

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. IPR2025-01183
Patent No. 11,687,971

**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.....	5
III.	UNPATENTABILITY GROUNDS.....	6
IV.	'971 PATENT.....	6
	A. Background.....	6
	B. Prosecution History	8
	C. POSITA	9
V.	CLAIM INTERPRETATION	9
VI.	GROUND 1: EAGLE IN VIEW OF BEHRENS AND OLKKONEN RENDERS OBVIOUS THE CHALLENGED CLAIMS	9
	A. Eagle (EX1005)	9
	B. Behrens (EX1006)	11
	C. Olkkonen (EX1007)	12
	D. Eagle in view of Behrens, in further view of Olkkonen.....	13
	1. Receiving different identifying information from the same device.....	16
	2. Filtering beacon service identifiers	19
	3. Actions.....	26
	E. Mapping to Challenged Claims	29
	1. Claim 1	29
	a. [1.PRE] “A method comprising:”	29
	b. [1.A.I] “receiving, at a wireless device, via a short range wireless protocol, a first plurality of beacon transmissions, each beacon transmission comprising three fields”	30
	c. [1.A.II] “(a) a MAC address,”	33
	d. [1.A.III] “(b) a unique identifier, wherein the unique identifier of each respective beacon transmission does not directly identify a location of a beacon transmitter, and”	34

e.	[1.A.IV] “(c) a beacon service identifier, wherein the beacon service identifier of each respective beacon transmission identifies that the unique identifier is relevant to stored information associated with a wireless beacon service,”	36
f.	[1.A.V] “wherein the stored information is not otherwise accessible to the wireless device utilizing the short range wireless protocol;”	38
g.	[1.B.I] “receiving, at the wireless device via a second wireless protocol, the stored information from one or more servers,”	39
h.	[1.B.II] “the stored information relating to a particular entity or object associated with a first unique identifier, and”	40
i.	[1.B.III] “wherein the second wireless protocol is different from the short range wireless protocol;”	41
j.	[1.C] “causing selection of one or more of the unique identifiers from the first plurality of beacon transmissions, by filtering the beacon transmissions which include a particular beacon service identifier indicating that a particular received beacon transmission is associated with a particular wireless beacon service; and”	41
k.	[1.D] “taking first further action relating to the stored information, if the first unique identifier is present among the selected one or more unique identifiers.”	42
2.	Claim 2	43
a.	[2.PRE] “The method of claim 1, wherein the receiving, at the wireless device, via a short range wireless protocol, of the first plurality of beacon transmissions occurs in a first time period, and”	43
b.	[2.A] “wherein the method further comprises, during a second time period:”	44
c.	[2.B.I] “receiving, at the wireless device, via a short range wireless protocol, a second plurality of beacon transmissions, each of the second plurality of beacon transmissions comprising three fields”	45

d.	[2.B.II] “(a) a MAC address,”	45
e.	[2.B.III] “(b) a unique identifier, wherein the unique identifier of each respective beacon transmission does not directly identify a location of a beacon transmitter, and”	46
f.	[2.B.IV] “(c) a beacon service identifier, wherein the beacon service identifier of each respective beacon transmission identifies that the unique identifier is relevant to stored information associated with a wireless beacon service,”	46
g.	[2.B.V] “wherein the stored information is not accessible to the wireless device utilizing the short range wireless protocol;”	47
h.	[2.C] “causing selection of one or more of the unique identifiers from the second plurality of beacon transmissions, by filtering the beacon transmissions which include the same particular beacon service identifier indicating that the particular received beacon transmission is associated with the same particular wireless beacon service; and”	47
i.	[2.D.I] “taking second further action relating to the stored information, if a second unique identifier is present among the one or more unique identifiers selected from the second plurality of beacon transmissions,”	48
j.	[2.D.II] “wherein the first unique identifier and the second unique identifier are both associated with the same particular entity or object, and wherein the second unique identifier is not equal to the first unique identifier, and further wherein the received beacon transmissions including the first and second unique identifiers are received from a same transmitting device.”	48
3.	Claim 3	49
a.	[3.A] “The method of claim 2 wherein the MAC address received in a beacon transmission including the second unique identifier is different from the MAC address received in a beacon transmission including the first unique identifier, but each such beacon transmission includes the same particular beacon service identifier, and”	49

- b. [3.B] “wherein a plurality of beacon transmissions including the particular service identifier and the first unique identifier are received in the first time period, and no beacon transmissions including the same particular service identifier and the second unique identifier are received in the first time period.” 51
- 4. Claims 4/40/53: “[Claim 3][Claim 37][Claim 53] wherein the second further action is based upon a function currently being performed on a device associated with the wireless beacon service.” 52
- 5. Claims 5/41/54: “[Claim 4][Claim 40][Claim 53] wherein the function is related to a current phone call, music being played, a video being played, a multi-player game, or a shared application.” 54
- 6. Claims 6/29/55/56: “[Claim 2][Claim 1][Claim 51][Claim 50] wherein the first [or the second] further action is [additionally] related to receiving advertising information for presentation to a user of the wireless device, based upon the first [or the second] unique [identifier][identifiers], or [based upon] information derived from the first [or second] unique identifier.” 55
- 7. Claims 7/30/42/57/58: “[Claim 2][Claim 1][Claim 37][Claim 51][Claim 52] wherein [one or more of] the first [and the second] further action [additionally] includes [receiving][causing the wireless device to receive] content from a server based upon information derived from [either] the first unique identifier [or the second unique identifier].” 56
- 8. Claims 8/43/59: “[Claim 2][Claim 37][Claim 51], wherein the first or second further action [additionally] includes [sending a message][or causing a server to send a message][causing the wireless device to send a message] to another device associated with an account related to the first and the second unique identifiers[, or information derived from the first or the second unique identifiers].” 57
- 9. Claims 10/44/62: “[Claim 2][Claim 37][Claim 51] wherein the second further action [additionally] includes [preventing][causing the wireless device to prevent] sending [of] the second unique identifier or information derived from

the second unique identifier by the [mobile] wireless device to at least one of the one or more servers.”	58
10. Claims 12/64: “[Claim 1][Claim 50] wherein the [taking] first further action [further][additionally] includes causing the wireless device[,] to: send the first unique identifier or information derived from the first unique identifier to at least one of the one or more servers, and [subsequently] receive the stored information in response.”	59
11. Claims 13/14/65/66: “[Claim 1][Claim 2][Claim 50][Claim 51] wherein the [computer program instructions, when executed by the one or more processors in the wireless device, further cause the wireless device to[:] receive] stored information [is received] at the wireless device from at least one of the one or more servers prior to [the taking of the first][performing one or more of the first and the second][performing the first][performing one or more of the first and the second] further action.”	59
12. Claims 15/36/46/67/80: “[Claim 1 further comprising][Claim 37 wherein the operations further comprise][Claim 50 wherein the computer program instructions... further cause the wireless device to][Claim 50 further comprising program instructions that... cause the wireless device to]: [using][use] the stored information to determine if the first unique identifier is present among the [first] selected one or more unique identifiers [from the first plurality of beacon transmissions].”	60
13. Claims 16/68: “[Claim 2][Claim 51] wherein all beacon transmitter devices participating in the particular wireless beacon service have the same particular beacon service identifier.”	61
14. Claim 18: “[Claim 2] wherein the steps performed at the wireless device are performed as a result of an application program executing on the wireless device.”	62
15. Claims 19/34/72: “[Claim 2][Claim 1][Claim 51] wherein the [second][first] further action is [additionally] related to either a product tied to a location or an advertisement tied to a location.”	62

16. Claims 22/48/75: “[Claim 2][Claim 37][Claim 51] wherein the second further action [additionally] includes [allowing][causing the wireless device to allow] a user associated with the [mobile] wireless device to [be provided] access to an object or device associated with the wireless beacon service.”	63
17. Claims 23/35/49/76: “[Claim 2][Claim 3][Claim 37][Claim 51] wherein the [taking][first or] second further action additionally [comprises: controlling][includes causing the wireless device to control] further communications between the [mobile] wireless device and at least one [other] device or server associated with an entity or object in proximity to the wireless device [based upon information derived from the first or second unique identifier].”	64
18. Claims 26/38/79: “[Claim 2 further comprising][Claim 37 wherein the operations further comprise][Claim 51 wherein the computer program instructions, when executed by the wireless device, further cause the wireless device to]: [using][use] the stored information to determine if the second unique identifier is present among the selected one or more of the unique identifiers from the second plurality of beacon transmissions.”	66
19. Claims 27/39/81: “[Claim 1][Claim 37][Claim 50] wherein [the][each] MAC address is a randomly generated 48 bit number matching a format of a Bluetooth BD_ADDR.”	66
20. Claim 28: “[Claim 3] wherein the short range protocol is derived from Bluetooth.”	66
21. Claim 37	67
a. [37.PRE] “A mobile wireless device comprising:”	67
b. [37.A] “one or more radios for providing reception and transmission for each of a Bluetooth wireless protocol and a second wireless protocol;	67
c. [37.B] “one or more processors; and”	68
d. [37.C] “one or more memory devices coupled to the one or more processors, the one or more memory devices storing a set of instructions that when executed by the one or more processors cause the one or more processors to perform operations including:”	68

e.	[37.D] “receiving from a beacon transmitter... a first plurality of beacon transmissions during a first time period...”	69
f.	[37.E] “receiving... stored information...;”	69
g.	[37.F] “selecting one or more unique identifiers... by filtering the beacon transmissions...;”	69
h.	[37.G] “taking first further action... if the first unique identifier is present...;”	69
i.	[37.H] “receiving, during a second time period, a second plurality of beacon transmissions...;”	69
j.	[37.I] “selecting one or more of the unique identifiers... by filtering the beacon transmissions...;”	69
k.	[37.J] “taking second further action... if a second unique identifier is present..., wherein the second unique identifier is associated with the same entity or object, and wherein the second unique identifier is not equal to the first unique identifier, and further wherein the received beacon transmissions including the first and second unique identifiers are received from a same transmitting device; and”	70
l.	[37.K] “wherein the [second beacon transmission] MAC address... is different from the [first beacon transmission] MAC address..., but each... includes the same particular beacon service identifier.”	70
22.	Claim 50	70
a.	[50.PRE] “A computer program product for installation in a non-volatile memory in a wireless device, the computer program product comprising computer program instructions that, when read from the non-volatile memory, and then executed by one or more processors in the wireless device, cause the wireless device to:”	70
b.	[50.A] “process a first plurality of beacon transmissions..., each beacon transmission comprising three fields...;”	71
c.	[50.B] “process stored information...;”	71

d.	[50.C] “select one or more of the unique identifiers... by filtering the beacon transmissions...; and”	71
e.	[50.D] “perform a first further action... if the first unique identifier is present...”	71
23.	Claim 51	72
a.	[51.PRE] “[Claim 50] wherein the computer program instructions, when executed by the one or more processors in the wireless device, cause the wireless device to:”	72
b.	[51.A] “during a first time period: process the first plurality of beacon transmissions..., and”	72
c.	[51.B] “during a second time period:”	72
d.	[51.C] “process a second plurality of beacon transmissions..., each beacon transmission comprising three fields...”	72
e.	[51.D] “select one or more of the unique identifiers... by filtering the beacon transmissions which include the same particular beacon service identifier...; and”	72
f.	[51.E] “perform a second further action... if a second unique identifier is present...”	73
24.	Claim 52: “[Claim 51] wherein the [first and second beacon transmission] MAC address [are different], but each... includes the same particular beacon service identifier, and... no beacon transmissions including the same service identifier and the second unique identifier are received in the first time period.”	73
VII.	CONCLUSION	74
1.	APPENDIX A: U.S. PATENT NO. 11,687,971 CLAIM LISTING	75

TABLE OF AUTHORITIES

CASES

<i>KSR Int’l v. Teleflex</i> , 550 U.S. 398 (2007)	18, 25, 28, 61
<i>Ohio Willow Wood Co. v. Alps South, LLC</i> , 735 F.3d 1333 (Fed. Cir. 2013)	5

OTHER AUTHORITIES

MPEP §2111.05	55
---------------------	----

EXHIBIT LIST

Exhibit	Description
1001	U.S. Patent No. 11,687,971
1002	Prosecution History of U.S. Patent No. 11,687,971
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_ios31_user_guide.pdf)

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. 11,687,971 issued from application no. 17/942,197, filed 2022-09-12, and claims priority to the following applications:

Application No.	Filing Date
17/366,826	2021-07-02
16/817,896	2020-03-13
15/271,410	2016-09-21
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

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.

