

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

TARGET CORPORATION,

Petitioner,

v.

PROXICOM WIRELESS, LLC,

Patent Owner.

Case IPR2020-00904

U.S. Patent No. 7,936,736

PETITION FOR *INTER PARTES* REVIEW

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	MANDATORY NOTICES (§42.8).....	5
	A. Real Party-In-Interest	5
	B. Related Matters.....	5
	A. Lead and Back-Up Counsel and Service Information	5
III.	PAYMENT OF FEES	6
IV.	REQUIREMENTS FOR INTER PARTES REVIEW	6
	A. Grounds for Standing	6
	B. Identification of Challenge.....	7
	1. The Specific Art on Which the Challenge is Based	7
	2. Statutory Grounds on Which the Challenge is Based.....	9
	3. How the Challenged Claims Are Unpatentable.....	9
V.	THE '736 PATENT.....	10
VI.	PROSECUTION HISTORY	12
VII.	LEVEL OF ORDINARY SKILL	13
VIII.	CLAIM CONSTRUCTION	14
IX.	GROUND OF UNPATENTABILITY.....	15
	A. Grounds 1-2: Claims 1, 5-8, 10, 12, 14-15, 18, 20-22	16
	1. Overview of Eagle	17
	2. Claim Chart—Eagle.....	24
	B. Ground 3: Claims 8, 14, 22	53
	1. Overview of Mgrdechian and Motivation to Apply Its Teachings to Eagle.....	53
	2. Claim Chart—Eagle in view of Mgrdechian	56

X. SECONDARY CONSIDERATIONS59
XI. CONCLUSION.....60

LIST OF EXHIBITS

Ex. 1001	U.S. Patent No. 7,936,736 (“736”)
Ex. 1002	File History of U.S. Patent No. 7,936,736 (“736 FH”)
Ex. 1003	Declaration of David Hilliard Williams (“Williams”)
Ex. 1004	U.S. Patent Application Publication No. 2005/0250552 (“Eagle”)
Ex. 1005	U.S. Patent No. 7,545,784 (“Mgrdechian”)
Ex. 1006	U.S. Patent Application Publication No. 2004/0243519 (“Perttila”)
Exs. 1007 - 1015	Reserved
Ex. 1016	<i>Lighting Science Group Corp. v. Nicor, Inc. et al.</i> , No. 6:16-cv-413-Orl-37GJK, Dkt. 98 (M.D. Fl. May 9, 2017)
Ex. 1017	<i>Lighting Science Group Corp. v. Leedarsen Lighting Co. et al.</i> , No. 6:17-cv-826-Orl-37GJK, Dkt. 31 (M.D. Fl. Oct. 27, 2017)
Ex. 1018	<i>Automatic Mfg. Sys., Inc. v. Primera Tech., Inc.</i> , No. 6:12-cv-1727-Orl-37DAB, Dkt. 58 (M.D. Fl. Nov. 21, 2013)
Ex. 1019	<i>zIT Consulting GMBH v. BMC Software, Inc.</i> , No. 6:15-cv-1012-Orl-37KRS, Dkt. 63 (M.D. Fl. Mar. 17, 2016)
Ex. 1020	<i>Proxicom Wireless, LLC v. Target Corp.</i> , No. 6:19-cv-01886-RBD-LRH, Dkt. 56 (M.D. Fl. Feb. 28, 2020)
Ex. 1021	<i>Proxicom Wireless, LLC v. Macy's, Inc., et al.</i> , No. 6:18-cv-64-Orl-37GJK, Dkt. 94 (M.D. Fl. Feb. 12, 2019)
Ex. 1022	U.S. Patent No. 7,877,082 (“Eagle Patent”)
Ex. 1023	U.S. Patent Publication No. 2005/0174975 (“Mgrdechian 975”)

Ex. 1024	U.S. Patent No. 8,295,819 (“Kaplan”)
Ex. 1025	U.S. Patent No. 9,734,198 (“Taylor”)
Ex. 1026	Declaration of Crena Pacheco

Pursuant to §§311-319 and §42,¹ Target Corporation (“Petitioner”) petitions for *inter partes* review (“IPR”) of claims 1, 5-8, 10, 12, 14-15, 18, and 20-22 (“Challenged Claims”) of U.S. Patent 8,374,736 (“’736”) (Ex. 1001), assigned to Proxicom Wireless, LLC (“PO”) according to USPTO records. There is a reasonable likelihood that at least one challenged claim is unpatentable as explained herein. Petitioner requests review of the Challenged Claims, and judgment finding them unpatentable under §102 and/or §103.

