Publication No. 2007/0264991 (“Jones”)
1039	U.S. Patent No. 8,321,497 (“Steiner”)
1040	U.S. Patent Application Publication No. 2007/0219875 (“Toulotte”)

MANDATORY NOTICES

A. Real Party-In-Interest

Petitioner Google LLC¹ is a real party-in-interest to this proceeding under 37 C.F.R. §42.8(b)(1).

B. Related Matters

A decision in this proceeding could affect or be affected by the following.

1. United States Patent & Trademark Office

U.S. Patent No. 11,334,918 issued from application no. 15/271,410, filed 2016-09-21, and claims priority to the following applications:

Application No.	Filing Date
14/861,563	2015-09-22
14/472,477	2014-08-29
13/775,435	2013-02-25
13/212,723	2011-08-18
12/364,828	2009-02-03
61/095,359	2008-09-09
61/095,001	2008-09-08

The following patent applications claim priority to U.S. Patent No. 11,334,918 and application no. 15/271,410:

¹ Google LLC is a subsidiary of XXVI Holdings Inc., which is a subsidiary of Alphabet Inc. XXVI Holdings Inc. and Alphabet Inc. are not real parties-in-interest to this proceeding.

Application No.	Filing Date
19/027,075 (pending)	2025-01-17
19/027,020 (pending)	2025-01-17
18/437,306 (pending)	2024-02-09
18/204,528	2023-06-01
17/942,197	2022-09-12
17/366,826	2021-07-02
16/817,896	2020-03-13

U.S. Patent No. 11,334,918 is the subject of *Samsung Electronics Co., Ltd. v. Secure Communication Technologies, LLC*, IPR2025-01049, filed 2025-05-30.

Petitioner is concurrently filing petitions for *inter partes* review of U.S. Patent Nos. 11,443,344 (application 17/366,826) and 11,687,971 (application 17/942,197) and recommends assigning each case to the same panel.

2. United States District Court

a. Eastern District of Texas

Secure Communication Technologies, LLC. v. Samsung Electronics Co., Ltd., No. 2:24-cv-00484 (E.D. Tex.), filed 2024-07-03.

C. Counsel and Service Information - §§42.8(b)(3) and (4)

Lead Counsel	Scott A. McKeown, Reg. No. 42,866
Backup Counsel	Libbie A. DiMarco (<i>pro hac vice</i> forthcoming) Victor Cheung, Reg. No. 66,229
Service Information	<u>E-mail:</u> SMcKeown-PTAB@wolfgreenfield.com Elizabeth.DiMarco@WolfGreenfield.com VCheung-PTAB@wolfgreenfield.com <u>Post and hand delivery:</u> WOLF, GREENFIELD & SACKS, P.C. 600 Atlantic Avenue Boston, MA 02210-2206 <u>Telephone:</u> 617-646-8000 <u>Facsimile:</u> 617-646-8646

A power of attorney is submitted with the Petition. Counsel for Petitioner consents to service of all documents via electronic mail.

Petitioner requests *inter partes* review (IPR) and cancellation of claims 1-4, 8-20, 22-25, 27-29, and 31 (“Challenged Claims”) of U.S. Patent No. 11,334,918 (EX1001, the “’918”).

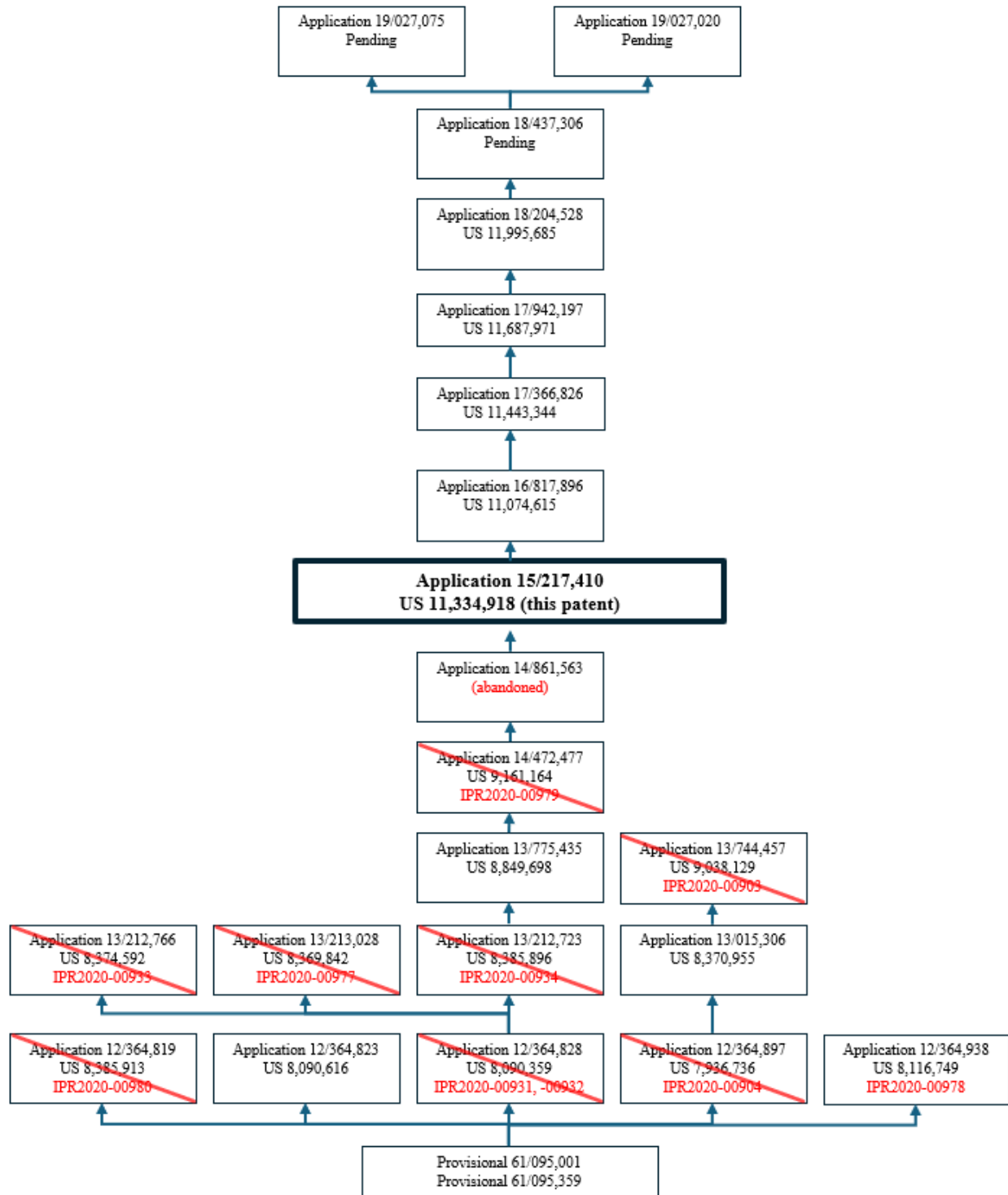
I. INTRODUCTION

The ’918 is directed to a mobile communication architecture for “facilitating the exchange of information” between two wireless devices, each device employing short-range communication (*e.g.*, Bluetooth) and long-range communication (*e.g.*, cellular) wireless capabilities. EX1001, 2:66-5:12. A first device may detect an identifier transmitted from a second device in short-range proximity and sends information identifying the second device to a server via long-range communications. EX1001, 3:4-28, 7:44-53, 8:9-25. Based on policy information stored at the server, the server may alert the first device to the second device’s presence with, *e.g.*, the second device’s contact information. EX1001, 3:29-35, 8:26-33, 8:60-9:27.

This architecture of exchanging information between nearby devices and servers was claimed in earlier patents within the ’918’s family (all claiming priority to the same provisional applications) and previously cancelled by the PTAB as known in the art. As shown in the diagram below, a majority of the family’s earlier patents were challenged before the PTAB, and claims directed to

the device-server architecture were found unpatentable in all but one proceeding.² *See* EX1014-EX1033 (IPR Petitions and Decisions). Unpatentability was further confirmed in the only two IPR proceedings appealed to the CAFC (IPR2020-00931, IPR2020-00933). *See* EX1034.

² IPR2020-00978 was denied institution for reasons/limitations not relevant to the '918 claims. EX1029, 15-18.



The '918 claims were prosecuted while the above-described IPRs were pending, but the claims issued before final judgment (with appeals exhausted), to

include three overall concepts: (1) the short-range and long-range communications architecture described above and found to be squarely in the prior art; (2) changing device identifiers over time, also found to be in the prior art; and (3) filtering based on short-range service identifiers. The PTAB already determined that the first two features, in combination, were well-known—in Eagle (EX1005) and Behrens (EX1006).³ Likewise, the PTAB has previously found that criteria-based filtering of short-range communicated identifiers was also known.⁴ Patent Owner is estopped from challenging here the PTAB’s findings regarding the same prior art teachings. *Ohio Willow Wood Co. v. Alps South, LLC*, 735 F.3d 1333, 1342 (Fed.

³ See EX1015, 7-8 and 15-34 (PTAB determining that Eagle anticipated claims including a server receiving a unique identifier from a wireless device over a “wide area link,” where that wireless device received the unique identifier over a “local wireless link,” and transmitting information back to the wireless device based on a policy); EX1031, 46-49 (PTAB acknowledging Behrens’ “combination of UIDs” and users exercising control over transmitted UIDs).

⁴ See EX1015, 17, 24 (PTAB finding that Eagle discloses determining which unique identifiers to send to the server); EX1033, 18-23 (PTAB determining that prior art systems disclosed suppressing/filtering communications to servers where unique identifiers were previously encountered).

Cir. 2013) (“Collateral estoppel protects a party from having to litigate issues that have been fully and fairly tried in a previous action and adversely resolved against a party-opponent.”).

As Patent Owner’s claims were being cancelled in previous IPRs, continuation patents were pursued to switch its filtering criteria to a new but existing parameter (service identifier) of Bluetooth/WiFi communications. The addition of filtering for known Bluetooth service identifiers to the claims cannot confer patentability because the reception of service identifiers and their use in filtering search results was known in the prior art, as Olkkonen (EX1007) illustrates.

Ground 1 explains how Eagle in view of Behrens renders obvious the same short-range/long-range architecture and changing identifiers previously presented to the PTAB—and Olkkonen renders obvious the “new” but trivial feature of using a service identifier for filtering.

Ground 2 explains how Perttila (EX1037) further renders obvious the use of access codes in an interaction between wireless devices.

Ground 3 explains how Jones (EX1038) further renders obvious the advertisement of Bluetooth services.

Accordingly, Petitioner requests that the Board institute IPR and cancel the Challenged Claims.

II. STANDING CERTIFICATION

Petitioner certifies that the '918 is available for IPR and that Petitioner is neither barred nor estopped from requesting IPR of the Challenged Claims. 37 C.F.R. §42.104(a).

III. UNPATENTABILITY GROUNDS

The Challenged Claims are unpatentable as follows:

Ground	References	Claims	Pre-AIA Basis
1	Eagle, Behrens, Olkkonen	1-4, 8-20, 22-25, 27-28, 31	§103
2	Eagle, Behrens, Olkkonen, Perttila	17	
3	Eagle, Behrens, Olkkonen, Jones	29	

The '918's earliest possible effective filing date is 2008-09-08. EX1001, code (60). Each relied-upon reference is pre-AIA §102(b) and/or (e) prior art even under the earliest 2008 filing date.

Name	Filing Date	Issue/Publication Date
Eagle (EX1005)	2005-05-05	2005-11-10
Behrens (EX1006)	2008-04-30 (PCT)	2010-06-03
Olkkonen (EX1007)	2004-11-03	2009-09-15
Perttila (EX1037)	2003-06-02	2004-12-02
Jones (EX1038)	2006-05-15	2007-11-15

The Declaration of Mark Lanning (EX1003, ¶¶1-297; “Lanning”) describes the prior art’s scope and content at the time of the ’918.

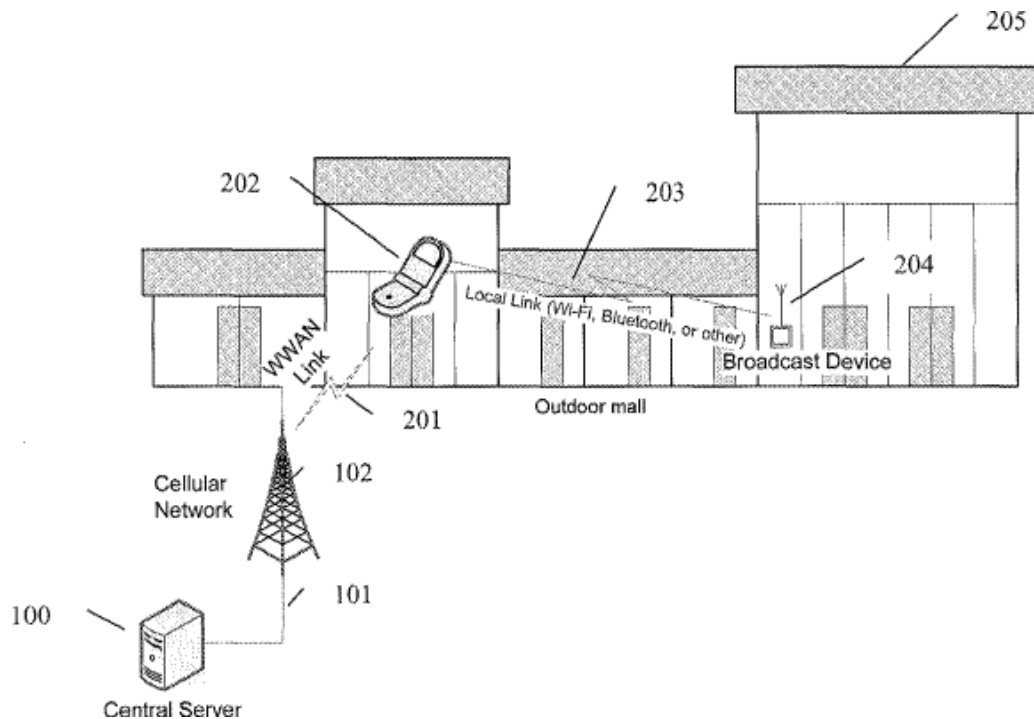
IV. ’918 PATENT⁵

A. Background

The ’918 is directed to the exchange of information between two wireless devices using short-range communications (*e.g.*, Bluetooth/WiFi), with the aid of a remote server using long-range communications (*e.g.*, cellular). EX1001, 2:66-5:12.