The following patent applications claim priority to U.S. Patent No.

11,687,971 and application no. 17/942,197:

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

U.S. Patent No. 11,687,971 is the subject of *Samsung Electronics Co., Ltd. v. Secure Communication Technologies, LLC*, IPR2025-01051, 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 11,344,918 (application 15/217,410) 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 1-8, 10, 12-16, 18-19, 22-23, 26-30, 34-44, 46, 48-59, 62, 64-68, 72, 75-76, and 79-81 (“Challenged Claims”) of U.S. Patent No. 11,687,971 (EX1001, the “’971”).

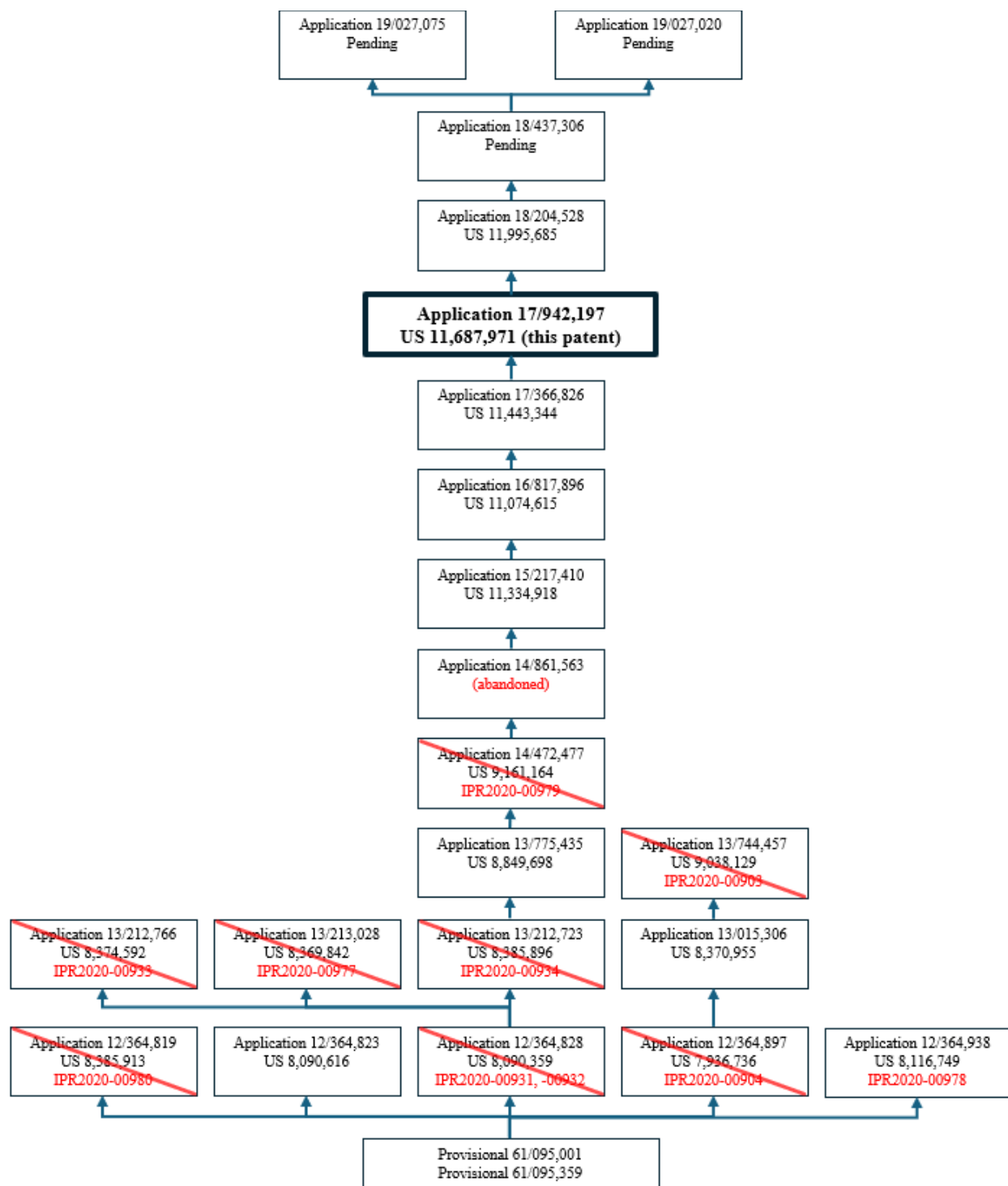
I. INTRODUCTION

The ’971 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, 1:5-24, 1:49-2:63. 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, 1:49-2:4, 5:25-34, 5:57-67. 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, 2:5-14, 6:7-14, 6:41-59, 6:60-7:8.

This architecture of exchanging information between nearby devices and servers was claimed in earlier patents within the ’971’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 (Petitions and Decisions in those IPRs). Unpatentability was further confirmed in the only two IPR proceedings appealed to the CAFC (from IPR2020-00931 and IPR2020-00933). *See* EX1034.

² IPR2020-00978 was denied institution for reasons/limitations not relevant to the '971 claims. EX1029, 15-18.



The '971 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 from another wireless device over a “local wireless link,” and transmitting information back to the wireless device based on a policy); EX1031, 46-49 (PTAB acknowledging that Behrens teaches using “a combination of UIDs” and that users may “exercise control over which or how many UIDs are transmitted”).

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.

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

II. STANDING CERTIFICATION

Petitioner certifies that the ’971 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 in view of Behrens and Olkkonen	1-8, 10, 12-16, 18-19, 22-23, 26-30, 34-44, 46, 48-59, 62, 64-68, 72, 75-76, 79-81	§103

The '971'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

The Declaration of Mark Lanning (EX1003, ¶¶1-302; "Lanning") describes the prior art's scope and content at the time of the '971.

IV. '971 PATENT⁵

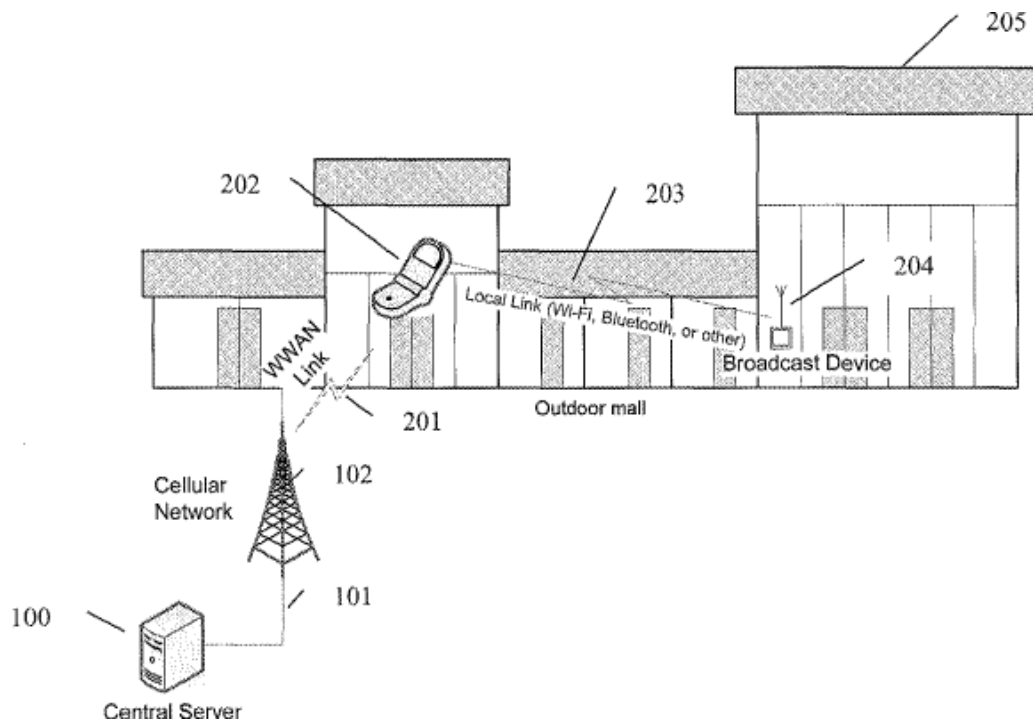
A. Background

The '971 is directed to the exchange of information between two wireless devices using short-range communications (*e.g.*, Bluetooth/WiFi), with the aid of a

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

remote server using long-range communications (*e.g.*, cellular). EX1001, 1:5-24, 1:49-2:63.

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, 5:25-34.



Device 204 is a device 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 the server 100 recognizes the identifying information as being associated with device 204. EX1001, 5:30-46. The server uses stored account settings or policy information to determine “what information and under which situations information may be disclosed to another

device or user” to facilitate further short-range communications. EX1001, 6:60-7:2, 13:53-64, 18:42-60.

The ’971 explains that devices in short-range proximity identify themselves with beacon transmissions including a MAC address, unique identifier, and beacon service identifier. EX1001, 2:15-20, 2:35-45, 7:35-40, 8:35-48. 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, 8:12-54; *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, ¶¶38-67.

B. Prosecution History

The Examiner’s first action allowed several dependent claims but rejected other claims for double patenting or under §101. EX1002, 127-140. Applicant submitted a terminal disclaimer and claim amendments in response. EX1002, 349-373.

The Examiner allowed the pending claims and repeated, as allowable subject matter, elements of the claimed beacon service identifier and stored information “in combination with the other limitations in the independent claims.” EX1002, 511-513. Lanning, ¶68.

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, ¶¶70-72.

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). No constructions are required because the claims are unpatentable under any reasonable construction as detailed below.

VI. GROUND 1: EAGLE IN VIEW OF BEHRENS AND OLKKONEN RENDERS OBVIOUS THE CHALLENGED CLAIMS

A. Eagle (EX1005)

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].

⁶ This same level was adopted in prior proceedings in the ’971 patent family and is now fixed by operation of estoppel. *See, e.g.*, EX1019, 8-9.

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).

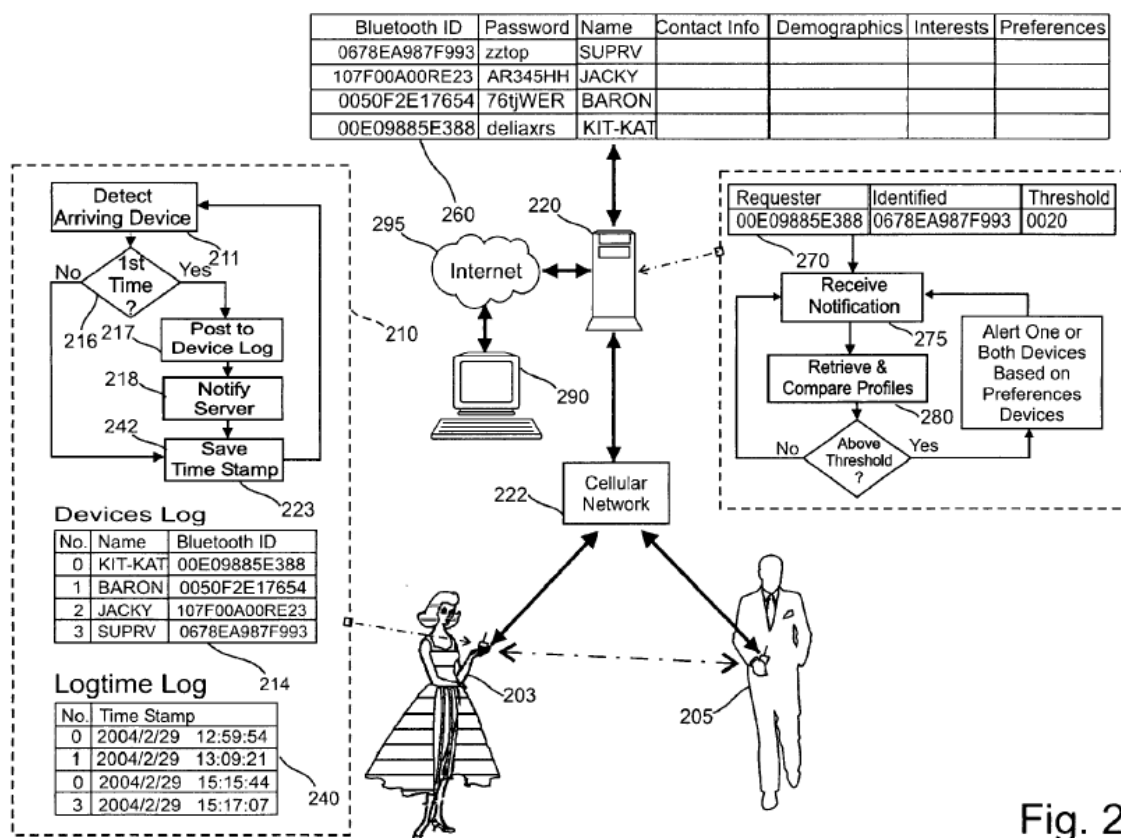


Fig. 2

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 (because, *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, ¶¶80-83.