I. INTRODUCTION

The ’736’s purported invention is the use of a “central server” to “broker the exchange of information between” two entities associated with two wireless devices. ’736, Abstract. “Rather than directly exchanging application data flow between the two devices using [a] short range wireless capability, a second wireless capability allows for one or more of the devices to communicate with a central server via the internet” to perform the exchange. *Id.*

¹ Section cites are to 35 U.S.C. or 37 C.F.R. as context indicates. All emphasis/annotations have been added unless noted. Annotations added to the figures herein generally quote the language of the Challenged Claims for reference.

The '736 admits that, prior to the alleged invention, wireless devices already were configured to use both the short-range and wide-area connections claimed in the '736. *Id.*, 2:9-21 (admitting “[m]ost mobile phones on the market today support at least two wireless standards; one for the cellular wireless wide area network connection (WWAN) and one for a wireless personal or local area network” such as “Bluetooth”). And the '736 admits that prior art systems already were using wireless devices for e-commerce and social networking applications. *Id.*, 1:54-66, 2:22-33.

The only purportedly novel element of the '736 claims is a server's use of a “disclosure policy” associated with a second wireless device for determining what “further information” may be provided to a first wireless device. For example, independent claims 1 and 15 require the “further information” to be provided to the first wireless device “only to the extent that” providing the information “is consistent with” the result of the comparison of an “information disclosure policy data” (associated with the identifier of the second wireless device) and “the first identification information” (associated with the first wireless device). But, as discussed herein, it was already well-known for wireless networks to use disclosure policies to limit the disclosure of information from one device to another, including specifically by deploying a server communicating with one or more wireless devices across a long-range wireless network to limit the disclosure of information provided

to a first wireless device about a second wireless device based on the disclosure policies of one or both devices.

For example, **Eagle** (Ex. 1004) discloses a known system for using a server to facilitate communications between portable communication devices. *E.g.*, Eagle Abstract, ¶[0003]. As further discussed in §IX below, an identified device uses Bluetooth to send identifying information to a requester device when they are in close proximity, and the requester device transmits that identifying information to a server using a long-range communication network. *Id.* ¶¶[0004], [0018]. The identifying information is then used by the server to retrieve “profile” data associated with the identified device, which includes privacy settings, and to determine whether to send the requester device an “alert” message containing information about the user of the identified device. *E.g.*, Eagle ¶¶[0007]; [0020]. **Eagle** further discloses that the “profile data” includes a list of devices owned by “friends” or “likely friends,” which defines a “trust network” of such devices that are allowed to receive that user’s private profile information. *E.g.*, Eagle ¶¶[0056], [0060], [0066]-[0067]. Devices outside that trust network may receive only public profile information. *E.g.*, *id.* ¶¶[0060], [0066].

As to claims 8, 14, and 22, to the extent it is argued that further disclosure is required beyond **Eagle**, **Mgrdechian** discloses limiting the requests for profile data from the first device to the server, as discussed in §IX.B.1.

Thus, and as further explained below, **Eagle** anticipates claims 1, 5-7, 10, 12, 15, 18, and 20-21 and, at minimum, renders obvious all the Challenged Claims. In addition, **Eagle** in view of **Mgrdechian** renders obvious dependent claims 8, 14, and 22. At best, the Challenged Claims of the '736 are directed to an obvious combination of prior art elements combined according to known methods to yield predictable results. *KSR Intern. Co. v. Teleflex Inc.*, 550 U.S. 398, 416 (2007). The claimed elements and the claimed arrangement of elements were anticipated by **Eagle** and, at most, the combination amounts to nothing more than a “predictable use of prior art elements according to their established functions.” *Id.* at 417.

The USPTO did not consider **Eagle**, **Mgrdechian**, or any other reference providing analogous disclosures during prosecution of the '736. Had such references been available and considered previously, the Challenged Claims would have been found unpatentable.