Fig. 2 (below) shows one implementation with devices 202 and 204 in short-range communication, and device 202 and server 100 in long-range communication. EX1001, 7:44-53.

⁵ Unless otherwise noted, all emphasis in the Petition (including figure annotations) is added.



Device 204 is associated with a museum exhibit that “transmits identifying information [to device 202] using short range wireless link 203,” which device 202 “passes... to the central server 100,” and server 100 recognizes the identifying information as associated with device 204. EX1001, 7:49-65. Based on account settings and policies, the server determines “what information and under which situations information may be disclosed to another device or user” to facilitate further short-range communications. EX1001, 4:49-67, 9:12-21, 16:5-16.

The '918 claims that devices in short-range proximity identify themselves with beacon transmissions including a MAC address, unique identifier, and beacon service identifier. EX1001, claim 1. Examples of service identifiers in an ad hoc Wi-Fi network include basic service set identifiers (BSSIDs, such as a 48-bit

address) and service set identities (SSIDs, which are network names). EX1001, 10:31-11:6; *see also* Olkkonen, 12:24-30, 18:60-39:39, 27:52-56, 32:20-25, 33:44-60 (describing functionality of known short-range BSSIDs, SSIDs, access codes, and service attributes). Lanning, ¶¶40-69.

B. Prosecution History

Prosecution of the '918 included rounds of office actions/amendments and appeals based on §§101, 112, 102, and 103. *See generally* EX1002.

In a Notice of Allowance, the Examiner stated that the prior art of record “does not disclose each of the proximity beacon transmissions including a MAC address and a unique identifier, determining if a particular short range transmission of the plurality of short range transmissions includes a MAC address, and utilizing the unique identifier.” EX1002, 2187-2190. Lanning, ¶¶70-71.

C. POSITA

On 2008-09-08, a person having ordinary skill in the art (“POSITA”) would have had a Bachelor’s degree in electrical or computer engineering, or a related field, with approximately 3-5 years of experience in wireless communications.⁶ A higher level of education may substitute for less experience. Lanning, ¶¶73-75.

⁶ This same level was adopted in prior proceedings in the '918 family and is now fixed by estoppel. *See* EX1019, 8-9.

V. CLAIM INTERPRETATION

Claim terms are construed herein using the standard used in civil actions under 35 U.S.C. §282(b), in accordance with the ordinary and customary meaning as understood by a POSITA and the patent's prosecution history. 37 C.F.R. §42.100(b).

A. “determining...proximity”

Claims [1.G] and [9.E] of the '918 recite: “determining [if/that] an entity or object... is [in/within] proximity to the mobile wireless device, by utilizing the identifier related information.”

During prosecution, Applicant provided examples of alleged support for these limitations to argue that they did not contain new matter. EX1002, 521-540. Thus, the limitations may encompass particular features in addition to their plain and ordinary meaning.

For example, *determining proximity* may be satisfied by disclosing a device's presence to another device. *See* EX1002, 524 (“Device 1... notifies the user that the entity... is in proximity”), 539 (“process... allows for disclosure of a user's presence (that is, their ‘proximity’”). That is, if one device's presence is not disclosed (or not permitted to be disclosed) to another device, those devices are determined not to be in “proximity.”

Furthermore, *utilizing identifier related information* may be satisfied by using identifier information as a filter to determine which identifiers to pass to a server to determine whether there is permission to disclose a device's presence to another. *See* EX1002, 524 (“if identifiers are found... employ an action... as a filter that determines which... identifiers should be passed to the server,” “permission... may require being on a friends list”).

Lanning, ¶¶77-80.

VI. GROUND 1: EAGLE IN VIEW OF BEHRENS AND OLKKONEN RENDERS OBVIOUS CLAIMS 1-4, 8-20, 22-25, 27-28, AND 31

A. Eagle

Eagle is directed to a mobile communication architecture or “social software introduction system” for “facilitating direct communications between consenting persons having similar interests.” Eagle, [0002], [0065].

The system includes cellular phones enabled with Bluetooth that identify other nearby devices by a unique identification value such as a Bluetooth address. Eagle, [0003], [0018]. When one device (hereinafter a “Requester Device”) detects a device (hereinafter an “Identified Device”) using the Identified Device's unique identification value, the Requester Device notifies a remote server of the unique identification value via a long-range cellular network. Eagle, [0003], [0020]. An example of devices 203 and 205, and a server 220, are shown in Fig. 2 (below).

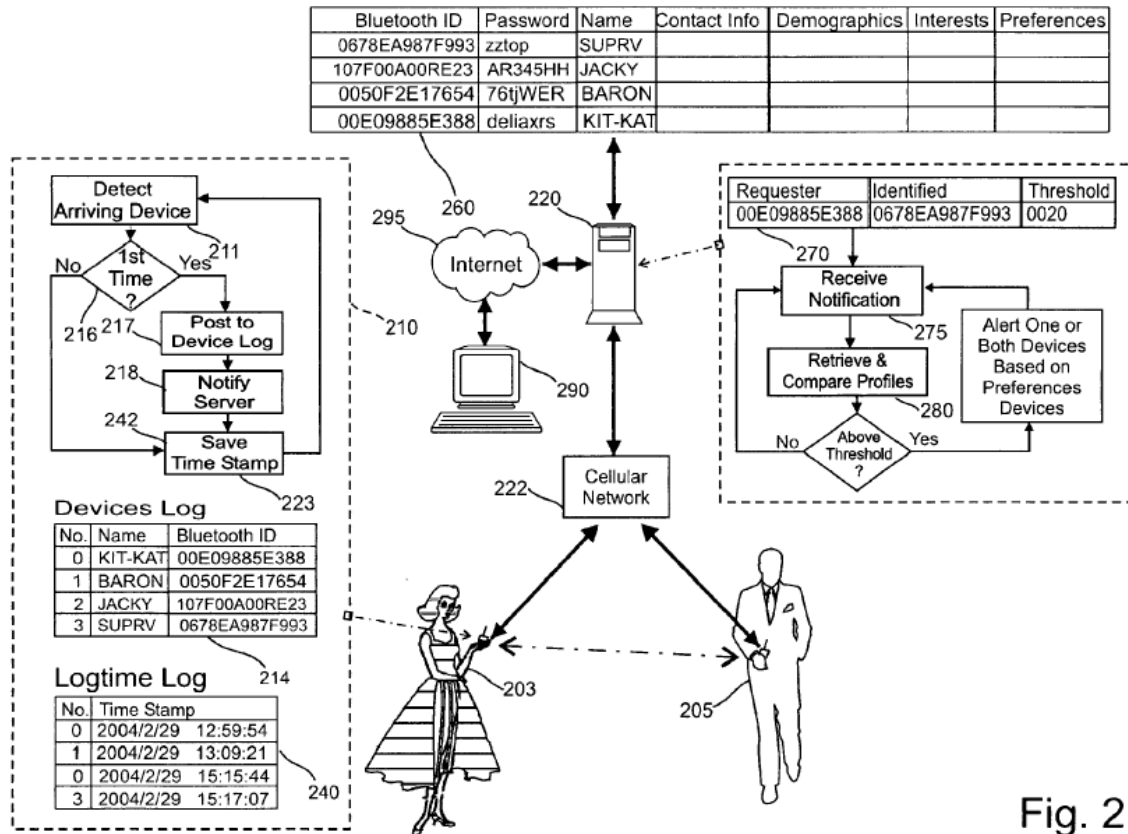


Fig. 2

The server stores profile data describing devices and their owners and “fetches the profile data associated with each of the two identified devices and performs a comparison.” Eagle, [0005], [0020]. If the profiles of a Requester Device and an Identified device match (*e.g.*, their profiles indicate they attended the same college), then an alert message is sent to each device. Eagle, [0005]-[0007], [0045], [0047], [0063]. An alert may contain contact information, descriptions of the device’s owner’s personal interests, “or any other information which is of use in a specific application [that] may be of use to identify, or promote communications between, nearby devices and their owners.” Eagle, [0007], [0021]. Lanning, ¶¶87-90.

B. Behrens

Behrens is directed to a system for automatically establishing contact between users who are in close proximity to each other. Behrens, Abstract, [0001].

In one example, a wireless device detects the presence of another wireless device by receiving unique identifiers (UIDs) over Bluetooth. Behrens, [0094], [0097]-[0098]. UIDs “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,” and may include MAC addresses and Bluetooth Device Addresses. Behrens, [0097].

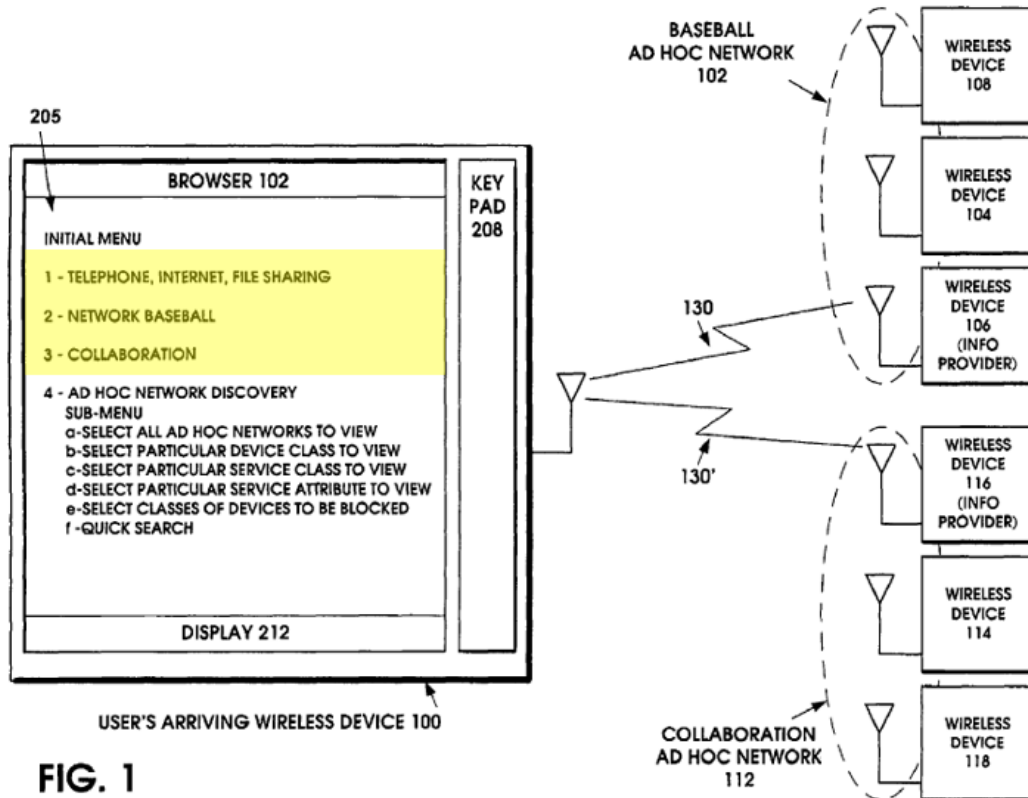
UIDs may be used in combination, and a “user may... exercise control over which or how many UIDs are transmitted by his device.” Behrens, [0061], [0103], [0115], [0122]. Accordingly, a user has “multiple or changing UIDs.” Behrens, [0061], [0115]. Lanning, ¶¶91-94.

C. Olkkonen

Olkkonen is directed to short-range wireless systems and connecting users for common purposes via ad hoc networking (*e.g.* “piconet” in Bluetooth). Olkkonen, 1:13-16, 1:46-2:3. Piconets are used for “collaborative work projects, collaborative games, multi-user gateways to the Internet, and the like.” that interested users may join. Olkkonen, 2:60-65. Olkkonen’s system thereby alerts

users of nearby piconets (or other ad hoc networks) that are of interest. Olkkonen, 4:65-5:4.

Olkkonen teaches that a wireless device may search for nearby piconets through inquiry and discovery processes. Olkkonen, 12:39-60, 13:33-50, 18:49-63; *see also* piconet examples illustrated throughout, 13:29-31:25. Devices in ad-hoc networks that receive inquiry messages “respond[] with information... characterizing the ad hoc network.” Olkkonen, 5:27-33. Responses are compiled into a discovery menu listing those characteristics “in accordance with the type of characteristics of interest to the user.” Olkkonen, 6:29-38. An exemplary menu 205 is shown in Fig. 1 (below; exemplary available network services highlighted).



Users have the ability to filter certain devices in the menu, for example by blocking and/or displaying devices with certain device classes, service classes, or service attributes. Olkkonen, 11:33-60, 22:8-21. Lanning, ¶¶95-98.

D. Eagle in view of Behrens, in further view of Olkkonen

The '918 is in the field of wireless communications, including claiming to improve secure communications using wireless service identifiers, safety and privacy with locally stored policies, and facilitating the exchange of information between two entities associated with two wireless devices. *See* EX1001, 2:48-57, 2:66-3:3. Lanning, ¶99.