B. Behrens (EX1006)

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].

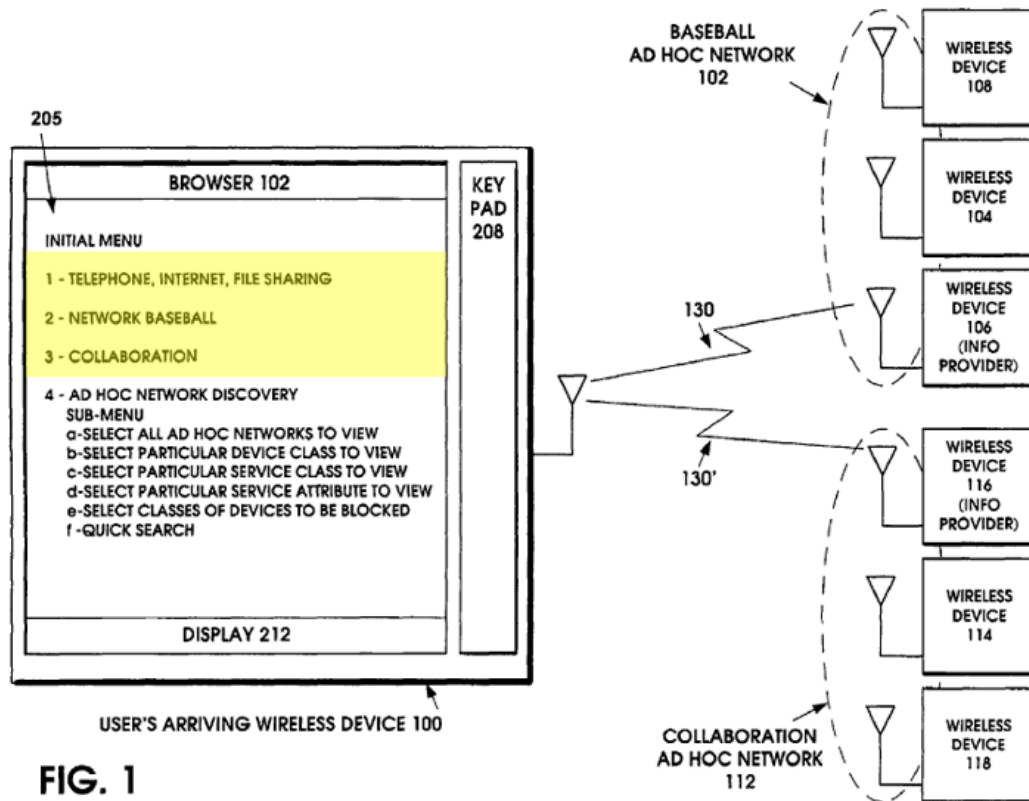
UIDs may be used in combination, and a "user may... exercise control over which or how many UIDs are transmitted by his device." Behrens, [0061], [0103], [0115], [0122]. Accordingly, a user has "multiple or changing UIDs." Behrens, [0061], [0115]. Lanning, ¶¶84-87.

C. Olkkonen (EX1007)

Olkkonen is directed to short-range wireless systems and connecting users for common purposes via ad hoc networking (*e.g.* a “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, ¶¶88-91.

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

The '971 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, 1:37-45, 1:49-51. Lanning, ¶92.

Eagle, Behrens, and Olkkonen are each analogous to the '971, 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 use a server that facilitates communications), [0008] (avoiding privacy problems); Behrens, [0001], [0136] (establishing contact between otherwise 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, ¶93.

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

⁷ Eagle and Behrens were previously asserted in related patent family IPRs that have reached final judgement (as discussed above). Any argument that Eagle or Behrens are not analogous art is therefore 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).

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 fields of information in short-range messages used to establish connections, the filtering of unique identifiers, or taking certain actions with respect to detected devices, such obvious variations would have been obvious to a POSITA in view of Behrens and Olkkonen. Lanning, ¶94.

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 and/or allow a user's phone to filter out irrelevant services like printing or devices like headsets. 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 stored information (*e.g.*, user profile information) to facilitate connections between wireless devices and potential further action, such as displaying contact information or joining a collaborative game, as taught by Olkkonen. Lanning, ¶95.

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 ’971 require receiving, at a wireless device from a *same transmitting device*, different beacon transmissions in two different time periods, 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, 37, 50-51. In other words, the claimed system changes its identifying data as a function of time to enhance security. EX1001, 7:66-8:11, 15:14-40, 18:35-41. Lanning, ¶96

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, ¶97

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 UUIDs” and has “control over which or how many UUIDs are transmitted by his device.” Behrens, [0103], [0115]. Lanning, ¶¶98-99. Behrens explains that the use of changing UUIDs 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, ¶¶100-103.

Additionally, a POSITA would have recognized that Behrens’ teaching of changing UUIDs 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, ¶104.

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 UIDs) 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 UIDs). *KSR Int’l v. Teleflex*, 550 U.S. 398, 417-418 (2007). Lanning, ¶105.

A POSITA would have also had a reasonable expectation of success in modifying Eagle with the teachings of Behrens. Use of UIDs (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, ¶106.

2. Filtering beacon service identifiers

The claims of the '971 require that beacon transmissions include a *beacon service identifier* that *identifies that the unique identifier is relevant to stored information associated with a wireless beacon service*. See, e.g., EX1001, claims 1-2, 37, 50-51. The same claims further require *filtering the beacon transmissions which include a particular beacon service identifier*. 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* as claimed, it would have been obvious to a POSITA to filter UUIDs based on beacon service identifiers (e.g., service class and/or device class information) received in inquiry responses, consistent with the teachings of Olkkonen, for the following reasons. Lanning, ¶¶107-108.

Eagle teaches that it is unnecessary for a Requester Device to notify the server of every UUID 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, ¶109.

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). As another example, both Eagle and Olkkonen teach that device class information is also received in Bluetooth inquiry responses and describes the type of the Identified Device (*e.g.*, a printer). Eagle, [0032] (class of device parameter received during discovery includes “device class” fields and a “service class” field); Olkkonen, 6:63-66. Discussed below, both service class and device class information would have been obvious criteria for filtering UIDs where some devices, such as printers, keyboards, etc., are not suited for use with a given application such as Eagle’s social introduction system. Lanning, ¶110.

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, ¶111.

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 devices in particular service classes or having particular service attributes (such as

⁸ While Olkkonen describes “advertisements” and “advertisement broadcaster” as classes of devices, a POSITA would have recognized that “advertisement” is not a standard type of Bluetooth device class. “Advertisement” is an intended use or service provided by the device, not a class of the device itself, and it would have been obvious to alternatively identify advertisement functions as custom service information. Lanning, ¶112.

those identifying a particular program, such as a “GAME PROGRAM”).

Olkkonen, 11:43-60. Lanning, ¶112.

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, ¶113.

Device class information (filtering for appropriate device class): As discussed above, Eagle describes that device class information is also received in inquiry responses. Eagle, [0032]. It would have been further obvious to a POSITA to filter UUIDs according to device classes so that notifications and alerts are tailored to specific desired uses within an application. Lanning, ¶114.

In particular, Eagle describes configuring its social introduction system for particular uses. For example, “companies interested in facilitating internal collaboration can use the invention to introduce people who are working on similar projects.” Eagle, [0065]. Other uses of the system include “meet[ing] people” and tracking “passengers” on a bus. Eagle, [0061], [0066]. Lanning, ¶115.

The same rationales discussed above for filtering based on service class information also apply to device classes—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. For example, where a company is implementing Eagle’s system to introduce “people,” it would have been obvious to filter UUIDs to device types that are associated with people, such as mobile phones that provide the additional benefit of enabling direct communications. Eagle, [0058] (alert message contains a phone number,

“[enabling] one user to simply call [the] nearby person’s cell phone”). In that same scenario, a Bluetooth-connected printer would be an example of a device to be filtered out as not being a device associated with “people.” Filtering functions based on device class preferences were well-known in the art. *See* Olkkonen, 11:33-60 (blocking the listing of printers and fax machines, or viewing all photocopier devices).⁹ Lanning, ¶116.

Therefore, it would have been obvious to modify Eagle’s Requester Device to filter inquiry responses so that only UIDs from devices in device classes relevant to particular implementations of Eagle’s social introduction service would be passed 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, ¶117.

Additionally: Eagle teaches that wireless device resources are limited. Eagle, [0024] (conserving memory by deleting old logs of Identified Devices), [0026]

⁹ Information identifying devices, *e.g.*, the printer and fax devices suggested by Olkkonen, are received within class of device information identifying the device’s type and capabilities. Eagle, [0032] (class of device parameters include device class and service class fields); EX1009, 1-2 (showing printing device and service classes). Lanning, ¶¶52-55.

(continuous scanning and logging expends phone battery life). By only contacting the server with useful UUIDs, 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, ¶118.

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, ¶119.

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 and class 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 and device 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, ¶120.

3. Actions

Several claims of the '971 require taking a first and/or second “action” relating to stored information. Claimed examples include actions related to: a function being performed on a device (claim 4), a multiplayer game (claim 5), receiving and presenting advertising information (claim 6), allowing a user access to an object or device (claim 22), controlling communications between devices (claim 23), and others. Lanning, ¶121.

Eagle also broadly describes that its social introduction system “enables a diverse suite of applications,” *e.g.*, connecting people working on similar projects, connecting users with like interests, as greeting beacons at trade shows, notifications of nearby resources, and more. 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, ¶122.

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, participating in network games, collaborative CAD designs, and more. 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, ¶123.

Behrens, like Eagle, teaches that when two wireless devices (and their users) detect each other in close proximity, further actions include receiving alerts from a server and connecting with the other device (Behrens, [0085], [0107]-[0110], [0139], [0158]-[0161]) or, alternatively, ignoring certain devices (Behrens, [0162]). Devices are ignored based on blacklist instructions received from a server. Behrens, [0026], [0101]-[0102], [0124]. Lanning, ¶124.

Accordingly, to the extent Eagle leaves to a POSITA what further actions to take, which relate to the variety of purposes for which two wireless devices may want to connect, it would have been obvious to perform various actions, as taught by Olkkonen or Behrens. Eagle's system provides a framework for detecting nearby devices but leaves to the POSITA what specific actions devices are to perform, which Olkkonen and Behrens disclose. The performance of any particular action taught by Olkkonen or Behrens would have been no more than a simple substitution of known elements (Olkkonen's and Behren's actions and

communications relate to Internet sharing, network baseball, CAD design, messaging, ignoring, etc.) for another (Eagle's exemplary actions related to social networking, greeting beacons, transportation, etc.) to obtain predictable results (facilitating the use of wireless devices in diverse ways). *KSR*, 550 at 417-418. Lanning, ¶125.

Furthermore, none of the wide variety of actions claimed in the '971 require more than ordinary skill. For example, joining ad hoc networks to take advantage of network resource, as taught by Olkkonen, would have been well within the skill of a POSITA, as Bluetooth ad hoc network functions were well-known as part of the Bluetooth standard, and the multitude of uses for wireless computing devices were also varied and well-known. Olkkonen, 1:20-3:14. Olkkonen specifically provides means for finding users (such as those that a user would have been alerted to in Eagle's system) and joining their networks. Olkkonen, Fig. 2B-2C, 15:64-16:64. Other claimed functions, such as sending and receiving data, or preventing communications based on received information, or presenting advertising information—spread amongst the many dependent claims—are basic or well-known computing actions that would have required no more than ordinary skill to take. Lanning, ¶126.

E. Mapping to Challenged Claims

Claims 1, 37, 50, and their dependent claims are directed to a “method,” “wireless device,” and “program product” but recite substantially similar limitations. Similar claims are discussed together below. Lanning, ¶¶127-294.

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 method comprising:”

To the extent this preamble is limiting, Eagle teaches *a method* for facilitating networking communications among multiple devices (*e.g.*, phones) and a server. Eagle, Abstract, [0003]-[0005]. 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, ¶127.