As explained in greater detail herein, all the features of the Challenged Claims were known well before the earliest possible priority date of the '736, and the purported invention is anticipated by the prior art and at most no more than an obvious combination of prior art elements combined according to known methods to yield predictable results. Petitioner requests that the Board institute trial and find the Challenged Claims unpatentable.

II. MANDATORY NOTICES (§42.8)

A. Real Party-In-Interest

Target Corporation is the real party-in-interest. No other party had access to or control over the present Petition, and no other party funded or participated in preparation of the present Petition. Proxicom asserts in the litigation that Petitioner infringes the '736 by utilizing instrumentalities provided at least in part by Acuity Brands (“Acuity”), but Acuity has not and is not funding, controlling, directing, or otherwise involved in this petition or proceeding.

B. Related Matters

Proxicom Wireless, LLC v. Target Corporation, No. 6:19-cv-1886-Orl-37LRH (M.D. Fla.) (pending).

The following table lists matters regarding related patents:

Patent No.	IPR
9,038,129	IPR2020-00903

A. Lead and Back-Up Counsel and Service Information

James L. Davis, Jr. (Reg. No. 57,325) (Lead)

ROPES & GRAY LLP

1900 University Avenue, 6th Floor

East Palo Alto, CA 94303-2284

Phone: 650-617-4000

Fax: 617-235-9492

james.l.davis@ropesgray.com

Target-Proxicom-IPR-Service@ropesgray.com

Cassandra Roth (Reg. No. 73,747)
Ropes & Gray LLP
1211 Avenue of the Americas
New York, NY 10036-8704
Phone: (212) 596-9000
Cassandra.Roth@ropesgray.com

Customer No. 28120

Mailing address for all PTAB correspondence:
ROPES & GRAY LLP, IPRM—Floor 43
Prudential Tower, 800 Boylston Street,
Boston, MA 02199-3600

Petitioner consents to electronic service of documents to the email addresses of the counsel identified above.

III. PAYMENT OF FEES

The undersigned authorizes the Office to charge the fee required by §42.15(a) and any additional fees to Deposit Account No. 18-1945, under Order No. 001008-0037-658.

IV. REQUIREMENTS FOR INTER PARTES REVIEW

A. Grounds for Standing

Pursuant to §42.104(a), Petitioner certifies that the '736 is available for IPR. Petitioner is not barred or estopped from requesting IPR challenging the claims of the '736 on the grounds identified herein.

B. Identification of Challenge

Pursuant to §42.104(b), Petitioner requests IPR of claims 1, 5-8, 10, 12, 14-15, 18, and 20-22 of the '736, and that the Board cancel the same as unpatentable. The '736 matured from U.S. Application 12/364,897 (filed 2/3/2009) and claims priority to U.S. Provisional Application 61/095,359 (filed 9/9/2008) and U.S. Provisional Application 61/095,001 (filed 9/8/2008).²

1. The Specific Art on Which the Challenge is Based

Petitioner relies upon the following prior art:

Name	Exhibit	Patent/ Publication	Filed	Issued/ Published	Prior art under at least
Eagle³	1004	U.S. 2005/0250552	5/5/2005	11/10/2005	§102(b)
Mgrdechian⁴	1005	U.S. 7,545,784	2/10/2005	6/9/2009	§102(e)

² Petitioner takes no position as to the propriety of the priority claims because the art presented herein predates the earliest possible filing of the '736 patent. Petitioner reserves the right to challenge these priority claims.

³ Eagle issued as U.S. Patent 7,877,082 (prior art under §102(e)). Ex. 1022.

⁴ Mgrdechian was also published as U.S. 2005/0174975 (prior art under §102(b)). Ex. 1023.