Eagle, Behrens, and Olkkonen are each analogous to the '918, as they are in the same field of wireless communications and/or reasonably pertinent to the objectives identified above.⁷ Eagle, Abstract (Bluetooth phones identify nearby devices and use a server that facilitates communications), [0008] (avoiding privacy problems); Behrens, [0001], [00136] (establishing contact between otherwise

⁷ Eagle and Behrens were previously asserted in related patent family IPRs that reached final judgement. Arguments that Eagle or Behrens are not analogous art are estopped. *See* EX1015, 33 (IPR2020-00903 FWD, finding Eagle analogous); EX1030, 70 (IPR2020-00979 Petition, arguing that Behrens is analogous); EX1031, 46-50 (IPR2020-00979 FWD, finding claims unpatentable).

unknown users in proximity), [0141] (applications in social networking, Internet forums); Olkkonen, 1:13-16 (short-range wireless systems), 4:65-5:4 (providing discovery of collaborative activities in nearby networks that would interest users). Lanning, ¶100.

The Challenged Claims are directed to the same well-known prior art systems cancelled in earlier IPRs against the parent patents, in which wireless devices communicating using short-range Bluetooth may leverage a remote policy server using a long-range wireless protocol for facilitating a secure short-range Bluetooth connection among those devices. *See* §I above.

To the extent Eagle is argued by Patent Owner as failing to expressly disclose details of: particular information in short-range messages used to establish connections, identifying beacon service identifiers, or the reception or use of certain information at a wireless device, such obvious variations would have been obvious to a POSITA in view of Behrens and Olkkonen. Lanning, ¶101.

For example, a POSITA seeking to address privacy risks in Eagle would have found it obvious to provide for changing unique identifiers from time to time, per Behrens. To make Eagle's system more efficient, a POSITA would have found it obvious to have participating devices broadcast a specific service identifier, per Olkkonen, to identify Eagle's social introduction application. A user's device would thus first filter unique identifiers for the correct service and then send the

unique identifiers to Eagle’s remote server, which maps unique identifiers to user profile information to facilitate connections between wireless devices, and then take potential further action, such as displaying contact information or joining a collaborative game, as taught by Olkkonen. And, as an overall security measure, the user’s device would have been configured to ignore blacklisted unique identifiers, as taught by Behrens. Lanning, ¶102.

Motivation to modify Eagle’s system in view of Behrens’ and/or Olkkonen’s teachings is discussed below, followed by a mapping of their combined teachings (“Eagle-Behrens,” “Eagle-Olkkonen,” or “Eagle-Behrens-Olkkonen” as applicable) to the Challenged Claims.

1. Receiving different identifying information from the same device

The claims of the ’918 require receiving, at a wireless device from a *single transmitter device*, different beacon transmissions at two different times, including a *first* transmission with a MAC address and unique identifier, and a *second* transmission with a different MAC address and different unique identifier. *See, e.g.,* EX1001, claims 1, 3, 8-10, 31. In other words, the claimed system changes its identifying data as a function of time to enhance security. EX1001, 4:42-48, 10:18-30, 17:33-59. Lanning, ¶103.

Eagle describes that Identified Devices identify themselves to Requester Devices with a “unique identification value, such as a Bluetooth device address

value.” Eagle, [0003]. To the extent it is argued that Eagle does not explicitly describe receiving different first and second MAC addresses and different unique identifiers from the same device, it would have been obvious to a POSITA for the following reasons. Lanning, ¶104.

Behrens teaches that devices in short-range proximity “uniquely identif[y]” themselves and their owners with a “combination” of unique identifiers (UIDs) including WLAN MAC addresses, Bluetooth Device addresses, unique numbers, and/or unique symbols. Behrens, [0061], [0097], [0111], [0115], [0122]. Moreover, a user can have “multiple or changing UID[s]” and has “control over which or how many UID[s] are transmitted by his device.” Behrens, [0103], [0115]. Lanning, ¶¶105-106. Behrens explains that the use of changing UID[s] comprised of combinations of different information advantageously allows a user to have a single managed account with different online identities (*e.g.* for different social events or parties), adding an additional method for users to create distinct or particular profile data in Eagle’s system. Behrens, [0115]; Eagle, [0063] (teaching mode indicators to select different profile data in different situations). That is, the identity of a user can be changed, protected, or masked by changing the identification information that uniquely identifies the user. Lanning, ¶¶107-110.

Additionally, a POSITA would have recognized that Behrens’ teaching of changing UID[s] would have prevented others from tracking devices based on static

identifiers, resolving known privacy and security concerns for short-range wireless communications. EX1010, [0002]-[0004]; EX1011, Abstract, [0006]; EX1012, [0002]-[0008]; and EX1013, [0008]-[0011] (addressing security, privacy, and tracking with temporary and/or random identification numbers and addresses). *See also* Behrens, [0003] (apprehension in sharing of personal information freely). Thus, where Bluetooth addresses and UUIDs are potentially transmitted “continuously or repeatedly” (Behrens, [0097]; Eagle, [0003]), the changing of identifiers advantageously prevents the tracking and correlating of users, activities, and devices over time. Lanning, ¶111.

The described modification would have been further obvious to a POSITA as it is no more than the application of a known technique (Behren’s teaching of changing combination UUIDs) to a known device ready for improvement (Eagle’s system that identifies devices by unique identification values and identifies profile data by mode indicator values) to yield predictable results (allowing for different online identities; enhancing privacy with changing UUIDs). *KSR Int’l v. Teleflex*, 550 U.S. 398, 417-418 (2007). Lanning, ¶112.

A POSITA would have also had a reasonable expectation of success in modifying Eagle with the teachings of Behrens. Use of UUIDs (which are data values used as identifiers) in place of Eagle’s unique identification values would have required no more than ordinary software coding skills to change such values,

and track, select, store, communicate, and analyze those values as known in the art. Moreover, where Behrens teaches that UIDs borrow from existing values such as a wireless device's addresses, Behrens provides techniques for obtaining those values and synchronizing UIDs with the server. Behrens, [0077]; *see also* Behrens, [0065], [0076] (user supplies UIDs to the server to link to user accounts). Modification would have been well within the skill of a POSITA. Lanning, ¶113.

2. Filtering beacon service identifiers

The claims of the '918 require determining that a *proximity beacon service identifier (PBSI)* received in a short-range transmission *indicates the particular short range transmission is associated with a proximity beacon service* (the proximity beacon service being related to one or more servers). *See, e.g.*, EX1001, claims 1 and 9. The same claims require that the above determination (that the PBSI indicates the proximity beacon service) must be made before determining if an Identified Device is within proximity of the Requester Device. That is, the PBSI is used to filter received beacon transmissions prior to further processing. As noted above, filtering of short-range parameters was shown to be well known in the art via previous IPRs. *See* §I.

To the extent Patent Owner argues that Eagle does not explicitly describe *beacon service identifiers* (or *PBSIs*) as claimed, it would have been obvious to a POSITA to filter UIDs based on beacon service identifiers (*e.g.*, service class

information) received in inquiry responses, consistent with the teachings of Olkkonen, for the following reasons. Lanning, ¶114-115.

Eagle teaches that it is unnecessary for a Requester Device to notify the server of every UID that it receives from nearby Identified Devices. For example, when an Identified Device is detected, the Requester Device “determine[s] whether the detection of a given device warrants the transmission of a notification message to the server” by filtering out recently detected devices. Eagle, [0023]-[0025]. Thus, Eagle teaches selectively notifying the server of nearby devices such that the user is not alerted of every device that is nearby, and communications with the server and mobile device communication processing are minimized. Lanning, ¶116.

Olkkonen teaches additional filtering techniques known to POSITAs in the context of Bluetooth ad hoc networks. For example, service class information (which may include service “attributes”) describes and identifies programs running in ad hoc networks (*e.g.*, a network baseball game). Olkkonen, Fig. 5 (showing a service class with a program identity service attribute), 30:22-28. This service identification information is received in Bluetooth inquiry responses. *See* Olkkonen, 5:27-33, 12:40-48, 13:33-43, and 17:49-63 (Identified Devices’ inquiry responses include service registry information “characterizing the ad hoc network”); 5:13-17 and 17:17-22 (service classes “characterize the ad hoc

network” and include, *e.g.*, the type of distributed program running). Lanning, ¶117.

Service class information (filtering for Eagle’s “BlueAware” application): It would have been obvious to use Olkkonen’s service class information to identify Eagle’s social introduction application (which is a service and a program running on wireless devices) such that Identified Devices identifying Eagle’s service are included in notifications to the server rather than non-participating devices. Lanning, ¶118.

For example, Olkkonen teaches that lists of discovered Identified Devices presented to the user in a discovery menu should be customized to user preferences, *e.g.*, by ignoring or blocking undesirable Identified Devices and by listing Identified Devices of interest. Olkkonen, 11:30-60. One such filter blocks all devices identifying themselves as providing an advertisement broadcast service. Olkkonen, 11:33-42, 22:34-43.⁸ In another example, a user may only want to see

⁸ Olkkonen describes “advertisement” and “advertisement broadcaster” classes of devices, but a POSITA would have recognized these as non-standard Bluetooth classes. If not described in standard class of device information, a POSITA would have alternatively identified “advertisement” as custom service information. Lanning, ¶119.

devices in particular service classes or having particular service attributes (such as those identifying a particular program, such as a “GAME PROGRAM”).

Olkkonen, 11:43-60. Lanning, ¶119.

As Eagle requires users to actively participate in its social introduction system by running a particular program (“BlueAware”) on their devices (Eagle, [0019], [0029], [0038], [0065]) and by registering information with a server (Eagle, [0029], [0045]-[0046]), POSITAs would have recognized that it would have been wasteful and inefficient to notify the remote server of *every* Bluetooth device that the Requester Device encounters without screening/filtering them first as participating in the service. In this regard, Eagle emphasizes that its system links users with “selection criteria that [are] useful to service users.” Eagle, [0011]. A notification identifying a device that is not even participating in Eagle’s social introduction system would have been useless to the remote server and would have increased communications and server load for no benefit. Therefore, it would have been obvious to modify Eagle’s Identified Devices to specifically identify Eagle’s social introduction application within inquiry response service class information (when the particular Identified Device participates in Eagle’s services) and to modify Eagle’s Requester Device to filter inquiry responses so that only UIDs identifying themselves as being relevant to Eagle’s social introduction system would be notified to the server. As a result, only UIDs from Identified Devices that

“warrant the transmission of a notification message to the server” (Eagle, [0024]) are actually notified to the server. Lanning, ¶120.

Additionally: Eagle teaches that wireless device resources are limited. Eagle, [0024] (conserving memory by deleting old logs of Identified Devices), [0026] (continuous scanning and logging expends phone battery life). By only contacting the server with useful UIDs, these resources are further conserved. Irrelevant Identified Devices do not need to be logged or tracked and do not need to be passed to the server using long-range wireless communications. Lanning, ¶121.

The described modifications would have been further obvious to a POSITA as no more than the application of a known technique (Olkkonen’s teachings of including service information in inquiry responses and filtering responses based on that information) to a known device ready for improvement (Eagle’s system that determines whether detection of an Identified Device warrants notification to the server) to yield predictable results (selectively notifying the server of Identified Devices). *KSR*, 550 at 417-418. Lanning, ¶122.

A POSITA would have also had a reasonable expectation of success in modifying Eagle to implement Olkkonen’s teachings to receive and analyze service information in inquiry responses. For example, a POSITA would have recognized that Bluetooth communications include several methods for conveying service information through various fields, including but not limited to those

within class-of-device information and extended inquiry responses (EIRs) that include fields for service class universally unique identifiers (UUIDs) and manufacturer specific data. Eagle, [0032]; EX1008, 1305-1310. Service information may be included in these fields or as appended to any inquiry response so that the necessary descriptive information is conveyed, as discussed above. Filtering based on those values would have required no more than ordinary data processing skills to receive and analyze those values well within the skill of a POSITA. Lanning, ¶123.

3. Networking applications

Claims 22-23 of the '918 require receiving information about another user that is a *nearby user of an application* such as a *multiuser game*. Lanning, ¶124.

Eagle broadly describes that its social introduction system “enables a diverse suite of applications” (*e.g.*, connecting people for work, connecting users with like interests, as tradeshow greeting beacons). Eagle, [0061]-[0068]. Alerts returned to the Requester Device therefore include “any... information which is of use in a specific application” and useful to “promote communication between[] nearby devices and their owners,” including contact information. Eagle, [0007], [0041], [0050]. Lanning, ¶125.

Olkkonen, like Eagle, teaches that users of wireless devices may connect for a variety of applications. For example, Olkkonen describes that wireless Bluetooth

devices form ad hoc networks or piconets for telephone, internet, and file sharing services, and for participating in network games. Olkkonen, 2:59-65, 6:19-21, 11:61-12:2, 18:60-63, 19:13-16, 20:41-43, 25:48-52, 25:63-26:33. Lanning, ¶126.

Accordingly, to the extent Eagle does not expressly describe that a user of an Identified Device is using an application such as a multiuser game, it would have been obvious that users in collaborative settings would have been participating in a variety of activities, including multiuser games, as taught by Olkkonen. The description of a user as being a user of a multiuser game would have been no more than a simple substitution of known elements (*e.g.*, Olkkonen's teaching that users participate in games) for another (*e.g.*, Eagle's discussions that users collaborate for a variety of social activities) to obtain predictable results (*e.g.*, facilitating the introduction to, and connection with, a user playing a multiuser game). *KSR*, 550 at 417-418. Lanning, ¶127.

Furthermore, modification of Eagle to encompass users playing multiuser games, as claimed in the '918 requires no more than ordinary skill. As Eagle and Olkkonen both explain, many uses for social introductions and collaboration existed. The fact that one user may have a particular type of application program on their device—a multiuser game—was in no way new. Inclusion of such a user in Eagle's social introduction system would have required no more than ordinary skill in the art. Lanning, ¶128.