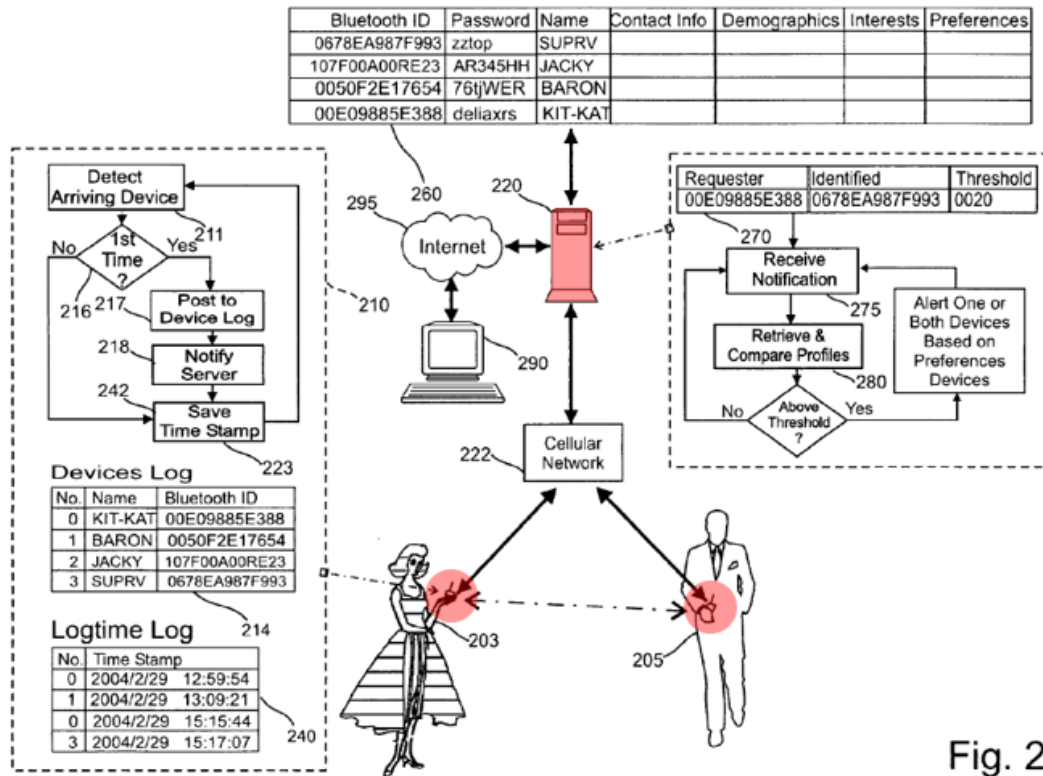


Fig. 2

- b. [1.A.I] “receiving, at a wireless device, via a short range wireless protocol, a first plurality of beacon transmissions, each beacon transmission comprising three fields”

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

Eagle-Behrens-Olkkonen teaches receiving, at a wireless device (e.g., receiving at a first Bluetooth phone), via a short range wireless protocol (e.g., via Bluetooth protocol), a first plurality of beacon transmissions (e.g., inquiry responses containing identifying information), each beacon transmission comprising three fields.

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].

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 *first plurality of beacon transmissions* from a plurality of Identified Devices. Lanning, ¶¶128-131.

The '971 does not provide express formatting details or examples regarding beacon transmission “fields.” See EX1001, 2:15-53 (beacon transmissions “comprise” or “include” a MAC address, unique identifier, and beacon service identifier). However, a POSITA would have recognized that the use of *fields* facilitates the recognition and interpretation of relevant information received in transmissions. Thus, to the extent Eagle does not explicitly describe every type of information communicated in a “field,” it would have been obvious to format beacon transmissions with fields so that the information conveyed by the Identified Device may be understood by the Requester Device. Lanning, ¶132; Olkkonen, 27:12-20 (inquiry response packet structure includes fields); EX1008, 283-285,

1259-1260, 1288, 1305-1310 (Bluetooth specification defines fields for address, class, service, and manufacturer information).

Discussed with respect to limitations [1.A.II]-[1.A.IV] below, Eagle-Behrens-Olkkonen teaches *each beacon transmission comprising three fields*.

c. [1.A.II] “(a) a MAC address,”

Eagle-Behrens discloses the beacon transmission including *a MAC address* in two separate ways.

i. MAC address in UUIDs

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

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

As discussed above (§VI.D.1), Behrens teaches that the Identified Device identifies itself to the Requester Device with a combination of UUIDs including, e.g., a 48-bit “Bluetooth Device Address” or BD_ADDR. Behrens, [0061], [0097], [0122]. The ’971 similarly acknowledges that a “MAC address” may be a “48 bit number matching a format of a Bluetooth BD_ADDR” (i.e., not requiring the actual device BD_ADDR) and that BD_ADDR addresses are a form of MAC address used in Bluetooth communications. EX1001, 2:57-59, 7:17-25.

Eagle-Behrens’s 48-bit BD_ADDR included as a UID identifying the Identified Device is therefore *a MAC address*. Lanning, ¶¶135-137.

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 MAC address* in its inquiry response. Eagle, [0033]-[0037] (describing a Bluetooth discovery process with devices sending inquiry messages and others providing inquiry responses); Olkkonen, 2:23-31 (“inquiry response is a message packet containing the responding device’s Bluetooth Device Address”), 27:12-20 (describing inquiry response FHS packet structure including sender’s a BD_ADDR); EX1008, 283 (describing the same).

The ’971 similarly acknowledges that a transmitting device’s MAC address is “always broadcast in any operation of a Bluetooth... link.” EX1001, 8:25-26, 8:42-44. Lanning, ¶¶138-139.

- d. [1.A.III] “(b) a unique identifier, wherein the unique identifier of each respective beacon transmission does not directly identify a location of a beacon transmitter, and”**

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

Eagle-Behrens teaches this limitation. As discussed above (§VI.D.1), the Identified Device can identify itself to the Requester Device with a transmission including a combination of UIDs. Behrens teaches that UIDs 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. UIDs like a unique number or symbol are included in beacon transmissions in addition to the MAC address identified for [1.A.II] above because UIDs may be a combination of different unique identifiers. Behrens, [0097], [0122].

Furthermore, UIDs *do not directly identify a location of a beacon transmitter*. Behrens, [0061], [0097] (“identifies a device, and, by association, the owner”). For example, numbers used for UIDs, absent specific intent (which is not found in Eagle-Behrens-Olkkonen), are combinations of letters and/or numbers that do not directly convey any location information. *See also* Eagle, [0008] (Bluetooth beacons provide “proximity detection,” not an “absolute location” like GPS and cellular location systems); EX1001, 4:54-57 (’971 patent describing Bluetooth allowing for “proximity detection”). Lanning, ¶¶140-143.

- e. **[1.A.IV] “(c) a beacon service identifier, wherein the beacon service identifier of each respective beacon transmission identifies that the unique identifier is relevant to stored information associated with a wireless beacon service,”**

Eagle-Olkkonen teaches each beacon transmission comprising *(c) a beacon service identifier (e.g., service class and/or device class information), wherein the beacon service identifier of each respective beacon transmission identifies that the unique identifier is relevant to stored information associated with a wireless beacon service (e.g., service class information and device class information each identify that the associated Identified Device UUIDs (received in the same responses) are relevant to Eagle’s social introduction system, which stores profile information at a server).*

As discussed above (§VI.D.2), it would have been obvious for an Identified Device to respond to inquiries from a Requester Device with *beacon service identifiers* such as service class information and/or device class information for the purpose of filtering UUIDs.

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—the *wireless beacon service* provided by the application program and the server. *See* §VI.D.2. Lanning, ¶¶144-146.

Device class information includes information that identifies the Identified Device’s type of device and is received in inquiry responses according to the Bluetooth specification. Eagle, [0032]; EX1008, 283-285, 1288 (inquiry response includes class of device).

As discussed above (§VI.D.2), it would have been obvious to use the service class and/or device class information to selectively provide UIDs of Identified Devices to the server. The server analyzes its database of stored profile information with those UIDs. Eagle, [0019]-[0021], [0041], [0045], [0051] (identification values used to fetch profile data); *see also* Behrens, [0075] (UIDs are linked to user accounts). The stored profile information (*i.e.*, *stored information* as claimed) includes information in a database that “describes each device and its owner,” such as bibliographic, demographic, and contact information. Eagle, [0005], [0045], [0050]. Lanning, ¶¶147-148.

Accordingly, because the service identifiers (service class and/or device class information) are used to select relevant UIDs for transmission to the server, and each selected relevant UID is used to fetch profile information at the server, the service class information and device class information are each *beacon service*

identifier[s] that identif[y] (through use as UID selection criteria) *that the unique identifier (UID) is relevant to stored information* (selected UIDs are known to be relevant to stored information at the server because they are selected based on the service class and/or device class information as being relevant to Eagle’s social introduction system) *associated with a wireless beacon service* (the stored information is associated with the server used for Eagle’s social introduction system). *See also* [1.B.I]-[1.B.II] below (describing the process of sending notifications to a server and receiving alerts in response) and [1.C] below (describing filtering unique identifiers based on beacon service identifiers to determine whether unique identifiers warrant notification to the server). Lanning, ¶149.

- f. [1.A.V] “wherein the stored information is not otherwise accessible to the wireless device utilizing the short range wireless protocol;”

Collateral estoppel applies: (*Eagle*) regarding communications with the server over a wide area link, not a local wireless link, and receiving stored information from the server, EX1015, 19-30, EX1017, 16-18, 27-28.

Eagle teaches this limitation. When the Requester Device receives an alert of stored profile information from the server (*see* [1.B.I] below), the reception is over a “large area wireless network such as a cellular phone network and/or the Internet.” Eagle, [0039]-[0042]. The Requester Device is not connected to the

server via Bluetooth, and therefore *the stored information is not otherwise accessible* to the Requester Device *utilizing the short range wireless protocol*.

Additionally, Eagle teaches that server profile data indicates thresholds that matches between two device profiles must exceed before alerts are sent (Eagle, [0006]-[0007], [0012], [0048]-[0049], [0052]-[0055]) and limits alert recipients to social circles (*e.g.*, trusted friends; Eagle, [0056], [0060], [0066]-[0067]).

Therefore, the stored information is additionally *not otherwise accessible to the wireless device utilizing the short range wireless protocol* unless certain thresholds are met. Lanning, ¶¶150-153.

- g. [1.B.I] “receiving, at the wireless device via a second wireless protocol, the stored information from one or more servers,”**

Collateral estoppel applies: (Eagle) see [1.A.V].

Eagle teaches *receiving, at the wireless device via a second wireless protocol* (*e.g.*, receiving, at the Requester Device via a cellular connection; *see* [1.A.V] above), *the stored information from one or more servers* (*e.g.*, stored profile information from the server).

When the Requester Device notifies the server of an Identified Device, 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, ¶¶154-157.

h. [1.B.II] “the stored information relating to a particular entity or object associated with a first unique identifier, and”

Collateral estoppel applies: (Eagle) regarding the server stored information relating to the unique identifier received from the second device and to an entity associated with the second device, EX1015, 20-21, 35, EX1017, 18, 27-28.

Eagle teaches this limitation. The Requester Device’s notification to the server includes the unique identifiers of the Identified Device (Eagle, [0048]; “UIDs” in view of Behrens, *see* §VI.D.1), and the server uses the received UIDs to fetch the *stored information* from the profile database (Eagle, [0005], [0020], [0041], [0045], [0050]-[0051]).

As the profile database of *stored information* describes each device and its owner with bibliographic/demographic and contact information (*see* [1.B.I] (VI.E.1.g)), the *stored information* therefore *relates to a particular entity or object*

associated with a first unique identifier (relates to the Identified Device and device owner associated with the UIDs). Lanning, ¶¶158-160.

- i. **[1.B.III] “wherein the second wireless protocol is different from the short range wireless protocol;”**

Collateral estoppel applies: (Eagle) *see* [1.A.V].

Eagle teaches that *the second wireless protocol* (large area wireless network; *see* [1.B.I]) *is different from the short range wireless protocol* (Bluetooth; *see* [1.A.I]). Lanning, ¶161.

- j. **[1.C] “causing selection of one or more of the unique identifiers from the first plurality of beacon transmissions, by filtering the beacon transmissions which include a particular beacon service identifier indicating that a particular received beacon transmission is associated with a particular wireless beacon service; and”**

Eagle-Olkkonen teaches this limitation. The Requester Device receives, from Identified Devices, inquiry responses including *beacon service identifiers* such as service class and/or device class information identifying relevance to Eagle’s social introduction system. *See* [1.A.IV].