These references were not cited in an Information Disclosure Statement (“IDS”) or otherwise identified by the Examiner, or applied in a rejection of the claims during prosecution of the ’736. The Examiner never considered the grounds presented herein or the testimony of Petitioner’s expert David H. Williams (“Williams,” Ex. 1003) regarding the scope and content of the prior art. *See* Ex. 1002. Because the presented grounds are not cumulative of any prior art previously considered, and are not the same or substantially the same as prior art or arguments previously considered, the Board should not exercise its discretion under §325(d). Co-pending district court proceedings also do not warrant the exercise of discretion under §314(a). *See, e.g., Precision Planting, LLC v. Deere & Company*, IPR2019-01044, Paper 17, *9-18. Applying the factors from *Apple Inc. v. Fintiv, Inc.*, IPR2020-00019, Paper 11 (Mar. 20, 2020), the Board should not exercise its discretion to deny institution under §314(a): (1) the district judge before whom this case is pending has granted every post-institution motion to stay that Petitioner has found (Exs. 1016-1019); (2) this case was filed on 10/2/2019; and while trial is currently set for 9/7/2021, it may be delayed due to a variety of factors including those relating to COVID-19; (3) the litigation is in its early stages and Petitioner did not delay in filing this Petition—the court has not ruled on Petitioner’s motion to dismiss or any substantive issue relating to the ’736, PO served its infringement contentions on 2/10/2020, identifying over 120 claims at issue in the litigation, PO

has refused to reduce the number of asserted claims, which would have also narrowed the number of claims challenged before the Board, and PO has not yet responded to Petitioner’s invalidity contentions in the litigation; (4) in addition to the claims asserted in the litigation, the petition challenges some claims not asserted in the litigation; (5) the litigation and PTAB parties are the same; and (6) as demonstrated herein, the merits of the grounds raised and public policy favor institution—the Challenged Claims are anticipated, and at minimum rendered obvious, by art that the USPTO never considered during prosecution, and PO has indicated that it intends to continue to assert this patent against numerous other defendants (Ex. 1020). This IPR should be instituted.

2. Statutory Grounds on Which the Challenge is Based

Ground	References	Basis	Claims
1	Eagle	§102	1, 5-7, 10, 12, 15, 18, and 20-21
2		§103	1, 5-8, 10, 12, 14-15, 18, and 20-22
3	Eagle in view of Mgrdechian	§103	8, 14, and 22

3. How the Challenged Claims Are Unpatentable

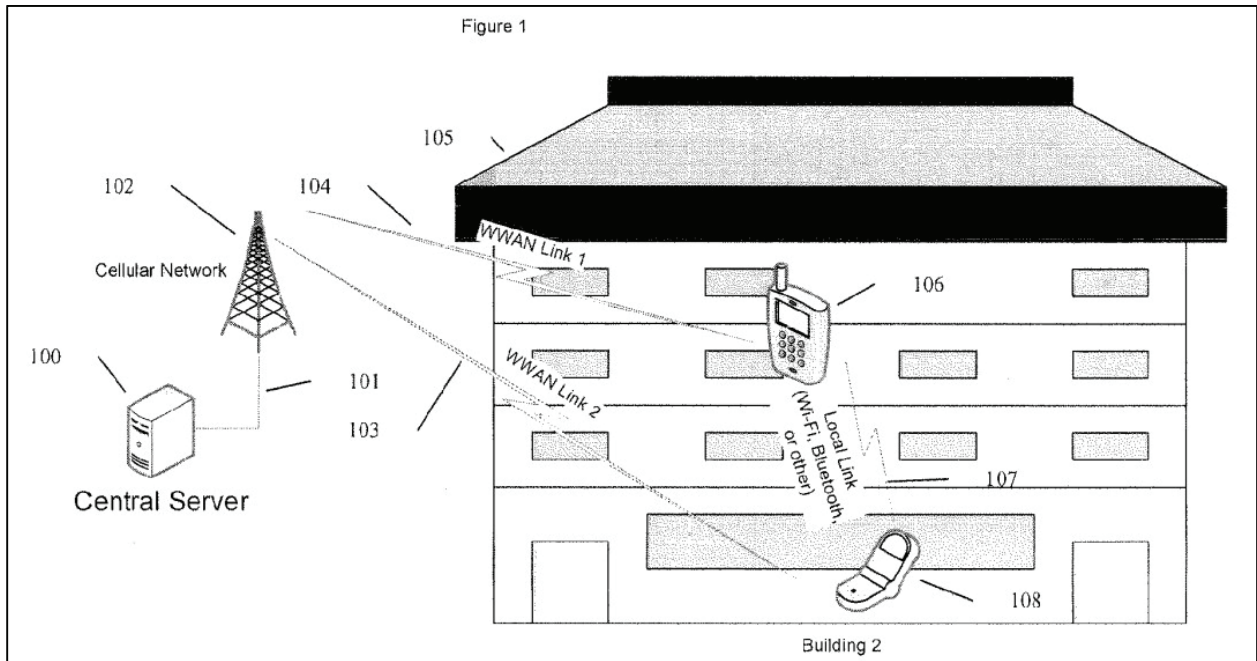
Petitioner provides the information required under §§42.104(b)(4)-(5) in

§IX.