4. Blacklists and friend lists

With respect to claim limitations of the '918 that require receiving information and using that information to determine whether another device is in proximity to a user device (*e.g.*, as in claims 1, 9), Eagle-Behrens renders obvious those limitations through the use of blacklists (*i.e.*, lists of UIDs to ignore) and friend lists (*i.e.*, lists of trusted UIDs). *See* [1.G] below. Lanning, ¶129.

In particular, Eagle teaches that the Requester Device determines whether the detection of an Identified Device “warrants” the notification of the Identified Device’s UIDs to the server. Eagle, [0020], [0024], [0040], [0051]. As discussed above (§VI.D.2), selectively notifying the server of nearby devices minimizes communications with the server and minimizes the mobile device’s communications processing. Lanning, ¶130.

In furtherance of this goal, Behrens teaches that a server may instruct a Requester Device to ignore devices having certain UIDs. Thus, the Requester Device “may store [unique identifiers (UIDs)] to be ignored in a blacklist,” received as instructions from the server, to eliminate spam and other unwanted behavior. Behrens, [0101]-[0102], [0124]. Lanning, ¶131.

Similarly, Eagle teaches that friend lists create a trust network of devices that should likely be identified to the Requester Device. For example, the server stores profile information “specifying a set of device IDs for devices owned by

‘friends’” that form a “trust network” of devices. Eagle, [0056], [0066]-[0067].

Based on the friend list, the Requester Device is “only” alerted to the presence of nearby Identified Devices that are in the Requester Device’s friend list—*i.e.*, part of its trust network—and have “common interests” in their profiles. Eagle, [0056]. Lanning, ¶132.

While Eagle describes the friend list on the server in an exemplary embodiment, it would have been obvious to a POSITA to alternatively store the friend list on the Requester Device to act as a filter for UIDs sent to the server. As discussed above (§VI.D.2), selectively notifying the server of nearby devices through filtering minimizes communications with the server and minimizes the mobile device’s communications processing. Therefore, by performing a basic check of received UIDs against a friends list prior to notification to the server, irrelevant UIDs may be ignored outright, conserving server and device resources. As Behrens teaches, lists for filtering, such as Behrens’ blacklist and Eagle’s friend list, may be stored on the wireless device, on the server, or both. Behrens, [0101]-[0102]. Indeed, an obvious and finite number of identifiable locations to store and use filtering lists would have been known to a POSITA with predictable results (*i.e.*, storing and filtering locally at the wireless device, storing and filtering remotely at a server). *KSR*, 550 at 402-403. Lanning, ¶¶133-134.

Moreover, where UIDs change over time (*see* §VI.D.1), Behrens provides for updating those UIDs with the server. Behrens, [0065], [0076] (user supplies UIDs to the server to link to user accounts). Accordingly, because it is the server that supplies the blacklisted and/or friend listed UIDs to the wireless device, a POSITA would have recognized that those UIDs would have been synced as needed. Lanning, ¶135.

For the reasons discussed above, it would have been obvious to modify the Requester Device to receive blacklists and/or friend lists from the server and use either list to filter received UIDs locally, conserving resources and avoiding undesirable devices.

The described modifications would have been further obvious to a POSITA as no more than the application of a known technique (Behrens' teachings of blacklists and local storage) to a known device ready for improvement (Eagle's system that determines whether detection of an Identified Device warrants notification to the server) to yield predictable results (selectively notifying the server of Identified Devices). *KSR*, 550 at 417-418. Lanning, ¶136.

A POSITA would have also had a reasonable expectation of success in modifying Eagle to implement Behrens' teachings. The use of lists to filter values (UIDs) is in no way unique to social introduction systems (*e.g.*, computers and networking components typically reference lists of IP addresses to allow or block

traffic), and comparing values to a blacklist or friend list would have only required basic data processing skills well within the skill of a POSITA. Lanning, ¶136.

5. Re-alerting a previously alerted device

With respect to claim limitations of the '918 that require receiving information and using that information to determine whether another device is in proximity to a user device (*e.g.*, as in claims 1 and 9), Eagle-Behrens renders obvious those limitations through the presentation of previously received alerts. *See* [1.G] below.

Eagle teaches that the same Identified Device may be encountered more than once. Eagle, [0023]-[0024]. While a Requester Device would not notify the server again of an Identified Device that it recently encountered (*i.e.*, Identified Device has not yet been removed from the Devices Log; Eagle, [0023]-[0024]), Eagle leaves to a POSITA whether the profile information of an Identified Device found on the recently encountered log would be presented again. Lanning, ¶¶137-138.

Behrens teaches that it would have been obvious to present the alert information on the Requester Device again for an Identified Device previously encountered. For example, if an Identified Device, “of which [a Requester Device] has previously stored the identifier and possibly received other data from, ... has reentered [the Requester Device’s] range,” then it is preferable to notify the user of that device again to make a connection. Behrens, [0035]. A POSITA would have

recognized that repeated alerts are advantageous where, *e.g.*, a user of a Requester Device did not or could not connect to the Identified Device the first time, wants repeated alerts because the Identified Device (and its owner) is of personal interest, or is prone to miss timely alerts on their device. Lanning, ¶139.

As Eagle's notifications to the user of the Requester Device are in the form of alerts including received profile information, it would have been obvious to present that alert information again, facilitating a connection between the devices. Eagle, [0007] (alerts include information useful to promote communication); Behrens, [0035] (sharing contact information). Furthermore, to conserve resources (*see* §VI.D.2), the Requester Device would not, again, notify the server and receive alert information, and it would have been obvious to present the same alert it previously received from the server. The use of stored information as an alternative to requesting information from a server would have been well-known and obvious to a POSITA. *See* EX1031, 36-38 (FWD in IPR2020-00979, finding it obvious, in this same field of endeavor, to check a local cache for information before querying a server). Lanning, ¶140.

Eagle leaves it to a POSITA to implement how the Requester Device would retrieve alert information. Eagle's server retrieves profile information for the alert via unique identifiers (UIDs). Eagle, [0019]-[0021], [0041], [0045], [0051] (identification values used to fetch profile data). Where the Requester Device

stores alert information for later retrieval, in view of Behrens as discussed above, it would have been obvious to use the same UIDs as relevant identifiers to catalog the information for storage and retrieval using a known method. Lanning, ¶140.

Therefore, it would have been obvious to modify Eagle's Requester Device to store received alert information for presentation to the user when a nearby Identified Device is detected more than once. The described modification would have been further obvious to a POSITA as no more than the application of a known technique (Behrens' teaching to provide an alert for a previously-alerted device) to a known device ready for improvement (Eagle's system that presents alerts but is silent as to whether alerts should be presented in certain situations) to yield predictable results (re-alerting the user). *KSR*, 550 at 417-418. Lanning, ¶141.

A POSITA would have also had a reasonable expectation of success in modifying Eagle to implement Behrens' teachings. Eagle already teaches receiving and presenting alerts on the Requester Device. Storage and retrieval of an alert (*e.g.*, contact information) would have only required basic data management skills well within the skill of a POSITA. Lanning, ¶142.

E. Mapping to Challenged Claims

Where collateral estoppel applies to a limitation because of the PTAB's final findings (with all appeals exhausted) regarding Eagle or Behrens, Petitioner has

stated below “*Collateral estoppel applies*” with cites to the relevant PTAB finding(s).

1. Claim 1

a. [1.PRE] “A mobile wireless device comprising:”

To the extent this preamble is limiting, Eagle teaches *a mobile wireless device* (e.g., a Bluetooth phone)

Eagle describes that a first Bluetooth phone carried by individual 203 (a Requester Device) is a wireless device that includes “short range radio transceivers that use the Bluetooth protocol” for communications. Eagle, Abstract, [0018]. For example, Fig. 2 (below) illustrates communications between a first Bluetooth phone carried by individual 203, a second Bluetooth phone carried by individual 205, and remote server 220. Eagle, Fig. 2, [0018], [0022]. Lanning, ¶¶143.

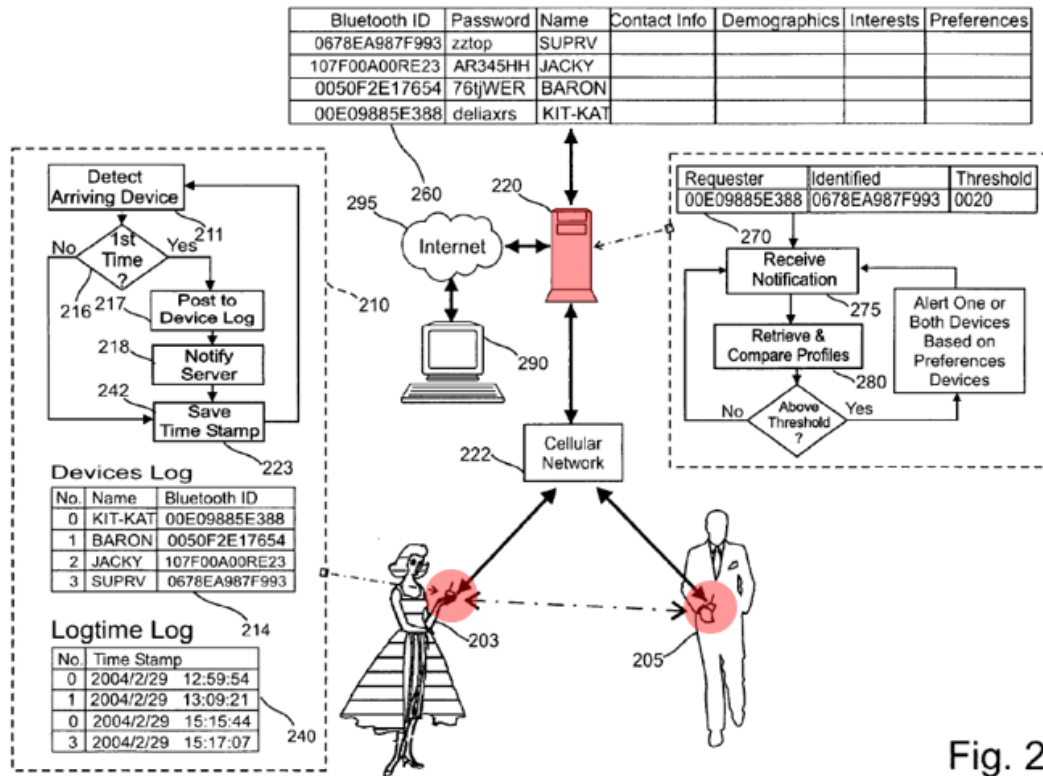


Fig. 2

b. [1.A] “a first radio; a second radio;”

Collateral estoppel applies: (*Eagle*) regarding communications with a server over a wide area link, EX1015, 19-30; EX1017, 16-18, 27-28; and regarding communication with a wireless device via a short-range wireless protocol, EX1015, 20; EX1017, 17-18.

Eagle teaches that the Requester Device is a cellular telephone that includes a “long range communications interface coupled to [a] long range communications network” (*first radio*) and “short range radio transceivers that use the Bluetooth protocol” (*second radio*). Eagle, [0018], claim 2; *see also* [0019]-[0020], [0022], [0028], [0038]-[0040]. Lanning, ¶¶144-145.

- c. **[1.B] “one or more processors; 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:”**

Eagle teaches the Requester device including *one or more processors*. Eagle, [0019] (“Each... Bluetooth enabled cellular phone[] includes a processor that is specially programmed”); *see also* [0020], [0028], claim 2.

Eagle teaches the Requester Device including *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* (e.g., the processor executes programming installed on the Requester Device).

Eagle teaches that its method for facilitating networking communications is performed, in part, by executing an application program that is “downloaded” and “installed” on the Requester Device. Eagle, [0028]-[0029]. Downloading, installing, and executing an application program as described obviously, if not necessarily, requires a *memory* on the device coupled to the processor. Lanning, ¶¶ 146-148; Olkkonen, 15:31-34, 35:39-41, 49:56-59 (describing programs stored in memory and executed by processors). *See also* Eagle, [0023]-[0024] (describing a memory for storing log data).

- d. [1.D] “receiving, using the first radio, identifier related information associated with a proximity beacon service, from one or more servers;”

Collateral estoppel applies: (Eagle) regarding receiving stored information from the server based on a unique identifier, EX1015, 19-30; EX1017, 16-18, 27-28.

Eagle-Behrens teaches *receiving, using the first radio* (e.g., receiving using the long-range communications interface), *identifier related information associated with a proximity beacon service* (e.g., information associated with Eagle’s social introduction system, such as blacklists, friend lists, and alerts), *from one or more servers* (e.g., from a server).

Eagle teaches the Requester Device communicating with a server using the long-range communications interface. Eagle, [0004], [0007], [0011], [0020]-[0021]. The server performs functions for Eagle’s social introduction system (“BlueAware”), which is a *proximity beacon service* that facilitates communications between Bluetooth devices such as the Requester Device and other Bluetooth devices “used as beacons to identify [themselves] to other nearby devices.” Eagle, [0008], [0043]-[0061] (describing server operations).

The Requester Device receives *identifier related information from the server* as discussed below. Lanning, ¶¶149-151.

i. Receiving blacklists and friend lists

It would have been obvious for the Requester Device to receive blacklist information and/or friend list information from the server. *See* §VI.D.4.

Regarding blacklists, Behrens teaches that the Requester Device “may store [unique identifiers (UIDs)] to be ignored in a blacklist,” received as instructions from the server, to eliminate spam and other unwanted behavior. Behrens, [0101]-[0102], [0124]. The blacklist received and used by the Requester Device to ignore UIDs and is therefore *identifier related information*. Lanning, ¶¶152-153.

Regarding friend lists, Eagle teaches that the server stores profile information “specifying a set of device IDs for devices owned by ‘friends’” that form a “trust network” of devices. Eagle, [0056], [0066]-[0067]. Based on the friend list, the Requester Device is only alerted to the presence of nearby Identified Devices that are in the Requester Device’s friend list—*i.e.*, part of its trust network. Eagle, [0056]. Lanning, ¶154.