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 UUIDs 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) and/or device class information (identifying a device type relevant to an implementation of Eagle's social introduction system; Eagle, [0032], [0061], [0065]-[0065]; §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).

The UUIDs received from Identified Devices and chosen (selected) to be notified to the server, and Eagle-Olkkonen therefore teaches *causing selection of one or more of the unique identifiers from the first plurality of beacon transmissions* (e.g., selecting UUIDs for notification to the server), *by filtering the beacon transmissions which include a particular beacon service identifier indicating that a particular received beacon transmission is associated with a particular wireless beacon service* (e.g., filtering received transmissions that include service class and/or attribute information relating to Eagle's social introduction system). Lanning, ¶¶162-165.

- k. **[1.D] "taking first further action relating to the stored information, if the first unique identifier is present among the selected one or more unique identifiers."**

As discussed for [1.C], Eagle-Olkkonen teaches the *selection of one or more unique identifiers*, which as discussed for [1.B.II] are included in notifications to

the server. The server uses received unique identifiers to fetch corresponding profile information from a database (*i.e.*, the *stored information*) and generate an alert for the Requester Device in alerts. Eagle, [0005], [0041], [0051]; *see also* [1.B.I]. The Requester Device receives the profile data and displays it. Eagle, [0019], [0021], [0058]. The user of the Requester Device is thereby alerted to the presence of users sharing similar personal interests, for example.

Each of the actions described above—notifying the server, receiving profile information, and displaying received profile information—are examples of *first further action relating to the stored information*. See EX1001, 24:41-50 (receiving information is an example of a further action), 25:3-8 (sending an identifier and receiving stored information in response is a further action). Moreover, because these actions are only taken for UIDs that are selected as being relevant (and not filtered out as irrelevant) as discussed for [1.C], these actions are performed *if the first unique identifier is present among the selected one or more unique identifiers*. Lanning, ¶¶166-167.

2. Claim 2

- a. **[2.PRE] “The method of claim 1, wherein the receiving, at the wireless device, via a short range wireless protocol, of the first plurality of beacon transmissions occurs in a first time period, and”**

The *receiving of the first plurality of beacon transmissions* may be defined as occurring in a *first time period*. Lanning, ¶168.

b. [2.A] “wherein the method further comprises, during a second time period:”

Eagle teaches its system operating over many time periods, including a *second time period*. For example, 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 in a *first time period*, and the same Identified Device is detected again one or more times in a *second time period* 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 period and a second day being a second

time period), a user of an Identified Device has “chang[ed] UUIDs” 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 UUIDs are transmitted”). As discussed above (§VI.D.2), changing UUIDs in this manner prevents tracking over time. Lanning, ¶¶169-170.

c. [2.B.I] “receiving, at the wireless device, via a short range wireless protocol, a second plurality of beacon transmissions, each of the second plurality of beacon transmissions comprising three fields”

Eagle-Behrens-Olkkonen teaches this limitation for the same reasons discussed for [1.A.I] (receiving beacon transmissions comprising three fields) and [2.A] (detecting devices in first and second time periods). The *three fields* are discussed below. Lanning, ¶171.

d. [2.B.II] “(a) a MAC address,”

Eagle-Behrens-Olkkonen teaches the *second beacon transmissions* including a *MAC address* in two separate ways discussed below. Lanning, ¶172.

i. MAC address in UUIDs

Collateral estoppel applies: (Behrens) regarding changing UUIDs, EX1031, 46-48 (claim 8).

Behrens teaches that (1) UUIDs may be a combination of different UUID values, and (2) UUIDs change. See §VI.D.I, [1.A.II], [2.A]. An Identified Device’s

UIDs may therefore be changed for the second time period 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, ¶¶173-174.

ii. MAC address in Bluetooth communications

As discussed for [1.A.II], Eagle teaches using Bluetooth protocols, which include a MAC address in each transmission. Lanning, ¶175.

- e. [2.B.III] “(b) a unique identifier, wherein the unique identifier of each respective beacon transmission does not directly identify a location of a beacon transmitter, and”**

Behrens teaches that (1) UIDs may be a combination of different UID values, and (2) UIDs change. *See* §VI.D.I, [1.A.III], [2.A]. An Identified Device’s UIDs may therefore be changed to *be different* for the second time period to use a unique “symbol” instead of the unique “number” used in the first time period. Behrens, [0061], [0097], [0103], [0115], [0122].

As discussed for [1.A.III], UIDs such as symbols do not *directly identify a location of a beacon transmitter*. Lanning, ¶¶176-178.

- f. [2.B.IV] “(c) a beacon service identifier, wherein the beacon service identifier of each respective beacon transmission identifies that the unique identifier is relevant to stored information associated with a wireless beacon service,”**

Eagle-Olkkonen teaches this limitation (for the second time period) for the same reasons discussed for [1.A.IV] (for the first time period).

Moreover, an Identified Device that is the same device continuing to participate in the same services, such as Eagle’s social introduction system, will include the same beacon service identifier (service class and/or device class). Lanning, ¶¶179-180.

- g. [2.B.V] “wherein the stored information is not accessible to the wireless device utilizing the short range wireless protocol;”**

Eagle teaches this limitation (for the second time period) for the same reasons discussed for [1.A.V] (for the first time period). Lanning, ¶181.

- h. [2.C] “causing selection of one or more of the unique identifiers from the second plurality of beacon transmissions, by filtering the beacon transmissions which include the same particular beacon service identifier indicating that the particular received beacon transmission is associated with the same particular wireless beacon service; and”**

Eagle-Olkkonen teaches this limitation (for the second time period) for the same reasons discussed for [1.C] (for the first time period).

Furthermore, as discussed above for [2.A], Eagle teaches periodically detecting devices in the first and second time periods. As the detection of Identified Devices—and subsequent transmissions of notifications and reception of alerts to/from the server, if any—is performed in each time period for the same purpose (*i.e.*, as part of Eagle’s social introduction system), Eagle-Olkkonen teaches *causing selection of one or more of the unique identifiers from the second*

plurality of beacon transmissions with the same *particular beacon service identifier* indicating an association with the same *particular wireless beacon service* as those discussed for [1.C]. Lanning, ¶¶182-183.

- i. **[2.D.I] “taking second further action relating to the stored information, if a second unique identifier is present among the one or more unique identifiers selected from the second plurality of beacon transmissions,”**

Eagle-Olkkonen teaches *taking second further action* in the second time period (relating to a second unique identifier), for the same reasons discussed for the first time period (relating to the first unique identifier). *See* [1.D].

For example, if the Identified Device has been removed from Eagle’s log of recently detected devices between the first and second time periods, then the same exemplary actions of notifying the server, receiving an alert, and displaying the alert will be performed again. Eagle, [0023]-[0024]. Lanning, ¶¶184-185.

- j. **[2.D.II] “wherein the first unique identifier and the second unique identifier are both associated with the same particular entity or object, and wherein the second unique identifier is not equal to the first unique identifier, and further wherein the received beacon transmissions including the first and second unique identifiers are received from a same transmitting device.”**

Eagle-Behrens teaches that *the first unique identifier and the second unique identifier are both associated with the same particular entity or object* because the first and second transmissions including the first and second unique identifiers are

received from the same detected Identified Device. *See* [2.A]. For the same reason, Eagle-Behrens teaches that *the received beacon transmissions including the first and second unique identifiers are received from a same transmitting device (i.e., the same Identified Device).*

Eagle-Behrens teaches that *the second unique identifier is not equal to the first unique identifier* because the first unique identifier includes a unique number (*see* [1.A.III] (VI.E.1.d)) and the second unique identifier includes a unique symbol in the Identified Device's changed UUIDs (*see* [2.B.III] (VI.E.2.e)). The same Identified Device, detected in the first time period and the second time period, therefore transmits *not equal* first and second unique identifiers, respectively. Lanning, ¶¶186-187.

3. Claim 3

- a. **[3.A] “The method of claim 2 wherein the MAC address received in a beacon transmission including the second unique identifier is different from the MAC address received in a beacon transmission including the first unique identifier, but each such beacon transmission includes the same particular beacon service identifier, and”**

Eagle-Behrens teaches MAC addresses in two separate ways. *See* [1.A.II] and [2.B.II]. Eagle-Behrens-Olkkonen further teaches this limitation for the following reasons. Lanning, ¶188.

i. MAC address in UIDs

Eagle-Behrens-Olkkonen teaches that *the MAC address received in a beacon transmission including the second unique identifier (e.g., second time period UIDs include the WLAN MAC address; see [2.B.II] (§VI.E.2.d.i)) is different from the MAC address received in a beacon transmission including the first unique identifier (e.g., changed from the first time period's UIDs including the BD_ADDR; see [1.A.II] (§VI.E.1.c.i)), but each such beacon transmission includes the same particular beacon service identifier (e.g., the first and second transmissions, received from the same Identified Device participating in Eagle's social introduction system, includes the same beacon service identifier; see [2.B.IV]). See §VI.D.1.* Behrens explains that the user may supply their UIDs to the server for synchronization. Behrens, [0065], [0076]. Lanning, ¶189.

ii. MAC address in Bluetooth communications

To the extent Eagle does not explicitly describe that the first and second MAC addresses accompanying each transmission received from the Identified Device according to the Bluetooth protocol (*see [1.A.II] and [2.B.II] (§VI.E.1.c.ii, §VI.E.2.d.ii) are different*, it would have been obvious to a POSITA to modify the Identified Device's MAC address 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 “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, ¶191.

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, ¶¶190-192.

- b. **[3.B] “wherein a plurality of beacon transmissions including the particular service identifier and the first unique identifier are received in the first time period, and no beacon transmissions including the same particular service identifier and the second unique identifier are received in the first time period.”**

Eagle-Behrens-Olkkonen teaches that *a plurality of beacon transmissions including the particular service identifier and the first unique identifier are received in the first time period.*

For example, as discussed for [2.A], a particular Identified Device may be detected by the Requester Device several times in the first time period. Eagle, [0023]. The same Identified Device that has not changed its UIDs (taught by Behrens; *see* §VI.D.1) and that continues to participate in Eagle’s social introduction system will therefore include the same first unique identifier and service identifier in a *plurality of transmissions* during the first time period.

The same Identified Device continuing to participate in Eagle’s social introduction system transmits a second unique identifier (that is different from the first unique identifier) and a beacon service identifier (that is the same as the first beacon service identifier) in the second time period. *See* [2.B.III] and [2.B.IV]. The second unique identifier is different from the first unique identifier because the same Identified Device changes its combination of UIDs between the first and second time periods. *See* [2.D.II]. Accordingly, *no beacon transmissions including the same particular service identifier and the second unique identifier are received in the first time period* because the second time period’s UIDs are not used in the first time period. Lanning, ¶¶193-195.

4. **Claims 4/40/53: “[Claim 3][Claim 37][Claim 53] wherein the second further action is based upon a function currently being performed on a device associated with the wireless beacon service.”**

Eagle-Olkkonen teaches that *the second further action is based upon a function currently being performed on a device associated with the wireless*

beacon service (e.g., joining and participating in a collaborative baseball game or CAD design in progress).

As discussed above (§VI.D.3), it would have been obvious to a POSITA for the Requester Device to take a variety of “actions” with respect to selected unique identifiers, including connecting with Identified Devices to take advantage of services or participate in collaborative activities.

Eagle explains that its social introduction system facilitates collaboration and presents the Requester Device with “information which is of use in a specific application” and useful to “promote communication” with Identified Devices. Eagle, [0007], [0041], [0050], [0065]. Collaboration may be for specific purposes, e.g., for social functions, work projects, and other “job[s] or subject[s],” and information presented on the Requester Device therefore includes contact information useful for connecting with Identified Devices, including contact information, Bluetooth addresses, and Bluetooth device names. Eagle, [0028], [0038], [0041], [0050], [0063]-[0065]. Lanning, ¶¶196-198.

Olkkonen describes other similar collaborative uses of Bluetooth networks, including collaborative programs, CAD design projects, and games in which an Identified Device may already be a participant. Olkkonen, 11:29-30 (“joining... game that is... being played”), 19:51-20:25 and 24:48-61 (describing information exchanged for a network baseball application program to “play ball” and update

scoreboards), 25:63-26:33 (collaborative CAD design routines update and share data among network members).