V. THE '736 PATENT

The '736 describes techniques for using a server to broker the exchange of information between wireless devices. '736, Abstract. The background section of the '736 concedes that wireless devices, such as mobile phones, had access to both a “wide area” cellular connection, and local “Bluetooth” connections that permit “peer to peer” communications. '736, 1:24-35, 2:22-33. The '736 combines these two well-known communication methods, and describes methods for exchanging information using “both a short range and a long range wireless capability.” '736, 2:51-55. Williams ¶¶60-61.

The '736's embodiments are directed to some variant of the same general functionality: (1) send an identifier from a second device to a first device using a short-range connection between the devices; (2) communicate the received identifier from the first device to a server; and (3) determine additional information that the server should communicate back to one or both devices. For example, Figure 1 of the '736 shows that “a central server 100 is connected to devices 106 and 108” through a combination of the Internet, and a “cellular network 102.” '736, 5:42-51. The devices are also able to communicate directly with each other via “a short range wireless link 107 such as a Bluetooth.” '736, 6:31-35.



'736 Fig. 1. The '736 states that each wireless device searches for nearby devices and exchanges “wireless identifier[s]” using Bluetooth. *E.g.*, '736, 6:47-51. Rather than exchange additional information directly with each other, this received identifying information is transmitted to a “central server” using a cellular or Internet connection, and the server returns “information related to any identifier that meets certain policy requirements.” '736, 2:67-3:5, 7:66-8:4. As an example of enforcing a “policy,” the '736 states that the server returns “relevant” information that a device is “authorized to receive.” '736, 8:2-6. Williams ¶¶62-65.

The '736 states that its disclosures can be used for “social networking” services, where the server will enforce a “pre-set policy” that allows content to be

shared with only devices included “on a friend list or belonging to a specific group or organization.” *See* ’736, 3:20-30, 4:29-47. Williams ¶66.

VI. PROSECUTION HISTORY

U.S. Patent Application 12/364,897, which matured into the ’736, was filed 2/3/2009. The originally-filed claims were generally directed to “a central server” utilizing one or more “Wide Area Network connections to exchange information” between applications executing on one or more “wireless devices,” where the central server receives, across the wide area link, “information...collected by a first wireless device from a second wireless device” using a separate “local wireless link,” and wherein that information is associated with one or more of: (a) “an identifier for an entity associated with the second wireless device”; (b) “behavior preferences of an entity” associated with an application running on either wireless device; or (c) “an identifier” for either device. ’736 FH (Ex. 1002), 47. Williams ¶¶67-68.

The Examiner issued a Notice of Allowance on 1/5/2011, following an interview with Applicant on 12/17/2010, allowing and re-ordering claims 1-5 and 7-24 (issued claims 1-23), subject to an Examiner’s amendment, and cancelling claim 6. ’736 FH, 98-111. The amendment required the server to (i) receive from the first wireless device “first identification information” that is associated with the first wireless device and “second identification information” that is associated with the second wireless device; (ii) “retriev[e] disclosure policy data” associated with the

second device “representing rules for privacy of information”; (iii) “compar[e] the information disclosure policy data and the first identification information”; and (iv) “provid[e] further information” to the first device about an entity associated with the second device “only to the extent that it is consistent with” the “disclosure policy data.” *Id.*, 102-103; Williams ¶69

The Applicant subsequently filed a post-allowance amendment on 1/24/2011, amending dependent claims 8, 15, 17, and 20 (issued claims 8, 20, 22, and 11, respectively) to make them “consistent with the specification and with one another.” *Id.*, 126-133. The Examiner issued a Supplemental Notice of Allowance on 4/4/2011 allowing all pending claims. *Id.*, 169. No explanation was provided for allowance. *Id.* The ’736 patent issued 5/3/2011. Williams ¶70.