As discussed above (§VI.D.4), it would have been obvious for the Requester Device to receive the friend list from the server and use it to filter received UIDs locally, conserving resources. Accordingly, the friend list is *identifier related information*. Lanning, ¶155.

ii. Receiving alerts

Eagle teaches notifying the server with the unique identifiers of the nearby devices (nearby Identified Devices). Eagle, [0048]; UIDs in view of Behrens, as discussed in §VI.D.1. The server uses the received UIDs to fetch profile information from a profile database. Eagle, [0005], [0020], [0041], [0045], [0050]-[0051].

The server compares the Requester Device's profile information with the Identified Device's profile information to determine whether they satisfy matching criteria. Eagle, [0005], [0020], [0024], [0040], [0042], [0048], [0051]. If so, an alert message is transmitted to the Requester Device. Eagle, [0006], [0020], [0052].

The alert message includes stored profile information associated with the matching Identified Device, *e.g.*, contact information and “any other information which is of use in a specific application” and useful to “promote communication between[] nearby devices and their owners.” Eagle, [0007], [0020]-[0021], [0053], [0058].

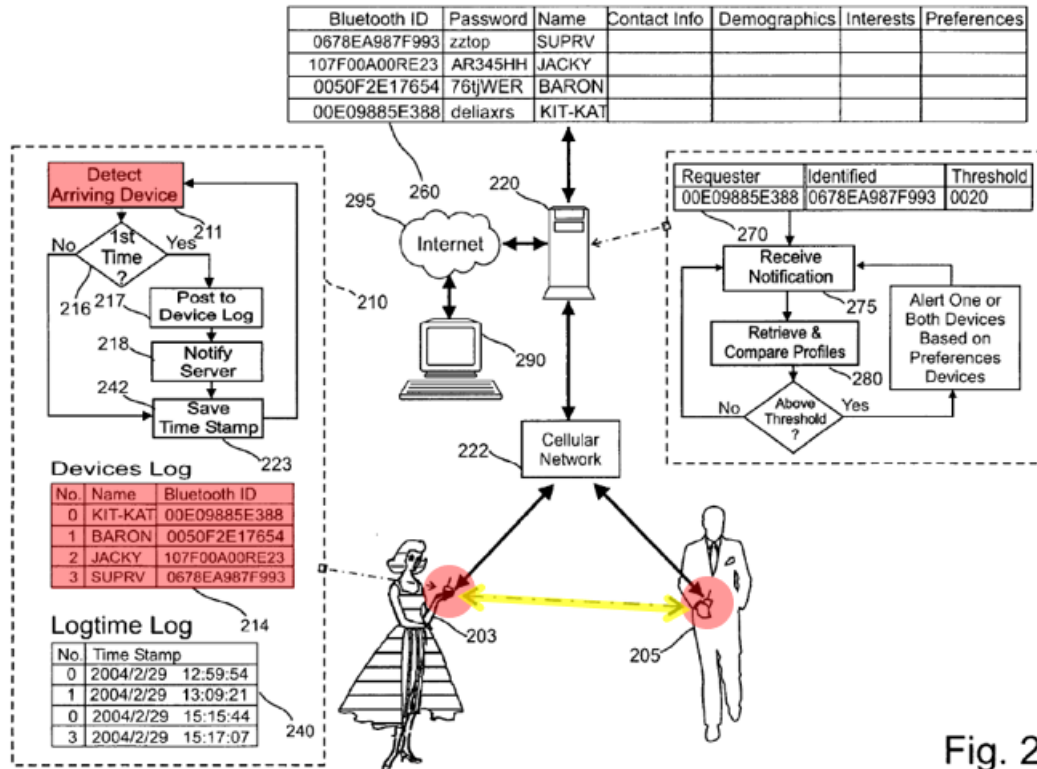
The server generates alerts from profile information fetched from a database using the UIDs of Identified Devices, and the profile information is therefore *identifier related information*. Lanning, ¶¶156-159.

- e. **[1.E.I] “receiving, using the second radio, a plurality of short range transmissions, including a plurality of proximity beacon transmissions when the device is located within a detection range of one or more beacon transmitter devices associated with the proximity beacon service, each of the proximity beacon transmissions including”**

Collateral estoppel applies: (Eagle) regarding receiving transmissions from a second wireless device via short-range protocol, EX1015, 20; EX1017, 17-18.

Eagle-Behrens-Olkkonen teaches *receiving, using the second radio (e.g., receiving the short range transceivers via Bluetooth protocol), a plurality of short range transmissions, including a plurality of proximity beacon transmissions (e.g., inquiry responses containing identifying information from Identified Devices), when the device is located within a detection range of one or more beacon transmitter devices (e.g., the Requester Device receives inquiry responses from discoverable Identified Devices in Bluetooth range) associated with the proximity beacon service, each of the proximity transmissions including (e.g., Identified Devices participating in Eagle’s social introduction system transmit certain information, see [1.E.II]-[1.E.IV]).*

Eagle explains that Bluetooth devices transmit *beacon transmissions* when “used as beacons to identify a device to other nearby devices” by transmitting “device identification codes.” Eagle, [0008]. The device log (Fig. 2, below) shows exemplary separate fields “name,” “Bluetooth ID,” etc. Lanning, ¶¶160-161.



By way of example, the Requester Device may detect the presence (step 211) of a second Bluetooth phone carried by individual 205 (an Identified Device) via reception of the Identified Device’s beacon transmissions, including for example a “Bluetooth ID” (an assigned address value). Eagle, Fig. 2, [0022]. This information is received when a Requester Device “perform[s] an inquiry function to determine the identity and Device Class of other ‘discoverable’ Bluetooth devices,” and the Identified Device responds to the inquiry. Eagle, [0033]-[0038]. Discoverable Bluetooth devices must be “within Bluetooth range” of the Requester Device to receive and respond to inquiry messages—approximately 10-100 meters. Eagle, [0003]-[0005], [0020], [0030], [0033]-[0037]. Lanning, ¶162.

Additionally, a Devices Log 214 stored in the Requester Device “indexes every device encountered by the phone” and, as shown in Fig. 2 above, the Requester Device has encountered several devices. Eagle, [0022]-[0025]. Accordingly, based on communications with Identified Devices, Eagle teaches that the Requester Device receives a *plurality* of beacon transmissions from a plurality of Identified Devices. Lanning, ¶163.

Discussed with respect to limitations [1.E.II]-[1.E.IV] below, Eagle-Behrens-Olkkonen teaches that Identified Devices participating in Eagle’s social introduction system (*i.e., associated with the proximity beacon service*) transmit certain information in *each of the proximity beacon transmissions*, as claimed. Lanning, ¶164.

f. [1.E.II] “a respective MAC address,”

Eagle-Behrens discloses respective beacon transmissions including *a respective MAC address* in two separate ways.

i. MAC address in UIDs

Collateral estoppel applies: (*Eagle*) regarding receiving a Bluetooth Device address as unique identifier, EX1015, 35-36; (*Behrens*) regarding receiving MAC addresses in UIDs, EX1031, 46-48.

Eagle-Behrens teaches *a respective MAC address* (*e.g., a BD_ADDR is included in the UIDs*).

As discussed above (§VI.D.1), Behrens teaches that the Identified Device identifies itself to the Requester Device with a transmission including a combination of UIDs including, *e.g.*, its respective 48-bit “Bluetooth Device Address” or BD_ADDR. Behrens, [0061], [0097], [0122]. The ’918 similarly acknowledges that a “MAC address” is, *e.g.*, a “Bluetooth BD_ADDR.” EX1001, 9:41, 26:4-7.

Eagle-Behrens’s 48-bit BD_ADDR included as a UID identifying the Identified Device is therefore *a respective MAC address*. Lanning, ¶¶166-168.

ii. MAC address in Bluetooth communications

Eagle teaches that the Requester Device and Identified Device use Bluetooth protocols. Eagle, [0018], [0028]. Accordingly, the Identified Device identifying itself to the Requester device would have included *a respective MAC address* in its inquiry response. Eagle, [0033]-[0037] (describing a Bluetooth discovery process between devices, such as a Requester Device (sending inquiries) and Identified Device (responding to inquiries)); Olkkonen, 2:23-31 (“inquiry response is a message packet containing the responding device’s Bluetooth Device Address”), 27:12-20 (FHS packet structure for an inquiry response contains a BD_ADDR and clock); EX1008, 283 (FHS packet sent in response to an inquiry contains the Bluetooth device address of the sender).

The '918 similarly acknowledges that the MAC address of the transmitting device is “always broadcast in any operation of a Bluetooth or [Wi-Fi] link.”

EX1001, 10:61-63. Lanning, ¶¶169-170.

g. [1.E.III] “a respective unique identifier, and”

Collateral estoppel applies: (*Eagle*) regarding receiving a unique identifier, EX1015, 20; EX1017, 17-18; (*Behrens*) regarding combination UUIDs, EX1031, 46-48.

Eagle-Behrens teaches each beacon transmission comprising *a respective unique identifier* (e.g., UUIDs including a unique number uniquely identifying a device and its owner).

As discussed above (§VI.D.1), the Identified Device can identify itself to the Requester Device with a transmission including a combination of UUIDs. Behrens teaches that UUIDs are “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.” Behrens, [0061], [0097]. Eagle-Behrens therefore teaches the beacon transmission including *a unique identifier*, such as a unique number or symbol that identifies the Identified Device and its owner. UUIDs like a unique number or symbol are included in beacon transmissions in addition to the MAC address identified for [1.E.II] above because UUIDs may be a combination of different unique identifiers. Behrens, [0097], [0122]. Lanning, ¶¶171-172.

h. [1.E.IV] “a Proximity Beacon Service Identifier (PBSI);”

Eagle-Olkkonen teaches each beacon transmission comprising *a Proximity Beacon Service Identifier (PBSI)* (e.g., service class information identifying Eagle’s social introduction system).

As discussed above (§VI.D.2), it would have been obvious for an Identified Device to respond to inquiries from a Requester Device with service class information for the purpose of filtering UIDs.

Service class information includes information that Identified Devices access from their service registries “characterizing the ad hoc network” of which it is a member. Olkkonen, 5:27-33, 12:40-48, 13:33-43, and 17:49-63. This information includes service class information identifying running application programs (Olkkonen, 5:13-17, 17:17-22, 30:22-28, Fig. 5) and, in view of Eagle, would have included an identification of Eagle’s social introduction system—a *Proximity Beacon Service Identifier* identifying the *proximity beacon service* provided by Eagle’s application program and server. See §VI.D.2. Lanning, ¶¶174-177.

i. [1.F.I] “determining if a particular short range transmission of the plurality of short range transmissions a) includes a MAC address, and”

Eagle teaches this limitation. The Requester Device maintains a Devices Log of detected Identified Devices by their unique identifiers, such as its Bluetooth

device address (BD_ADDR) (*a MAC address*). Eagle, [0022]-[0023]. Logging the MAC address requires the Requester Device to parse inquiry responses to find the location of the MAC address and, if it finds a value in that location (*i.e., determines that the particular inquiry response includes a MAC address*), then records the value. Lanning, ¶¶178-179.

- j. **[1.F.II] “b) includes the proximity beacon service identifier (PBSI) and if c) the PBSI indicates the particular short range transmission is a proximity beacon transmission associated with the proximity beacon service;”**

Eagle-Olkkonen teaches this limitation. The Requester Device receives, from Identified Devices, inquiry responses including *PBSIs* such as service class information identifying Eagle’s social introduction system. *See* [1.E.IV]. Lanning, ¶¶180-181.

As discussed above (§VI.D.2), Eagle teaches the Requester Device determining whether the detection of an Identified Device “warrants” the transmission of the Identified Device’s UIDs to the server (Eagle, [0020], [0024], [0040], [0051]), and Olkkonen teaches to filter and select only the UIDs of Identified Devices that are relevant to Eagle’s social introduction system. This selection of UIDs is based on the received service class information (identifying service relevant to Eagle’s social introduction system; Olkkonen, 11:33-60, 22:34-43; §VI.D.2). Selecting techniques (*i.e., techniques for analyzing data to determine*

the presence of a desired value) were well-known in the art. *E.g.*, Olkkonen, 22:8-12, 22:34-43 (determining if data “matches” a desired type). Lanning, ¶182.

To determine whether inquiry responses include service class information indicating that the UUIDs in those inquiry responses should be selected for notification to the server (*i.e.*, *determines if the PBSI indicates the particular short range transmission is a proximity beacon transmission associated with the proximity beacon service*), the Requester Device must therefore parse the inquiry responses to find the service class information, and, if it finds values in those service class locations (*i.e.*, *determines that the inquiry response includes the PBSI*), then determines if the service class information identifies Eagle’s social introduction system. Lanning, ¶183.

- k. **[1.G] “then: determining if an entity or object associated with the proximity beacon service is in proximity to the mobile wireless device, by utilizing the identifier related information and the unique identifier.”**

- i. **Eagle**

As an initial matter, a POSITA would have recognized that the proximity of a Bluetooth device is necessarily determined by the reception of Bluetooth signals due to their limited physical range. *See* [1.E.I]. Therefore, a beacon transmission received from a Bluetooth device (and/or the entity/person holding or associated with it) is already in “proximity” to the Requester Device. Lanning, ¶184.

Additionally, Eagle's system *then determines*⁹ *if an entity or object associated with the proximity beacon service (e.g., with respect to an Identified Device that had been determined to be relevant to Eagle's social introduction system, showing an alert) is in proximity to the mobile wireless device (e.g., the alert indicates the device is nearby), by utilizing the identifier related information (e.g., by displaying received profile information) and the unique identifier (e.g., alerts received and displayed as showing proximity are associated with the UUIDs utilized for identifying the particular Identified Device).* For example, a "nearby...restroom" (Eagle, [0061]) is determined to be in proximity to a tradeshow beacon by alerting the user of its presence or location with the information received from the server (Eagle, [0020]-[0021], [0048]). The restroom in proximity is directly associated with a tradeshow beacon's UUIDs because the associated UUIDs' server data identifies that particular restroom via the server's visual notification/alert functions processed by the device (Eagle, [0020]-[0021], [0048]) and is therefore *utilized* in the determination of nearby restroom proximity. Lanning, ¶185.