Accordingly, as Eagle teaches collaborative applications of its system for work projects and social functions, and as Olkkonen teaches examples of Bluetooth work projects (CAD design) and social functions (network baseball), it would have been obvious to a POSITA for the Requester Device to join those Bluetooth networks and participate in those collaborative functions.

As the Requester Device would be joining the Identified Device and participating in an in-progress CAD design project or baseball game, it is *based upon a function currently being performed on a device associated with the wireless beacon service*. Lanning, ¶¶199-201.

5. Claims 5/41/54: “[Claim 4][Claim 40][Claim 53] wherein the function is related to a current phone call, music being played, a video being played, a multi-player game, or a shared application.”

As discussed for claim 4, *the function is, e.g., related to a multi-player game* such as a baseball game, *a shared application* such as a CAD design project, or other “collaborative work projects, collaborative games..., and the like.” Olkkonen, 2:59-65, 20:41-43, 25:63-26:33. Lanning, ¶202.

6. **Claims 6/29/55/56: “[Claim 2][Claim 1][Claim 51][Claim 50] wherein the first [or the second] further action is [additionally] related to receiving advertising¹⁰ information for presentation to a user of the wireless device, based upon the first [or the second] unique [identifier][identifiers], or [based upon] information derived from the first [or second] unique identifier.”**

As discussed for [1.B.I] and [1.D], *the first further action* includes, *e.g.*, receiving and displaying information about an Identified Device *based upon the first unique identifier* (its UIDs). This information is *advertising information received for presentation to a user* of the Requester Device because it advertises the Identified Device (and its owner) as having interests relevant to the Requester Device (and its owner).

Eagle describes other actions based on UIDs, including receiving and presenting “special instructions or announcements” at a trade show, information regarding “nearby resources or facilities, such as an approaching free taxi, or a nearby public restroom,” and “products and expertise” from salesmen. Eagle, [0061]-[0063]. These are also *advertising information for presentation*, as they make the user of the Requester Device aware of useful information and available goods and services. Lanning, ¶¶203-204, 235, 278-279.

¹⁰ “Advertising” information is non-functional descriptive material that should not be accorded patentable weight. MPEP §2111.05.

As discussed for [2.D.I], the same type of action discussed for the *first further action* above may also occur as the *second further action* in the second time period, further meeting this claim.

7. **Claims 7/30/42/57/58: “[Claim 2][Claim1][Claim 37][Claim 51][Claim 52] wherein [one or more of] the first [and the second] further action [additionally] includes [receiving][causing the wireless device to receive] content from a server based upon information derived from [either] the first unique identifier [or the second unique identifier].”**

Collateral estoppel applies: (Eagle) regarding receiving an alert from the server based on determinations regarding friends and trust networks, EX1015, 21-30 (claim 1.d), EX1017, 19-28 (claims 1.f-1.g).

As discussed for [1.B.I], [1.D], and [2.D.I], *the first and the second further action includes, e.g., receiving content from a server based on the first and second unique identifiers (e.g., receiving and displaying alerts based on the first and second unique identifiers used to search stored information in the server).*

Eagle further teaches that the reception of content from the server is *based on information derived from the first or second unique identifiers*. For example, Eagle teaches that an alert is only provided to a Requester Device if profile data associated with an Identified Device (identified by unique identifier) indicates that the user associated with an Identified Device is “trusted” as a “friend” of the user of the Requester Device. Eagle, [0056], [0066]. As the profile data is fetched from

the profile database based on the unique identifiers, the trust information is *derived from* the unique identifiers. Lanning, ¶¶205-206, 236, 257, 280-281.

8. **Claims 8/43/59: “[Claim 2][Claim 37][Claim 51], wherein the first or second further action [additionally] includes [sending a message][or causing a server to send a message][causing the wireless device to send a message] to another device associated with an account related to the first and the second unique identifiers[, or information derived from the first or the second unique identifiers].”**

As discussed for claims 4 and 5, the Requester Device takes further actions such as participating in a network baseball game or collaborative CAD design. Such actions include *sending a message to another device* because all updates in those collaborations are relayed to all devices participating in those collaborations, including the devices associated with the first and the second unique identifier (e.g., the Identified Device that is participating in the collaboration). The Identified Device is *another device* (i.e., not the Requester Device) and is *associated with an account related to the first and the second unique identifiers* (e.g., the Identified Device and its owner have an account with profile information stored at the server, associated by its UIDs; *see* Eagle, [0045] (users are assigned user names and passwords to edit profile information); *see also* [1.B.II] (profile database information fetched by UIDs)).

For example, Olkkonen teaches that for the network baseball program, “update score” and “play ball” routines update game service records and send

those updates to every member of the network. Olkkonen, 20:11-25; *see also* 7:15-18, 14:41-15:3, 18:4-13 (all updates are distributed to all network members).

Updates for the collaborative CAD design program follow similar messaging steps. Olkkonen, 25:63-26:2. Lanning, ¶¶207-208, 258, 282.

9. **Claims 10/44/62: “[Claim 2][Claim 37][Claim 51] wherein the second further action [additionally] includes [preventing][causing the wireless device to prevent] sending [of] the second unique identifier or information derived from the second unique identifier by the [mobile] wireless device to at least one of the one or more servers.”**

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

Eagle teaches this limitation.

For example, 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 the second unique identifier represents a device recently detected, *the second further action includes preventing sending of the second unique identifier or information derived from the second unique identifier by the wireless device to at least one of the one or more servers* (preventing the Requester Device from notifying the server of the second unique identifier). Lanning, ¶¶209-211, 259, 283.

10. **Claims 12/64: “[Claim 1][Claim 50] wherein the [taking] first further action [further][additionally] includes causing the wireless device[,] to: send the first unique identifier or information derived from the first unique identifier to at least one of the one or more servers, and [subsequently] receive the stored information in response.”**

As discussed for [1.D], Eagle-Behrens teaches that *taking first further action* (e.g., notifying the server) *further includes causing the wireless device to send the first unique identifier or information derived from the first unique identifier to at least one of the one or more servers* (e.g., sending a notification including the unique identifier to the server), *and receive the stored information in response* (e.g., receiving an alert containing stored profile information in response).

Lanning, ¶¶212, 284.

11. **Claims 13/14/65/66: “[Claim 1][Claim 2][Claim 50][Claim 51] wherein the [computer program instructions, when executed by the one or more processors in the wireless device, further cause the wireless device to[:] receive] stored information [is received] at the wireless device from at least one of the one or more servers prior to [the taking of the first][performing one or more of the first and the second][performing the first][performing one or more of the first and the second] further action.”**

As discussed for [1.D], Eagle teaches that *the stored information is received at the wireless device from at least one of the one or more servers prior to the taking of the first further action* (e.g., the alert containing stored profile information from the server is received prior to taking the first further action of displaying the information). Lanning, ¶¶213-214, 285-286.

- 12. Claims 15/36/46/67/80: “[Claim 1 further comprising][Claim 37 wherein the operations further comprise][Claim 50 wherein the computer program instructions... further cause the wireless device to][Claim 50 further comprising program instructions that... cause the wireless device to]: [using][use] the stored information to determine if the first unique identifier is present among the [first] selected one or more unique identifiers [from the first plurality of beacon transmissions].”**

Eagle-Behrens teaches *using the stored information to determine if the first unique identifier is present among the selected one or more of the unique identifiers from the first plurality of beacon transmissions* (e.g., using received blacklist instructions to determine if a detected Identified Device is present among the selected received UIDs).

As discussed above (§VI.D.3), it would have been obvious for the Requester Device to take a variety of “actions” with respect to selected unique identifiers, including ignoring an Identified Device (detected in either the first or second time periods) if its UIDs are found on a blacklist received from a server. *See Behrens, [0101]-[0102], [0124]* (receiving blacklist instructions stored on a server and ignoring UIDs listed therein).

Eagle-Behrens-Olkkonen leaves to a POSITA the order of operations for the selection (e.g., filtering based on service identifier as taught by Olkkonen) and blacklist filtering (e.g., ignoring blacklisted UIDs as taught by Behrens), and it would have been obvious to perform the selection first and then filter based on the

received blacklist, as there are only two finite and predictable options (filter first, blacklist second; or blacklist first, filter second) and they both produce substantially the same result (narrowing down Identified Devices based on two criteria). *KSR*, 550 at 402-403. Lanning, ¶¶215-217, 239, 260, 287, 293.

13. Claims 16/68: “[Claim 2][Claim 51] wherein all beacon transmitter devices participating in the particular wireless beacon service have the same particular beacon service identifier.”

Eagle-Olkkonen teaches that *all beacon transmitter devices participating in the particular wireless beacon service have the same particular beacon service identifier*.

As discussed above regarding Eagle-Olkkonen (§VI.D.2) and for [1.A.IV] and [2.B.IV], an Identified Device participating in Eagle’s social introduction system will include the same beacon service identifier (service class and/or device class information) in different time periods. Similarly, other Identified Devices participating in Eagle’s social introduction system and that are the same type of device (*e.g.*, where Eagle’s system is applied to a social function for phones; *see* discussion of Device class information in §VI.D.2) will also transmit the same beacon service identifier. Lanning, ¶¶218-219, 288.

14. Claim 18: “[Claim 2] wherein the steps performed at the wireless device are performed as a result of an application program executing on the wireless device.”

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

Eagle teaches that the Requester Device includes a processor “programmed with an application program... that enable[s] the cellular phone to identify and log the presence of other... Bluetooth devices that are nearby, and to display an identification of those devices.” Eagle, [0019]. *See also* Eagle, [0020] (application program (“BlueAware”) executes on the processor to generate and send notification messages), [0029] (installing software and registering with the server); Olkkonen, 15:10-13, 15:31-42 (example executing a “network baseball application program”), 25:63-26:33 (program routines for collaborative CAD design). Lanning, ¶¶220-221.

15. Claims 19/34/72: “[Claim 2][Claim 1][Claim 51] wherein the [second][first] further action is [additionally] related to either a product tied to a location or an advertisement tied to a location.”

Eagle teaches that *the second further action is related to either a product tied to a location or an advertisement tied to a location.*

As discussed for [1.D] and [2.D.I], exemplary first and second further actions include displaying alerts based on profile information fetched at the server. Eagle teaches that such information may be an advertisement of “special

instructions or announcements whenever [the Requester Device] come[s] within range of a greeting beacon near the entrance to [a trade] show” and are therefore tied to the “physical infrastructure” at the trade show. Eagle, [0061].

Reception and display of instructions or announcements are therefore *related to a product or advertisement* (e.g., the trade show product and its announcements) *tied to a location* (e.g., tied to the trade show location). *See also* Eagle, [0061] (additional use includes identifying a nearby restroom, which is *a product or advertisement tied to a location*). Lanning, ¶¶222-224, 237, 289.

Regarding claim 34, as discussed for [2.D.I], the same type of action discussed for the *first further action* above may also occur as the *second further action* in the second time period.

- 16. Claims 22/48/75: “[Claim 2][Claim 37][Claim 51] wherein the second further action [additionally] includes [allowing][causing the wireless device to allow] a user associated with the [mobile] wireless device to [be provided] access to an object or device associated with the wireless beacon service.”**

Eagle-Olkkonen teaches that *the second further action includes allowing a user associated with the wireless device to be provided access to an object or device associated with the wireless beacon service* (e.g., providing the user of the Requester Device access to printers, Internet gateways, and files through the Identified Device that is associated with Eagle’s social introduction system).

As discussed above (§VI.D.3), it would have been obvious for the Requester Device to take a variety of “actions” with respect to selected unique identifiers, including connecting with Identified Devices to take advantage of services or participate in collaborative activities.

Olkkonen teaches that network services include providing user access to printers, fax machines, Internet gateways, and shared files. Olkkonen, 6:19-21, 18:60-63, 19:13-16, 25:48-52. Lanning, ¶¶225-227, 261, 290.

- 17. Claims 23/35/49/76: “[Claim 2][Claim 3][Claim 37][Claim 51] wherein the [taking][first or] second further action additionally [comprises: controlling][includes causing the wireless device to control] further communications between the [mobile] wireless device and at least one [other] device or server associated with an entity or object in proximity to the wireless device [based upon information derived from the first or second unique identifier].”**

Eagle-Behrens-Olkkonen teaches this limitation in two ways.

First, as discussed for claim 10, Eagle teaches that *the taking second further action additionally comprises: controlling further communications between the wireless device and at least one device or server (e.g., not sending a notification to the server if the associated device was previously encountered) associated with an entity or object in proximity to the wireless device (e.g., the server is associated with the user being blocked, who is in Bluetooth proximity of the Requester Device and is registered with Eagle’s social introduction system)*. Lanning, ¶¶228-229.

Second, as discussed for claim 15, 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, ¶230.

Eagle-Behrens therefore further teaches that *taking second further action additionally comprises: controlling further communications between the wireless device and at least one device (e.g., instructing the Requester Device to ignore and block further contact with an Identified Device if its UID is on a blacklist received from a server) or server (e.g., not notifying the server of that Identified Device) associated with an entity or object in proximity to the wireless device (e.g., the Identified Device and the server are associated with the user being blocked, who is in Bluetooth proximity of the Requester Device and is registered with Eagle’s social introduction system)*. Lanning, ¶¶230, 238, 262-263, 291.

Additionally, with respect to claim 49, because the actions of not notifying the server and blocking communications with an Identified Device are each based

on information determined using those received UIDs (e.g., that the UIDs have recently been detected or that the UIDs are on a blacklist), the controlling is *based upon information derived from the first or second unique identifier*. Lanning, ¶¶262-263.

- 18. Claims 26/38/79: “[Claim 2 further comprising][Claim 37 wherein the operations further comprise][Claim 51 wherein the computer program instructions, when executed by the wireless device, further cause the wireless device to]: [using][use] the stored information to determine if the second unique identifier is present among the selected one or more of the unique identifiers from the second plurality of beacon transmissions.”**

Eagle-Behrens-Olkkonen teaches this limitation (for the second unique identifier) for the same reasons discussed for claim 15 (for the first unique identifier). Lanning, ¶¶232, 253, 292.

- 19. Claims 27/39/81: “[Claim 1][Claim 37][Claim 50] wherein [the][each] MAC address is a randomly generated 48 bit number matching a format of a Bluetooth BD_ADDR.”**

Eagle-Behrens-Olkkonen teaches that *the MAC address is a randomly generated 48 bit number matching a format of a Bluetooth BD_ADDR* (e.g., obvious to use a randomized BD_ADDR). See [3.A]. Lanning, ¶¶233, 254, 294.

- 20. Claim 28: “[Claim 3] wherein the short range protocol is derived from Bluetooth.”**

Eagle-Behrens-Olkkonen teaches the method of claim 3, including a randomized BD_ADDR to be “used in all the functions of the Bluetooth device that normally use the BD_ADDR.” EX1011, [0006]-[0013]. See [3.A].

Randomized BD_ADDR values were not part of the Bluetooth specification prior to the '971 patent (*i.e.*, Bluetooth version 2.1). Therefore, using randomized BD_ADDRs in Bluetooth communications would have been communicating with a *short range protocol derived from Bluetooth*. Lanning, ¶234.

21. Claim 37

Claim 37 recites a “wireless device” (including radio(s), a processor, and memory) that performs functions substantially similar to steps in claim 1-2’s “method,” and is obvious over Eagle-Behrens-Olkkonen for the same reasons. *See* §VI.E.1-§V.E.2. Limitations specific to claim 37’s device are discussed below.

a. [37.PRE] “A mobile wireless device comprising:”

To the extent this preamble is limiting, Eagle-Behrens-Olkkonen teaches a *mobile wireless device* (*e.g.*, the Requester Device is a phone communicating via Bluetooth and cellular protocols). *See* [1.A.I]. Lanning, ¶240.

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

Eagle teaches the Requester device including *one or more radios for providing reception and transmission for each of a Bluetooth wireless protocol and a second wireless protocol*. Eagle, [0018] (“cellular telephones which incorporate short range radio transceivers that use the Bluetooth protocol”), claim 2 (including a “short range radio transmitter” and “receiver,” and a “long range

communications interface coupled to [a] long range communications network”); *see also* [0019]-[0020], [0022], [0028], [0038]-[0040]. Lanning, ¶241.

c. [37.B] “one or more processors; and”

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. Lanning, ¶242.

d. [37.C] “one or more memory devices coupled to the one or more processors, the one or more memory devices storing a set of instructions that when executed by the one or more processors cause the one or more processors to perform operations including:”

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]. A POSITA would have recognized that downloading, installing, and executing an application program as described obviously, if not necessarily, requires a *memory* on the device coupled to

the processor. Lanning, ¶¶243-244; Olkkonen, 15:31-34, 35:39-41, 49:56-59; Eagle, [0023]-[0024].

- e. **[37.D] “receiving from a beacon transmitter... a first plurality of beacon transmissions during a first time period...”**

See [1.A.I]-[1.A.V] (receiving beacon transmissions comprising three fields), [2.PRE] (first transmissions are received in a first time period).

Lanning, ¶¶245-252 (corresponding to [37.D]-[37.K].

- f. **[37.E] “receiving... stored information...;”**

See [1.B.I]-[1.B.II].

- g. **[37.F] “selecting one or more unique identifiers... by filtering the beacon transmissions...;”**

See [1.C].

- h. **[37.G] “taking first further action... if the first unique identifier is present...;”**

See [1.D].

- i. **[37.H] “receiving, during a second time period, a second plurality of beacon transmissions...;”**

See [2.A]-[2.B.V].

- j. **[37.I] “selecting one or more of the unique identifiers... by filtering the beacon transmissions...;”**

See [2.C].

- k. **[37.J] “taking second further action... if a second unique identifier is present..., wherein the second unique identifier is associated with the same entity or object, and wherein the second unique identifier is not equal to the first unique identifier, and further wherein the received beacon transmissions including the first and second unique identifiers are received from a same transmitting device; and”**

See [2.D.I]-[2.D.II].

- l. **[37.K] “wherein the [second beacon transmission] MAC address... is different from the [first beacon transmission] MAC address..., but each... includes the same particular beacon service identifier.”**

See [3.A].

22. Claim 50

Claims 50-51 recite a “computer program product” that performs functions substantially similar to steps in claim 1-3’s “method” and in claim 37’s “wireless device,” and are obvious over Eagle-Behrens-Olkkonen for the same reasons. *See* §VI.E.1-§V.E.2, §VI.E.21. Limitations specific to claim 50-51’s program product are discussed below.

- a. **[50.PRE] “A computer program product for installation in a non-volatile memory in a wireless device, the computer program product comprising computer program instructions that, when read from the non-volatile memory, and then executed by one or more processors in the wireless device, cause the wireless device to:”**

See [37.B]-[37.C]; Eagle, [0028]-[0029] (wireless device including memory coupled to processors executing an installed program).

Furthermore, to the extent this preamble is limiting, “non-volatile” memory would have been well-known to POSITAs (Behrens, [0106] (device includes “memory, which may be FLASH memory”) and it would have been obvious to a POSITA to use existing non-volatile memories for program storage so that the device does not need to download and install the program repeatedly. Lanning, ¶264.

b. [50.A] “process a first plurality of beacon transmissions..., each beacon transmission comprising three fields...;”

See [37.D] (receiving beacon transmissions), [37.F]-[37.G] (selecting one or more unique identifiers and, *e.g.*, notifying the server, requires *processing* the transmissions). Lanning, ¶265.

c. [50.B] “process stored information...;”

See [1.B.I]-[1.B.III], [37.E] (receiving stored information) and [1.D] (taking first action relating to the stored information, *e.g.*, displaying the information; thereby *processing* the information). Lanning, ¶266.

d. [50.C] “select one or more of the unique identifiers... by filtering the beacon transmissions...; and”

See [37.F]. Lanning, ¶267.

e. [50.D] “perform a first further action... if the first unique identifier is present....”

See [37.G]. Lanning, ¶268.

23. Claim 51

- a. **[51.PRE] “[Claim 50] wherein the computer program instructions, when executed by the one or more processors in the wireless device, cause the wireless device to:”**

See claim 50.

- b. **[51.A] “during a first time period: process the first plurality of beacon transmissions..., and”**

See [50.A] processing the first plurality of beacon transmissions), [37.D] (the first plurality of beacon transmission are received in a first time period). The time period in which the processing occurs may be defined as a *first time period*. Lanning, ¶270.

- c. **[51.B] “during a second time period:”**

See [37.H]. Lanning, ¶271.

- d. **[51.C] “process a second plurality of beacon transmissions..., each beacon transmission comprising three fields...;”**

See [37.H] (receiving second beacon transmissions in a second time period) and [37.I]-[37.J] (selecting one or more unique identifiers and, *e.g.*, notifying the server, requires *processing* the transmissions). Lanning, ¶272.

- e. **[51.D] “select one or more of the unique identifiers... by filtering the beacon transmissions which include the same particular beacon service identifier...; and”**

See [37.I]. Lanning, ¶273.

- f. **[51.E] “perform a second further action... if a second unique identifier is present....”**

See [37.J]. Lanning, ¶274.

24. **Claim 52: “[Claim 51] wherein the [first and second beacon transmission] MAC address [are different], but each... includes the same particular beacon service identifier, and... no beacon transmissions including the same service identifier and the second unique identifier are received in the first time period.”**

See [37.K] and [3.A]-[3.B]. Lanning, ¶275.

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.¹¹

VII. 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.

¹¹ <https://www.uspto.gov/sites/default/files/documents/InterimProcesses-PTABWorkloadMgmt-20250326.pdf>

1. APPENDIX A: U.S. PATENT NO. 11,687,971 CLAIM LISTING

Claim 1
[1.PRE] A method comprising:
[1.A] [1.A.I] receiving, at a wireless device, via a short range wireless protocol, a first plurality of beacon transmissions, each beacon transmission comprising three fields [1.A.III] (a) a MAC address, [1.A.III] (b) a unique identifier, wherein the unique identifier of each respective beacon transmission does not directly identify a location of a beacon transmitter, and [1.A.IV] (c) a beacon service identifier, wherein the beacon service identifier of each respective beacon transmission identifies that the unique identifier is relevant to stored information associated with a wireless beacon service, [1.A.V] wherein the stored information is not otherwise accessible to the wireless device utilizing the short range wireless protocol;
[1.B.I] receiving, at the wireless device via a second wireless protocol, the stored information from one or more servers, [1.B.II] the stored information relating to a particular entity or object associated with a first unique identifier, and [1.B.III] wherein the second wireless protocol is different from the short range wireless protocol;
[1.C] causing selection of one or more of the unique identifiers from the first plurality of beacon transmissions, by filtering the beacon transmissions which include a particular beacon service identifier indicating that a particular received beacon transmission is associated with a particular wireless beacon service; and
[1.D] taking first further action relating to the stored information, if the first unique identifier is present among the selected one or more unique identifiers.
Claim 2
[2.PRE] The method of claim 1, wherein the receiving, at the wireless device, via a short range wireless protocol, of the first plurality of beacon transmissions occurs in a first time period, and
[2.A] wherein the method further comprises, during a second time period:
[2.B] receiving, at the wireless device, via a short range wireless protocol, a second plurality of beacon transmissions, each of the second plurality of beacon transmissions comprising three fields (a) a MAC address, (b) a unique identifier, wherein the unique identifier of each respective beacon transmission does not directly identify a location of a beacon transmitter, and (c) a beacon service identifier, wherein the beacon service identifier of each respective beacon transmission identifies that the unique identifier is relevant to stored information associated with a wireless beacon service, wherein the stored information is not accessible to the wireless device utilizing the short range wireless protocol;

[2.C] causing selection of one or more of the unique identifiers from the second plurality of beacon transmissions, by filtering the beacon transmissions which include the same particular beacon service identifier indicating that the particular received beacon transmission is associated with the same particular wireless beacon service; and
[2.D] taking second further action relating to the stored information, if a second unique identifier is present among the one or more unique identifiers selected from the second plurality of beacon transmissions, wherein the first unique identifier and the second unique identifier are both associated with the same particular entity or object, and wherein the second unique identifier is not equal to the first unique identifier, and further wherein the received beacon transmissions including the first and second unique identifiers are received from a same transmitting device.
Claim 3
[3.A] The method of claim 2 wherein the MAC address received in a beacon transmission including the second unique identifier is different from the MAC address received in a beacon transmission including the first unique identifier, but each such beacon transmission includes the same particular beacon service identifier, and [3.B] wherein a plurality of beacon transmissions including the particular service identifier and the first unique identifier are received in the first time period, and no beacon transmissions including the same particular service identifier and the second unique identifier are received in the first time period.
Claim 4
The method of claim 3 wherein the second further action is based upon a function currently being performed on a device associated with the wireless beacon service.
Claim 5
The method of claim 4 wherein the function is related to a current phone call, music being played, a video being played, a multi-player game, or a shared application
Claim 6
The method of claim 2 wherein the first or the second further action is related to receiving advertising information for presentation to a user of the wireless device, based upon the first or the second unique identifier, or information derived from the first or second unique identifier.
Claim 7

The method of claim 2 wherein one or more of the first and the second further action includes receiving content from a server based upon information derived from either the first unique identifier or the second unique identifier.
Claim 8
The method of claim 2, wherein the first or second further action includes sending a message to another device associated with an account related to the first and the second unique identifiers.
Claim 10
The method of claim 2 wherein the second further action includes preventing sending of the second unique identifier or information derived from the second unique identifier by the wireless device to at least one of the one or more servers.
Claim 12
The method of claim 1 wherein the taking first further action further includes causing the wireless device, to: send the first unique identifier or information derived from the first unique identifier to at least one of the one or more servers, and receive the stored information in response.
Claim 13
The method of claim 1 wherein the stored information is received at the wireless device from at least one of the one or more servers prior to the taking of the first further action.
Claim 14
The method of claim 2 wherein the stored information is received at the wireless device from at least one of the one or more servers prior to performing one or more of the first and the second further action.
Claim 15
The method of claim 1 further comprising: using the stored information to determine if the first unique identifier is present among the first selected one or more unique identifiers.
Claim 16
The method of claim 2 wherein all beacon transmitter devices participating in the particular wireless beacon service have the same particular beacon service identifier.
Claim 18
The method of claim 2 wherein the steps performed at the wireless device are performed as a result of an application program executing on the wireless device.
Claim 19
The method of claim 2 wherein the second further action is related to either a product tied to a location or an advertisement tied to a location.