To the extent [1.G] may be satisfied in other ways (e.g., by filtering UUIDs for notification to the server and/or by determining permission for disclosing

⁹ See Claim Interpretation in §V.A.

proximity; *see* §V.A), Eagle-Behrens teaches additional proximity determinations as discussed below. Lanning, ¶186.

ii. Blacklists and friend lists

As discussed for [1.D] (§VI.E.1.d.i), Eagle-Behrens teaches receiving UID blacklists and/or friend lists that identify UIDs to ignore or to select for alerts, respectively. That is, the Requester Device using a blacklist would ignore received UIDs on the blacklist and not notify the server of those UIDs. Behrens, [0101]-[0102], [0124] (“ignore” UIDs). Likewise, the Requester Device using a friend list would notify the server of UIDs when they are on the friend list. Eagle, [0056] (alert messages only for trusted persons on friend lists). The friend list only serves as an initial filter of UIDs, as the Requester must still contact the server to determine whether the UID on the trusted friend list has “common interests [and] is nearby.” Eagle, [0056].

Accordingly, Eagle-Behrens teaches *determining if an entity or object associated with the proximity beacon service (e.g., determining, in relation to the Identified Device that identified Eagle’s social introduction system, see [1.F.II]) is in proximity to the mobile wireless device (e.g., deciding to notify the server of UIDs and receive alerts in response that determine that the Identified Device is nearby) by utilizing the identifier related information* (using the blacklist and/or

friend list as a filter of UIDs) *and the unique identifier* (checking UIDs against those lists). Lanning, ¶¶187-188.

iii. Alerts

Eagle further teaches that the same Identified Device may be encountered more than once. Eagle, [0023]-[0024] (scenarios include detecting an Identified Device already in the Devices Log). While a Requester Device would not notify the server again of an Identified Device that it recently encountered (*i.e.*, Identified Device has not yet been removed from the Devices Log; Eagle, [0023]-[0024]), Eagle leaves to a POSITA whether the profile information of an Identified Device found on the recently encountered log would be presented again.

As discussed above (§VI.D.5), it would have been obvious to present the alert information on the Requester Device again for an Identified Device previously encountered, as taught by Behrens. For example, Behrens teaches that if an Identified Device, “of which [a Requester Device] has previously stored the identifier and possibly received other data from, ... has reentered [the Requester Device’s] range,” then it is preferable to notify the user of that device again to make a connection. Behrens, [0035]. As Eagle’s notifications to the user of the Requester Device are in the form of alerts including received profile information, it would have been obvious to present that alert information again, facilitating a

connection between the devices. Eagle, [0007] (alerts include information useful to promote communication); Behrens, [0035] (sharing contact information).

Accordingly, Eagle-Behrens teaches *determining if an entity or object associated with the proximity beacon service (e.g., determining, in relation to the Identified Device that identified Eagle's social introduction system, see [1.F.II]) is in proximity to the mobile wireless device (e.g., deciding to alert the user of the Requester Device of identified nearby Identified Devices) by utilizing the identifier related information* (using the previously received alert information for presentation to the user) *and the unique identifier (e.g., UUIDs are the identifying information used throughout Eagle's system to, e.g., log and lookup devices in the Device Log; UUIDs here are used to identify the UUID as previously logged and to retrieve profile information for alerts).* Lanning, ¶¶189-191.

2. Claim 2: “[Claim 1], wherein the MAC address is a randomly generated 48 bit number matching a format of a Bluetooth BD_ADDR.”

Eagle teaches that the MAC address is a 48-bit number matching a format of a Bluetooth BD_ADDR (e.g., the Identified Device's BD_ADDR).

To the extent Eagle does not explicitly describe that *the MAC address is a randomly generated 48 bit number matching a format of a Bluetooth BD_ADDR*, it would have been obvious to a POSITA to use a randomly generated number for the BD_ADDR for privacy and security.

In particular, POSITAs recognized that concerns regarding privacy and tracking through identifiers—and the changing of identifiers as a solution to those concerns—was well-known in short-range wireless communications systems. *See* §VI.D.1. Known solutions included the use of randomly generated identification numbers, such as a periodically “randomized version of the BD_ADDR” to be “used in all the functions of the Bluetooth device that normally use the BD_ADDR.” EX1011, [0006]-[0013]. As documented in the prior art, one method for randomizing the BD_ADDR included generating a pseudonym BD_ADDR with a random number generator and substituting the pseudonym BD_ADDR for the real BD_ADDR in transmissions such as inquiry responses. EX1011, [0054], [0057], [0088]. Lanning, ¶194.

Therefore, a POSITA would have been motivated to modify the Identified Device (and other Bluetooth devices in the system) to randomize the BD_ADDR value transmitted in Bluetooth communications and would have had a reasonable expectation of success in doing so. Lanning, ¶¶192-195.

3. Claim 3

- a. [3.PRE] “The mobile wireless device of claim 1 wherein the one or more processors further execute the instructions to perform operations including:”**

The processor executes instructions. *See* [1.B]. Lanning, ¶196.

- b. **[3.A] “receiving, by the second radio, a first proximity beacon transmission including a first MAC address and a first unique identifier at a first time; and”**

Eagle-Behrens teaches this limitation for the same reasons discussed for [1.E].

In particular, Eagle-Behrens teaches receiving, by the second radio, a plurality of proximity beacon transmissions including “respective” MAC addresses and unique identifiers. *See* [1.E]. The limitation merely labels a particular beacon transmission and its contents, among the plurality, as “first.”

Furthermore, the receiving of the first beacon transmission may be defined as occurring at a *first time*. Lanning, ¶¶197-199.

- c. **[3.B.I] “receiving, by the second radio, a second proximity beacon transmission including a second MAC address and a second unique identifier at a second time,”**

Eagle teaches its system operating over many time periods, including a *second time period*. For example, Eagle teaches that the Requester Device periodically scans the environment for Identified Devices. Eagle, [0026], [0033]. Furthermore, the same Identified Device may be detected at different times (Eagle, [0023]) and a Requester Device may join and leave existing networks and activities, or detect and re-detect other devices as they move in and out of range of each other (Olkkonen, 1:46-61, 2:51-65 (explaining Bluetooth operations)). Any device that is in Bluetooth range of the Requester Device and that is in a

“discoverable” mode will respond to the Requester Device’s inquiries and be detected as an Identified Device. Eagle, [0019], [0033]-[0037].

For illustrative purposes to address this claim and other related limitations, it may be assumed that a particular Identified Device is detected one or more times at a *first time* (as discussed for [3.A])), and the same particular Identified Device is detected again one or more times at a *second time* that follows the first time period. In both time periods, the Identified Device remains a participant in the same services and networks (e.g., participating in Eagle’s social introduction system and running Eagle’s software, participating in an ongoing baseball game or CAD design project). For example, over the course of a work week or while attending a multi-day event (e.g., one day being a first time and a second day being a second time), a user of an Identified Device has “chang[ed] UIDs” overnight to present themselves with a “new online identity” on the second day while still having a “single user account” on the server. Behrens, [0061], [0115]; *see also* [0103] (user “exercise[s] control over which or how many UIDs are transmitted”). As discussed above (§VI.D.2), changing UIDs in this manner prevents tracking over time. Lanning, ¶¶200-201.

Accordingly, for the same reasons that Eagle-Behrens teaches *receiving, by the second radio, a first proximity beacon transmission including a first MAC address and a first unique identifier at a first time* (see [3.A]), Eagle-Behrens

teaches receiving, by the second radio, a second proximity beacon transmission including a second MAC address and a second unique identifier at a second time.

Lanning, ¶202.

d. [3.B.II] “the second MAC address being different from the first MAC address and”

Eagle-Behrens-Olkkonen teaches *the second MAC address being different from the first MAC address* in two separate ways .

i. MAC address in UIDs

Collateral estoppel applies: (*Behrens*) regarding changing UIDs, EX1031, 46-48.

Behrens teaches that (1) UIDs may be a combination of different UID values, and (2) UIDs change. *See* §VI.D.1, [1.E.III], [3.B.I]. An Identified Device’s UIDs may therefore be changed for the second time to use a WLAN MAC address instead of the BD_ADDR used in the first time period. Behrens, [0061], [0097], [0103], [0111], [0115], [0122]. Lanning, ¶¶203-204.

ii. MAC address in Bluetooth communications

A POSITA would have been motivated to modify the Identified Device (and other Bluetooth devices in the system) to periodically randomize the BD_ADDR value transmitted in Bluetooth communications for privacy and security. *See* discussion of claim 2 above.

Accordingly, because the BD_ADDR is periodically randomized, *the second MAC address is different from the first MAC address*. Lanning, ¶¶205-206.

e. [3.B.III] “the second unique identifier being different from the first unique identifier; and”

Behrens teaches that (1) UUIDs may be a combination of different UUID values, and (2) UUIDs change. *See* §VI.D.1, [1.E.III], [3.B.I]. An Identified Device’s UUIDs may therefore be changed to *be different* for the second time to use a unique “symbol,” instead of the unique “number” used in the first time. Behrens, [0061], [0097], [0103], [0115], [0122]. Lanning, ¶¶207-208.

f. [3.C] “associating the first and second unique identifier with a single beacon transmitter device.”

Eagle-Behrens teaches this limitation.

As discussed above for [3.B.I], the first and second unique identifier (UUIDs) received in the first and second times, respectively, are received from the same Identified Device—*i.e.*, the first and second UUIDs come from the same *single beacon transmitter device*.

As discussed for [1.D], the Requester Device notifies the server of the UUIDs so that the server fetches stored profile information from a profile database and then transmits alerts back to the Requester Device identifying the Identified Device. When the Identified Device has been removed from Eagle’s log of recently detected devices between the first and second time, then the same actions of

notifying the server, receiving an alert, and displaying the alert will be performed each time. Eagle, [0023]-[0024]. The first and second alerts contain, *e.g.*, the phone number or other contact information for the Identified Device and any other information useful to “promote communication between[] nearby devices and their owners.” Eagle, [0007], [0020]-[0021], [0053].

Accordingly, because the Requester Device receives the same contact information for the same Identified Device in response to notifying the server of the *first unique identifier* and the *second unique identifier*, the Requester Device *associates* both UIDs with *a single beacon transmitter device*. Lanning, ¶¶209-212.

4. **Claim 4: “[Claim 1], wherein the one or more processors further execute the instructions to perform operations including: further determining that at least one beacon transmitter device associated with the proximity beacon service is in proximity to the mobile wireless device, by utilizing an action function including one or more previously downloaded¹⁰ unique identifiers.”**

The processor executes instructions. *See* [1.B].

¹⁰ “Previously downloaded unique identifiers” lacks antecedent basis. Petitioner applies prior art to this term as best understood and reserves the right to pursue §112 deficiencies in district court. Lanning, ¶214.

Eagle-Behrens teaches *determining that at least one beacon transmitter device associated with the proximity beacon service is in proximity to the mobile wireless device* based on blacklists and friend lists or alerts. See [1.G].

As discussed regarding the *determining* using blacklists and friend lists, the Requester Device checks whether UUIDs received from Identified Devices are present on those blacklists and friend lists. See discussion of [1.G]. Accordingly, *further determining* is performed *by utilizing an action function (e.g., comparing UUIDs against the blacklist and/or friend list) including one or more previously downloaded unique identifiers (e.g., the blacklist and friend list received from the server include UUIDs of Identified Devices to be ignored or notified to the server)*. Lanning, ¶¶213-215.

As discussed regarding the *determining* using prior alerts of Identified Device profile information, the Requester Device presents previously received alert information to the user if a recently detected Identified Device (still on the Devices Log) is detected again by the Requester Device. See discussion of [1.G]. Furthermore, because Eagle and Behrens each teach that Bluetooth devices and alert information are both associated with UUIDs, both the determination that an Identified Device is recently detected and the retrieval of alert information would have been performed using those UUIDs. Eagle, [0031] (devices identified by unique identification values), [0041] and [0051] (profile information fetched by

unique identifiers); Behrens, [0035] (re-detected device has same “identifier”). Accordingly, *further determining* is performed by utilizing an action function (e.g., presenting previously received alert information) *including one or more previously downloaded unique identifiers* (e.g., Identified Devices in Eagle’s Devices Log are detected by UIDs, and those UIDs were previously downloaded from Identified Devices during discovery; using UIDs to identify previously downloaded alert information). Lanning, ¶216.

5. Claims 8/31

- a. **[8.PRE]/[31.PRE] “[Claim 1][Claim 3] wherein the one or more processors further execute the instructions to...”**

The processor executes instructions. *See* [1.B]. Lanning, ¶¶217, 272-273.

- a. **[8.A]/[31.A] “receiving, via a second radio, the plurality of proximity beacon transmissions further includes receiving a first unique identifier at a first time that is different from a second unique identifier received at a second time; and”**

See [3.A] (receiving first unique identifier at first time via second radio), [3.B.I] (receiving second unique identifier at second time via second radio), and [3.B.III] (first and second unique identifiers are different). Lanning, ¶¶218, 274.

- b. **[8.B]/[31.B] “associating the first and second unique identifier with a single beacon transmitter device.”**

See [3.C]. Lanning, ¶¶219, 275.

6. Claim 9

Claim 9 recites a “method” “for facilitating use of proximity beacons,” which includes steps substantially similar to the functions of claim 1’s “mobile wireless device” and are obvious over Eagle-Behrens-Olkkonen for the same reasons. *See* §VI.E.1.

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

To the extent this preamble is limiting, Eagle teaches *a method for facilitating use of proximity beacons* (e.g., using beacon transmissions from Bluetooth devices), *the method executing within a mobile device* (e.g., the Requester Device includes a processor to execute instructions). *See* discussion of claim 1. Lanning, ¶220.

- b. **[9.A] “communicating... identifier related information...;”**

See [1.D]. Lanning, ¶¶221-225 ([9.A]-[9.E])

- c. **[9.B] “receiving... a plurality of proximity beacon transmissions...;”**

See [1.E.I]-[1.E.IV].

- d. **[9.C] “...a particular short range transmission... includes a MAC address,”**

See [1.F.I].

- e. **[9.D] “...(PBSI) is present, and c) determining that... the particular short range transmission is... associated with the proximity beacon service; and”**

See [1.F.II].

- f. **[9.E] “...then... determining that an entity or object... is within proximity....”**

See [1.G].

7. Claim 10

- a. **[10.PRE] “The method of claim 9,”**

See claim 9.

- b. **[10.A] “wherein a first one of the plurality of proximity beacon transmissions received at a first time includes a first unique identifier, and wherein a second one of the plurality of proximity beacon transmissions received at a second time includes a second unique identifier the second unique identifier being different from the first unique identifier; and”**

See [3.A] (first unique identifier), [3.B.I] (second unique identifier), and [3.B.III] (first and second unique identifiers are different). Lanning, ¶227.

- c. **[10.B] “associating both the first unique identifier and the second unique identifier with a particular entity or object in proximity to the mobile device.”**

See [3.C.] (associating with a single Identified Device, which is an object in Bluetooth proximity to the Requester Device, and with the Identified Device’s user, which is an entity in Bluetooth proximity; *see* Eagle, [0007], [0020]-[0021] (alert identifies device and its owner). Lanning, ¶228.

8. **Claim 11: “[Claim 9] wherein the MAC address is selected from a group consisting of (a) a randomly generated 48 bit number matching a format of a MAC address and (b) a Bluetooth BD_ADDR.”**

See claim 2 (randomly generated BD_ADDR).

See [1.E.II] (BD_ADDR).

Lanning, ¶¶229-230.

9. **Claim 12**

- a. **[12.PRE] “The method of claim 9”**

See claim 9.

- b. **[12.A] “wherein a first one of the plurality of proximity beacon transmissions is received at a first time and includes a first unique identifier and first MAC address, and the Proximity Beacon Service Identifier (PBSI); and”**

See [1.E.I]-[1.E.IV] (receiving a unique identifier, MAC address, and PBSI)

and [3.A] (defining a first reception at a first time). Lanning, ¶232.

- c. **[12.B] “wherein a second one of the plurality of proximity beacon transmissions received at a second time includes a second unique identifier different from the first unique identifier and a second MAC address different from the first MAC address, and the Proximity Beacon Service Identifier; and”**

See [1.E.I]-[1.E.IV] (receiving a unique identifier, MAC address, and PBSI)

and [3.B.I]-[3.B.III] (defining a second reception at a second time with a different unique identifier and different MAC address).

Additionally, Eagle-Olkkonen teaches that the PBSI in the first and second transmissions is the same because, *e.g.*, the first and second transmissions are received from the same Identified Device participating in Eagle's same social introduction system, which is identified by the same PBSI. *See* [3.B.I]. Lanning, ¶¶233-234.

- a. **[12.C] “associating both the first unique identifier and the second unique identifier with the same entity or object in proximity to the mobile device.”**

See [10.B]. Lanning, ¶235.

10. **Claims 13/15: “[Claim 9, further comprising][Claim 1, wherein the instructions further comprise:] preventing the sending of the unique identifier, using the first radio, to the one or more servers, based upon previous detections of the respective unique identifier associated with the proximity beacon transmission.”**

Collateral estoppel applies: (*Eagle*) regarding determining to transmit notifications to the server based on timestamps, EX1015, 17, 23-24; EX1017, 14.

Eagle teaches maintaining a timestamped log of encountered devices, used to determine whether to transmit a notification message with UIDs to the server. Eagle, [0022]-[0024], [0048].

Therefore, if it is determined that a unique identifier (UID) received in an inquiry response represents a device recently detected, the Requester Device will not notify the server of the UID.

Accordingly, Eagle teaches *preventing the sending of the unique identifier* (e.g., preventing the notification of UUIDs to the server), *using the first radio, to the one or more servers* (e.g., communication with the server uses the first radio; see [1.A] and [1.D]), *based upon previous detections of the respective unique identifier associated with the proximity beacon transmission* (e.g., based upon recent detection of the same UUID received in the inquiry response). Lanning, ¶¶236-238, 242.

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

Collateral estoppel applies: (Eagle) (see claims 13/15 above).

Eagle-Behrens teaches *further sending the unique identifier* (e.g., notifying the server with UUIDs of an Identified Device not recently detected), *using the first radio, to at least one server of the one or more servers* (e.g., communication with the server uses the first radio; see [1.A] and [1.D]), *and receiving further information relating to an object or entity associated with being within proximity to the mobile device* (e.g., receiving an alert including profile information of the nearby Identified Device and its owner).

Eagle teaches notifying the server with the unique identifiers of the nearby Identified Devices, e.g., when an Identified Device is not on its Devices Log of

recently detected devices. Eagle, [0023]-[0024], [0048]; UIDs in view of Behrens. The server uses the received UIDs to fetch profile information from a profile database. Eagle, [0005], [0020], [0041], [0045], [0050]-[0051]. The server compares the Requester Device's profile information with the Identified Device's profile information to determine whether they satisfy matching criteria. Eagle, [0005], [0020], [0024], [0040], [0042], [0048], [0051]. If so, an alert message is transmitted to the Requester Device. Eagle, [0006], [0020], [0052].

The alert message includes stored profile information associated with the matching Identified Device, *e.g.*, contact information and “any other information which is of use in a specific application” and useful to “promote communication between[] nearby devices and their owners.” Eagle, [0007], [0020]-[0021], [0053], [0058]. Lanning, ¶¶239-241, 251.

12. Claims 16/24: “[Claim 1, wherein the instructions further comprise:][Claim 9, additionally comprising:] controlling further communications between the mobile device and at least one device or server associated with an entity or object in proximity to the mobile device.”

Eagle-Behrens teaches this limitation in two ways.

First, as discussed for claim 13, Eagle teaches preventing the Requester Device from notifying the server with UIDs of nearby Identified Devices recently encountered. Eagle therefore teaches *controlling further communications (e.g., not sending a notification to the server) between the mobile device and at least one*

device or server associated with an entity or object in proximity to the mobile device (e.g., between the Requester Device and the server, which is associated with Identified Devices as providing services under Eagle’s social introduction system). Lanning, ¶¶243-244.

Second, as discussed for claim 1, Eagle-Behrens teaches receiving, from a server, a blacklist of UIDs that the Requester Device should ignore. Behrens, [0101]-[0102], [0124]. POSITAs would have recognized that obvious ways for implementing blacklisted UIDs included not notifying the server of such UIDs (*see* Eagle, [0023]-[0025] (“determining whether... detection of a given device warrants the transmission of a notification message to the server”)) and/or blocking the Requester Device from contacting those associated Identified Devices (*see* Behrens, [0026], [0101] (blacklists “stop the other user[s] from further contacting [the user to be ignored]”)). Lanning, ¶245.

Eagle-Behrens therefore teaches *controlling further communications between the mobile device and at least one device or server associated with an entity or object in proximity to the mobile device (e.g., not permitting communication between the Requester Device and the server for notification of blacklisted UIDs, the server being associated with Identified Devices as providing services under Eagle’s social introduction system; preventing communication*

between the Requester Device and other Identified Devices on the blacklist).

Lanning, ¶¶246, 265.

13. **Claim 17: “[Claim 9], further comprising: receiving, using the first radio, access code information by the mobile device from at least one of the servers; and utilizing the access code information to gain access to the entity or object determined to be in proximity to the mobile device.”**

Eagle teaches that the Requester Devices receives alerts from the server (*using the first radio, see [1.A] and [1.D]*) including *access code information* in the form of contact information, such as phone numbers, email addresses, and website URLs. Eagle, [0007], [0050]. Upon receiving an alert, the Requester Device *utilizes* the contact information to connect with (or *gain access to*) the nearby Identified Device and its owner/user. Eagle, [0058] (alert contains a phone number for the Requester Device to call, useful in crowded areas), [0063] (system “put[s] the attendee in contact” with others). Because Eagle only provides contact information to matched profiles, contact information acts as credentials that grant access to the other devices, people, and resources, and are therefore *access codes* as claimed. Lanning, ¶¶247-248.

- 14. Claims 18/28: “[Claim 9][Claim 1], wherein [the] receiving [of] the identifier related information, using the first radio, is performed in response to [executing instructions for] sending at least the unique identifier to at least one of the one or more servers using the first radio.”**

Eagle teaches *receiving the identifier related information, using the first radio* (e.g., receiving alerts of profile information from the server). See [1.A], [1.D], [9.A]. See also [1.B] (executing instructions).

As discussed for [1.D] and claim 14, alerts are received from the server *in response to sending at least the unique identifier to at least one of the one or more servers using the first radio* (e.g., the Requester Device receives alerts in response to notifying the server with UIDs of nearby Identified Devices). Lanning, ¶¶249-250, 269-271.

- 15. Claim 20: “[Claim 19] wherein the further information relates to... advertising content.”¹¹**

As discussed for claims 14 and 19, Eagle teaches receiving *further information* including profile information about an Identified Device and its owner. This information is *advertising content* because it advertises the Identified Device (and its owner) as having interests relevant to the Requester Device (and its owner). Eagle, [0007], [0021], [0058].

¹¹ “Advertising” content is non-functional descriptive material that carries no patentable weight. MPEP §2111.05.

Other alerted information (*e.g.*, instructions, announcements, resources, facilities, products, expertise) are also *advertising content*, as they make the user of the Requester Device aware of nearby information, goods, and services. Lanning, ¶¶252-253.

16. Claim 22: “[Claim 19] wherein the further information relates to a nearby user of an application on another device, in common with an application on the mobile device.”

i. Eagle’s BlueAware application

Eagle teaches that its method for facilitating networking communications is performed, in part, by executing an application program (“BlueAware”) on the Requester Device and participating Identified Devices. Eagle, [0028]-[0029]. Accordingly, when the server provides the further information regarding devices participating in Eagle’s system (*e.g.*, providing profile information in an alert or identifying a device in blacklists or friend lists), that information *relates to a nearby user of an application on another device, in common with an application on the mobile device* (relates to users/devices of participants in Eagle’s social networking system, which requires installing the BlueAware application). Lanning, ¶¶254-255.

i. Baseball application

Eagle-Olkkonen additionally teaches that *the further information* (*e.g.*, the received alert information) *relates to a nearby user of an application on another device* (*e.g.*, relates to the user of the Identified Device, who is participating in a

network baseball game), *in common with an application on the mobile device (e.g., the Requester Device also has the network baseball game).*

As discussed for claims 14 and 19, Eagle teaches receiving an alert of profile information about an Identified Device and its owner. This information *relates to a nearby user* because the Identified Device and its owner are near the Requester Device (*e.g., in Bluetooth proximity*). Lanning, ¶¶256-258.

Eagle-Olkkonen further teaches that the user of the Identified Device is a *user of an application on another device, such as a multiuser game (e.g., a participant in a collaborative baseball game program).*

As discussed above (§VI.D.3), it would have been obvious to a POSITA that users using Eagle's system in collaborative settings would have been participating in a variety of activities, including ongoing multiuser games installed on user devices, as taught by Olkkonen. *See also* Olkkonen, 11:29-30 (joining a game "being played"), 15:10-13, 15:31-42, 19:51-20:25 and 24:48-61 (describing program modules for a "network baseball application program... in [the Bluetooth device]"). Additionally, since the Requester Device may have previously been a participant in a network baseball game (*see* Olkkonen, 1:46-61, 2:51-65 (a Requester Device may join/leave existing networks and activities)), it would have been obvious to a POSITA that the Requester Device also stores the same network

baseball application program, and so the Identified Device's application is *in common with an application on the mobile device*. Lanning, ¶¶259-263.

17. Claim 23: “[Claim 22] wherein the application is a multiuser game.”

See claim 22 (baseball application).

18. Claims 25/27: “[Claim 9, wherein the step of determining that an entity or object is within proximity further comprises:][Claim 1, wherein... the one or more processors further execute the instructions... for determining that an entity or object is within proximity by further:] comparing the identifier related information with the unique identifier or information derived from the unique identifier.”

As discussed for claim 4, Eagle-Behrens teaches *determining* that an Identified Device *is in proximity* based on blacklists and friend lists. *See also* [1.G]. Eagle-Behrens further teaches this limitation.

For example, to use blacklists and friend lists, the Requester Device checks whether UIDs received from Identified Devices are present on those blacklists and friend lists. *See* discussion of [1.G]. Accordingly, the *determining* is performed by *comparing the identifier related information with the unique identifier or information derived from the unique identifier* (e.g., comparing UIDs against UIDs on the blacklist/friend list). *See also* discussion of claim 4. Lanning, ¶¶266-268.

VII. GROUND 2: EAGLE IN VIEW OF BEHRENS, OLKKONEN, AND PERTTILA RENDERS OBVIOUS CLAIM 17

Eagle-Behrens-Olkkonen renders obvious claim 17. *See* §VI.E.13. To the extent PO argues that Eagle’s contact information is not an *access code*, Perttila renders obvious the use of access codes.

Eagle provides a framework for social introductions and suggests various commercial uses (*e.g.*, taxi/transportation services, publicizing products, Eagle, [0061]-[0063]) but leaves to the POSITA further transactional details regarding, *e.g.*, how merchants would have actually provided products to users and how users would have accessed those products. Lanning, ¶278.