Claim 22
The method of claim 2 wherein the second further action includes allowing a user associated with the wireless device to be provided access to an object or device associated with the wireless beacon service.
Claim 23
The method of claim 2 wherein the taking second further action additionally comprises: controlling further communications between the wireless device and at least one device or server associated with an entity or object in proximity to the wireless device.
Claim 26
The method of claim 2 further comprising: using the stored information to determine if the second unique identifier is present among the selected one or more of the unique identifiers from the second plurality of beacon transmissions.
Claim 27
The method of claim 1 wherein the MAC address is a randomly generated 48 bit number matching a format of a Bluetooth BD_ADDR.
Claim 28
The method of claim 3 wherein the short range protocol is derived from Bluetooth.
Claim 29
The method of claim 1 wherein the first further action is related to receiving advertising information for presentation to a user of the wireless device, based upon the first unique identifier, or information derived from the first unique identifier.
Claim 30
The method of claim 1 wherein the first further action includes receiving content from a server based upon information derived from the first unique identifier.
Claim 34
The method of claim 1 wherein the first further action is related to either a product tied to a location or an advertisement tied to a location.
Claim 35
The method of claim 3 wherein the taking second further action additionally comprises: controlling further communications between the wireless device and at least one device or server associated with an entity or object in proximity to the wireless device.
Claim 36

The method of claim 1 further comprising:
using the stored information to determine if the first unique identifier is present among the selected one or more of the unique identifiers from the first plurality of beacon transmissions.

Claim 37

[37.PRE] A mobile wireless device comprising:

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

[37.B] one or more processors; and

[37.C] one or more memory devices coupled to the one or more processors, the one or more memory devices storing a set of instructions that when executed by the one or more processors cause the one or more processors to perform operations including:

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

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

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

[37.G] taking first further action relating to the stored information, if the first unique identifier is present among the selected one or more unique identifiers;

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

the stored information is not accessible to the wireless device utilizing the Bluetooth wireless protocol;
[37.I] selecting one or more of the unique identifiers from the second plurality of beacon transmissions, by filtering the beacon transmissions which include the same particular beacon service identifier indicating that a particular received beacon transmission is associated with the same particular wireless beacon service;
[37.J] taking second further action relating to the stored information, if a second unique identifier is present among the one or more unique identifiers selected from the second plurality of beacon transmissions, wherein the second unique identifier is associated with the same entity or object, and wherein the second unique identifier is not equal to the first unique identifier, and further wherein the received beacon transmissions including the first and second unique identifiers are received from a same transmitting device; and
[37.K] wherein the MAC address received in a beacon transmission including the second unique identifier is different from the MAC address received in a beacon transmission including the first unique identifier, but each such beacon transmission includes the same particular beacon service identifier.
Claim 38
The mobile wireless device of claim 37 wherein the operations further comprise: using the stored information to determine if the second unique identifier is present among the selected one or more of the unique identifiers from the second plurality of beacon transmissions
Claim 39
The mobile wireless device of claim 37 wherein each MAC address or a respective beacon transmission is a randomly generated 48 bit number matching a format of a Bluetooth BD_ADDR.
Claim 40
The mobile wireless device of claim 37 wherein the second further action is based upon a function currently being performed on a device associated with the wireless beacon service.
Claim 41
The mobile wireless device of claim 40 wherein the function is related to a current phone call, music being played, a video being played, a multi-player game, or a shared application.
Claim 42

The mobile wireless device of claim 37 wherein one or more of the first further action and the second further action includes receiving content from a server based upon information derived from either the first unique identifier or the second unique identifier.
Claim 43
The mobile wireless device of claim 37, wherein the first or second further action includes sending a message or causing a server to send a message to another device associated with an account related to the first and the second unique identifiers.
Claim 44
The mobile wireless device of claim 37 wherein the second further action includes preventing sending of the second unique identifier or information derived from the second unique identifier by the mobile wireless device to at least one of the one or more servers.
Claim 46
The mobile wireless device of claim 37 wherein the operations further comprise: using the stored information to determine if the first unique identifier is present among the first selected one or more unique identifiers.
Claim 48
The mobile wireless device of claim 37 wherein the second further action includes allowing a user associated with the mobile wireless device to be provided access to an object or device associated with the wireless beacon service.
Claim 49
The mobile wireless device of claim 37 wherein the first or second further action additionally comprises: controlling further communications between the mobile wireless device and at least one device or server associated with an entity or object in proximity to the wireless device based upon information derived from the first or second unique identifier.
Claim 50
[50.PRE] A computer program product for installation in a non-volatile memory in a wireless device, the computer program product comprising computer program instructions that, when read from the non-volatile memory, and then executed by one or more processors in the wireless device, cause the wireless device to:
[50.A] process a first plurality of beacon transmissions, received at the wireless device via a Bluetooth wireless protocol, each beacon transmission comprising three fields (a) a MAC address, (b) a unique identifier, wherein the unique

identifier of each respective beacon transmission does not directly identify a location of a beacon transmitter, and (c) a beacon service identifier, wherein the beacon service identifier of each respective beacon transmission identifies that the unique identifier is relevant to stored information associated with a wireless beacon service, wherein the stored information is not otherwise accessible to the wireless device utilizing the Bluetooth wireless protocol;
[50.B] process stored information transferred from one or more servers to the wireless device via a second wireless protocol, wherein the stored information relates to an entity or object associated with a first unique identifier, and wherein the second wireless protocol is different from the Bluetooth wireless protocol;
[50.C] select one or more of the unique identifiers from the first plurality of beacon transmissions, by filtering the beacon transmissions which include a particular beacon service identifier indicating that a particular received beacon transmission is associated with a particular wireless beacon service; and
[50.D] perform a first further action, the first further action relating to the stored information, if the first unique identifier is present among the selected one or more unique identifiers.
Claim 51
[51.PRE] The computer program product of claim 50 wherein the computer program instructions, when executed by the one or more processors in the wireless device, cause the wireless device to:
[51.A] during a first time period: process the first plurality of beacon transmissions in the first time period, and
[51.B] during a second time period:
[51.C] process a second plurality of beacon transmissions, received at the wireless device via the Bluetooth wireless protocol, each beacon transmission comprising three fields (a) a MAC address, (b) a unique identifier, wherein the unique identifier of each respective beacon transmission does not directly identify a location of a beacon transmitter, and (c) a beacon service identifier, wherein the beacon service identifier of each respective beacon transmission identifies that the unique identifier is relevant to stored information associated with a wireless beacon service, wherein the stored information is not otherwise accessible to the wireless device utilizing the Bluetooth wireless protocol;
[51.D] select one or more of the unique identifiers from the second plurality of beacon transmissions, by filtering the beacon transmissions which include the same particular beacon service identifier indicating that the particular received beacon transmission is associated with the same particular wireless beacon service; and

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

Claim 52

The computer program product of claim 51 wherein the MAC address received in a beacon transmission including the second unique identifier is different from the MAC address received in a beacon transmission including the first unique identifier, but each such beacon transmission includes the same particular beacon service identifier, and wherein a plurality of beacon transmissions including the particular beacon service identifier and the first unique identifier are received in the first time period, and no beacon transmissions including the same service identifier and the second unique identifier are received in the first time period.

Claim 53

The computer program product of claim 52 wherein the second further action is based upon a function currently being performed on a device associated with the wireless beacon service.

Claim 54

The computer program product of claim 53 wherein the function is related to a current phone call,
music being played,
a video being played,
a multi-player game, or
a shared application.

Claim 55

The computer program product of claim 51 wherein the first or the second further action is additionally related to receiving advertising information for presentation to a user of the wireless device, based upon the first or the second unique identifiers, or based upon information derived from the first or second unique identifier.

Claim 56

The computer program product of claim 50 wherein the first further action is additionally related to receiving advertising information for presentation to a user of the wireless device, based upon the unique identifier, or based upon information derived from the first unique identifier.

Claim 57
The computer program product of claim 51 wherein one or more of the first further action and the second further action additionally includes causing the wireless device to receive content from a server based upon information derived from either the first unique identifier or the second unique identifier.
Claim 58
The computer program product of claim 52 wherein the first further action additionally includes causing the wireless device to receive content from a server based upon information derived from the first unique identifier.
Claim 59
The computer program product of claim 51, wherein the first or second further action additionally includes causing the wireless device to send a message to another device associated with an account related to the first or the second unique identifiers, or information derived from the first or the second unique identifiers.
Claim 62
The computer program product of claim 51 wherein the second further action additionally includes causing the wireless device to prevent sending the second unique identifier or information derived from the second unique identifier by the wireless device to at least one of the one or more servers.
Claim 64
The computer program product of claim 50 wherein the first further action additionally includes causing the wireless device to: send the first unique identifier or information derived from the first unique identifier to at least one of the one or more servers, and subsequently receive the stored information in response thereto.
Claim 65
The computer program product of claim 50 wherein the computer program instructions, when executed by the one or more processors in the wireless device, further cause the wireless device to receive stored information at the wireless device from at least one of the one or more servers prior to performing the first further action.
Claim 66
The computer program product of claim 51 wherein the computer program instructions, when executed by the one or more processors in the wireless device, further cause the wireless device to: receive stored information at the wireless device from at least one of the one or more servers prior to performing one or more of the first and the second further action.

Claim 67
The computer program product of claim 50 wherein the computer program instructions, when executed by the one or more processors in the wireless device, further cause the wireless device to: use the stored information to determine if the first unique identifier is present among the first selected one or more unique identifiers
Claim 68
The computer program product of claim 51 wherein all beacon transmitter devices participating in the particular wireless beacon service have the same particular beacon service identifier.
Claim 72
The computer program product of claim 51 wherein the second further action is additionally related to either a product tied to a location or to an advertisement tied to a location.
Claim 75
The computer program product of claim 51 wherein the second further action additionally includes causing the wireless device to allow a user associated with the wireless device to access to an object or device associated with the wireless beacon service.
Claim 76
The computer program product of claim 51 wherein the second further action additionally includes causing the wireless device to control further communications between the wireless device and at least one other device or server associated with an entity or object in proximity to the wireless device.
Claim 79
The computer program product of claim 51 wherein the computer program instructions, when executed by the wireless device, further cause the wireless device to: use the stored information to determine if the second unique identifier is present among the selected one or more of the unique identifiers from the second plurality of beacon transmissions.
Claim 80
The computer program product of claim 50 further comprising program instructions that, when executed by the one or more processors, cause the wireless device to: use the stored information to determine if the first unique identifier is present among the selected one or more of the unique identifiers from the first plurality of beacon transmissions.

Claim 81

The computer program product of claim 50 wherein the MAC address is a randomly generated 48 bit number matching a format of a Bluetooth BD ADDR.

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 IPR2025-01051 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 13,969 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.