Perttila is in the same field of wireless communications and reasonably pertinent to objectives of facilitating the exchange of information and validating commercial transactions. EX1001, 2: 8-24; Perttila, Abstract, [0001], [0006]-[0008], [0016], [0026], [0042]-[0043].¹² Lanning, ¶279.

Perttila teaches a method for wirelessly providing users access to services and products in a secure way through electronic coupon redemptions. Perttila,

¹² Related patents’ claims were previously found unpatentable over Perttila.

Arguments that Perttila is not analogous or does not teach features already decided by the PTAB/CAFC are estopped. EX1018-EX1023 (IPR petitions, FWDs), EX1034 (CAFC opinion).

Abstract, [0008]. For example, a user's Bluetooth device detects a Bluetooth beacon inside a store, notifies a server that it detected that beacon, and in return receives an electronic coupon for redemption inside that store. Perttila, [0011], [0028], [0037]-[0039]; EX1019, 13-14; EX1034, 6-7. The coupon may be a ticket to purchase or receive a "merchant offering," redeemed electronically by transferring and validating coupon information with the server. Perttila, [0005], [0041], claims 17, 26. Through validation, used/expired coupons may be rejected, providing merchants control over offerings. Perttila, [0043]; *see* [0006] (describing coupons with time/location limitations). Lanning, ¶280.

A POSITA applying Eagle's proximity-aware system for commercial purposes would have been motivated to look towards known e-commerce solutions for implementation, and it would have been obvious to modify Eagle's server to alert the Requester Device of nearby offerings with an *access code* (coupon data including an "e-coupon ID" or "electronic data set") that is *utilized to gain access* to offerings *in proximity to the mobile device*, as taught by Perttila, to advantageously "ensure that the user has rights" to offerings—permitting merchants to control their offerings. Perttila, [0005]-[0015], [0043]. Moreover, the modification would have been no more than the application of a known technique (Perttila's e-coupon access codes) to a known device ready for improvement (Eagle's system that identifies nearby resources and facilitates interactions) to

yield predictable results (controlling access to those resources) with a reasonable expectation of success (techniques for transferring and analyzing data were within the skill of a POSITA). *KSR*, 550 at 417-418. Lanning, ¶¶281-282.

VIII. GROUND 3: EAGLE IN VIEW OF BEHRENS, OLKKONEN, AND JONES RENDERS OBVIOUS CLAIM 29

Eagle-Behrens-Olkkonen renders obvious claim 9. *See* §VI.E.6.

Claim 29 adds: “proximity beacon transmissions are received... without requiring the mobile device to first perform a step of transmitting to the one or more beacon transmitter devices from which the plurality of proximity beacon transmissions are received.”

To the extent PO argues that Eagle teaches an active discovery method (*see* [1.E] above) but does not teach receiving beacon transmissions *without requiring the mobile device to first perform a step of transmitting*, Jones renders obvious this alternative method for discovery.

Jones, in the same field of endeavor of wireless communications and reasonably pertinent to objectives of facilitating the exchange of information between entities and devices (Jones, [0001], [0023]-[0026] (describing difficulties in discovering and connecting with nearby wireless services)), teaches different techniques for discovering nearby short-range wireless services. For example, a wireless device “passively discover[s] services by listening to advertised service messages provided by other local [Bluetooth] devices.” Jones, [0027].

Accordingly, devices providing services (*e.g.*, printing, games) broadcast advertising messages with service information “without prompting by a request message” from a user device. Jones, [0023]-[0025], [0034]. Lanning, ¶285.

A POSITA would have recognized power consumption/conservation as a universal design consideration, especially important for battery-powered mobile devices. Eagle recognized the trade-off between scanning to “provide a rich depiction” of the user’s environment and its effect on battery-life. Eagle, [0026]. A POSITA would have been motivated to find more power-efficient alternatives to Eagle’s active discovery method, and Jones provides an explicit, well-known alternative to Eagle’s exact problem by teaching a “passive” discovery method. By simply listening for broadcasted service advertisements (broadcast repeatedly or periodically; Jones [0034]), Eagle’s Requester Device would not have to transmit any discovery requests and would have saved time and energy as a result. Jones’ passive configuration is one of a finite number of identified, predictable solutions (active, passive, or mixed; Jones [0027], [0043]-[0045]) yielding predictable results (conserving power through passive listening), and a POSITA would have had a reasonable expectation of success listening for service messages, a function Eagle’s system already performs, without sending a request first. Lanning, ¶¶288-289.

Petitioner reserves the right to respond to any Patent Owner discretionary denial arguments in opposition briefing under the March 26, 2025 Memorandum concerning Interim Processes for PTAB Workload Management.¹³

IX. CONCLUSION

The Board should institute review and cancel the Challenged Claims.

Respectfully submitted,
Google LLC

Dated: July 2, 2025 By: /Scott A. McKeown/
Scott A. McKeown, Reg. No. 42,866
WOLF, GREENFIELD & SACKS, P.C.

¹³ <https://www.uspto.gov/sites/default/files/documents/InterimProcesses-PTABWorkloadMgmt-20250326.pdf>

1. APPENDIX A: U.S. PATENT NO. 11,334,918 CLAIM LISTING

Claim 1
[1.PRE] A mobile wireless device comprising:
[1.A] a first radio; a second radio;
[1.B] one or more processors; 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:
[1.D] receiving, using the first radio, identifier related information associated with a proximity beacon service, from one or more servers;
[1.E] receiving, using the second radio, a plurality of short range transmissions, including a plurality of proximity beacon transmissions when the device is located within a detection range of one or more beacon transmitter devices associated with the proximity beacon service, each of the proximity beacon transmissions including a respective MAC address, a respective unique identifier, and a Proximity Beacon Service Identifier (PBSI);
[1.F] determining if a particular short range transmission of the plurality of short range transmissions a) includes a MAC address, and b) includes the proximity beacon service identifier (PBSI) and if c) the PBSI indicates the particular short range transmission is a proximity beacon transmission associated with the proximity beacon service;
[1.G] then: determining if an entity or object associated with the proximity beacon service is in proximity to the mobile wireless device, by utilizing the identifier related information and the unique identifier.
Claim 2
The mobile wireless device of claim 1, wherein the MAC address is a randomly generated 48 bit number matching a format of a Bluetooth BD_ADDR.
Claim 3
[3.PRE] The mobile wireless device of claim 1 wherein the one or more processors further execute the instructions to perform operations including:
[3.A] receiving, by the second radio, a first proximity beacon transmission including a first MAC address and a first unique identifier at a first time; and
[3.B] receiving, by the second radio, a second proximity beacon transmission including a second MAC address and a second unique identifier at a second time, the second MAC address being different from the first MAC address and the second unique identifier being different from the first unique identifier; and

[3.C] associating the first and second unique identifier with a single beacon transmitter device.
Claim 4
The mobile wireless device of claim 1, wherein the one or more processors further execute the instructions to perform operations including: further determining that at least one beacon transmitter device associated with the proximity beacon service is in proximity to the mobile wireless device, by utilizing an action function including one or more previously downloaded unique identifiers.
Claim 8
The mobile wireless device of claim 1 wherein the one or more processors further execute the instructions to perform operations including:
receiving, via a second radio, the plurality of proximity beacon transmissions further includes receiving a first unique identifier at a first time that is different from a second unique identifier received at a second time; and
associating the first and second unique identifier with a single beacon transmitter device.
Claim 9
[9.PRE] A method for facilitating use of proximity beacons, the method executing within a mobile device, and the method comprising:
[9.A] communicating between the mobile device and one or more servers and receiving, at the mobile device, identifier related information, using a first radio;
[9.B] receiving, at the mobile device using a second radio, a plurality of short range transmissions, including a plurality of proximity beacon transmissions from one or more beacon transmitter devices associated with a proximity beacon service, each of the proximity beacon transmissions including a respective MAC address, a respective unique identifier (UID), and a Proximity Beacon Service Identifier (PBSI);
[9.C] a) determining that a particular short range transmission of the plurality of short range transmissions includes a MAC address,
[9.D] b) determining that the Proximity Beacon Service Identifier (PBSI) is present, and c) determining that the PBSI indicates the particular short range transmission is a proximity beacon transmission associated with the proximity beacon service; and
[9.E] when the three determining steps a) b) and c) are each true, then d) determining that an entity or object associated with the proximity beacon service is within proximity to the mobile device, by utilizing the identifier related information and the unique identifier.
Claim 10

[10.PRE] The method of claim 9,
[10.A] wherein a first one of the plurality of proximity beacon transmissions received at a first time includes a first unique identifier, and wherein a second one of the plurality of proximity beacon transmissions received at a second time includes a second unique identifier the second unique identifier being different from the first unique identifier; and
[10.B] associating both the first unique identifier and the second unique identifier with a particular entity or object in proximity to the mobile device.
Claim 11
The method of claim 9 wherein the MAC address is selected from a group consisting of (a) a randomly generated 48 bit number matching a format of a MAC address and (b) a Bluetooth BD ADDR.
Claim 12
[12.PRE] The method of claim 9
[12.A] wherein a first one of the plurality of proximity beacon transmissions is received at a first time and includes a first unique identifier and first MAC address, and the Proximity Beacon Service Identifier (PBSI); and
[12.B] wherein a second one of the plurality of proximity beacon transmissions received at a second time includes a second unique identifier different from the first unique identifier and a second MAC address different from the first MAC address, and the Proximity Beacon Service Identifier; and
[12.C] associating both the first unique identifier and the second unique identifier with the same entity or object in proximity to the mobile device.
Claim 13
The method of claim 9, further comprising preventing the sending of the unique identifier, using the first radio, to the one or more servers, based upon previous detections of the respective unique identifier associated with the proximity beacon transmission.
Claim 14
The mobile wireless device of claim 1, wherein the instructions further comprise: sending the unique identifier, using the first radio, to at least one server of the one or more servers, and receiving further information relating to an object or entity associated with being within proximity to the mobile device.
Claim 15
The mobile wireless device of claim 1, wherein the instructions further comprise: preventing the sending of the unique identifier, using the first radio, to the one or more servers, based upon previous detections of the respective unique identifier associated with the proximity beacon transmission.

Claim 16
The mobile wireless device of claim 1, wherein the instructions further comprise: controlling further communications between the mobile device and at least one device or server associated with an entity or object in proximity to the mobile device.
Claim 17
The method of claim 9, further comprising: receiving, using the first radio, access code information by the mobile device from at least one of the servers; and utilizing the access code information to gain access to the entity or object determined to be in proximity to the mobile device.
Claim 18
The method of claim 9, wherein receiving the identifier related information, using the first radio, is performed in response to sending at least the unique identifier to at least one of the one or more servers using the first radio.
Claim 19
The method of claim 9, additionally comprising: sending the unique identifier, using the first radio, to at least one server of the one or more servers, and receiving further information relating to an object or entity associated with being within proximity to the mobile device.
Claim 20
The method of claim 19, wherein the further information relates to one or more of the following: a loyalty program; a payment service; or a coupon relating to an entity in proximity to the mobile device; or advertising content.
Claim 22
The method of claim 19, wherein the further information relates to a nearby user of an application on another device, in common with an application on the mobile device.
Claim 23
The method of claim 22, wherein the application is a multiuser game.
Claim 24
The method of claim 9, additionally comprising: controlling further communications between the mobile device and at least one device or server associated with an entity or object in proximity to the mobile device.

Claim 25
The method of claim 9, wherein the step of determining that an entity or object is within proximity further comprises: comparing the identifier related information with the unique identifier or information derived from the unique identifier.
Claim 27
The mobile wireless device of claim 1, wherein the one or more processors further execute the instructions to perform the operations for determining that an entity or object is within proximity by further: comparing the identifier related information with the unique identifier or information derived from the unique identifier.
Claim 28
The mobile wireless device of claim 1, wherein the receiving of the identifier related information, using the first radio, is performed in response to the one or more processors executing instructions for: sending at least the unique identifier to at least one of the one or more servers using the first radio.
Claim 29
The method of claim 9, wherein the proximity beacon transmissions are received, at the mobile device, without requiring the mobile device to first perform a step of transmitting to the one or more beacon transmitter devices from which the plurality of proximity beacon transmissions are received.
Claim 31
[31.PRE] The mobile wireless device of claim 3 wherein the one or more processors further execute the instructions to perform operations including:
[31.A] receiving, via a second radio, the plurality of proximity beacon transmissions further includes receiving a first unique identifier at a first time that is different from a second unique identifier received at a second time; and
[31.B] associating the first and second unique identifier with a single beacon transmitter device.

CERTIFICATE OF SERVICE UNDER 37 C.F.R. §42.6(E)(4)

I certify that on July 2, 2025, a copy of the foregoing document, including any exhibits or appendices filed therewith, is being served via *Priority Mail Express* at the following correspondence address of record for the patent:

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

A courtesy copy was also sent via electronic mail to Patent Owner's counsel of record in IPR2025-01049 at the following addresses:

Brent Bumgardner	brent@nelbum.com
Charles Austin Ginnings	austin@nelbum.com
Christopher G. Granaghan	chris@nelbum.com
Timothy E. Grochocinski	tim@nelbum.com
Taryn N. Trusty	taryn@nelbum.com

Date: July 2, 2025

/MacAulay Rush/
MacAulay Rush
Paralegal
WOLF, GREENFIELD & SACKS, P.C.

CERTIFICATE OF WORD COUNT

Pursuant to 37 C.F.R. §42.24, the undersigned certifies that the foregoing Petition for *Inter Partes* Review contains 13,991 words excluding a table of contents, a table of authorities, Mandatory Notices under §42.8, a certificate of service or word count, or appendix of exhibits or claim listing. Petitioner has relied on the word count feature of the word processing system used to create this paper in making this certification.

Date: July 2, 2025

/MacAulay Rush/

MacAulay Rush

Paralegal

WOLF, GREENFIELD & SACKS, P.C.