VII. LEVEL OF ORDINARY SKILL

A person of ordinary skill in the art (“POSITA”) on or before 9/8/2008, would have had a minimum of a Bachelor’s degree in Electrical Engineering, or a related field, and approximately 3-5 years of professional experience in the field of wireless communications. Additional graduate education could substitute for professional experience, or significant experience in the field could substitute for formal education. Williams ¶¶36-38.

VIII. CLAIM CONSTRUCTION

Terms of claims subject to IPR are to be “construed using the same claim construction standard that would be used to construe the claim in a civil action under §282(b), including construing the claim in accordance with the ordinary and customary meaning of such claim as understood by one of ordinary skill in the art and the prosecution history pertaining to the patent.” §42.100(b). Only terms necessary to resolve the controversy need to be construed. *Nidec Motor v. Zhongshan Broad Ocean Motor*, 868 F.3d 1013, 1017 (Fed. Cir. 2017).

For review purposes, Petitioner interprets the claim terms according to their plain and ordinary meaning consistent with the specification.

While the Challenged Claims use terms of degree (e.g., “Wide Area Network,” “local wireless link”), the prior art relied on herein discloses the ’736’s examples of those terms as shown in §IX.A below. *See, e.g.*, ’736, 2:10-16 (“cellular wireless wide area network connection (WWAN) ... such as CDMA (IS-2000), GSM, W-CDMA, WiMax, etc.”), 5:59-63 (“Communications network(s) providing the connection 101 can typically be part of a remote access network, a global network (e.g., the Internet), a worldwide collection of computers...”), 17:45-47 (“The device detects a broadcast device, and interacts over the internet with the server via the WWAN connection...”), 19:43-45 (“a local, or personal area network wireless protocol such as ... Bluetooth”) (emphasis added). Williams ¶¶72-76.

Likewise, regardless of the scope of a central server exchanging information between one application (as recited in “a central server utilizing one or more wireless Wide Area Network connections to exchange information between one or more applications executing on first and second wireless devices” (claims 1 and 15)), the prior art relied on herein expressly discloses a central server exchanging information between applications running on a first and second wireless device as shown in §IX.A below. Williams ¶77.

A district court in another proceeding has construed terms in related patents, but these constructions do not impact the outcome of this IPR. *See* Ex. 1021.

IX. GROUNDS OF UNPATENTABILITY

The '736 is directed to a method and system for facilitating communications between two wireless devices through a server. At their core, the claims are directed to (1) sending an identifier from a second wireless device to a first wireless device using a short-range connection; (2) communicating the identifier from the first wireless device to a server; (3) comparing a “disclosure policy” for the second wireless device with an identifier associated with the first wireless device; and (4) providing “further information” about the second wireless device to the first wireless device, but “only to the extent that it is consistent with the... disclosure policy.” Claims 1, 5-7, 10, 12, 15, 18, and 20-21 are anticipated and, at minimum, all

Challenged Claims are obvious in view of the prior art cited herein, as explained below. Williams ¶¶102-103.

For example, **Eagle** discloses a system for using a server to facilitate communications between Bluetooth-enabled devices. **Eagle** discloses all the claimed features of '736 claims 1, 5-7, 10, 12, 15, 18, and 20-21, including wireless devices that exchange “identifiers” using a short-range Bluetooth connection, and a server that will receive the identifiers from the devices, retrieve user preferences and disclosure policies, and transmit back information consistent with those policies.

As to claims 8, 14, and 22, Eagle renders these claims obvious. To the extent it is argued that further disclosure is required beyond **Eagle**, **Mgrdechian** discloses limiting unnecessary requests for profile data from the first device to the server based on whether the information is already available at the first device, as discussed in §IX.B.1.

As shown below, the prior art renders the Challenged Claims of the '736 unpatentable. This Petition is supported by the Declaration of David Williams, which describes the scope and content of the prior art at the time of the alleged invention of the '736. Williams ¶¶36-200.

A. Grounds 1-2: Claims 1, 5-8, 10, 12, 14-15, 18, 20-22

As further set forth below, claims 1, 5-7, 10, 12, 15, 18, and 20-21 are anticipated by Eagle and claims 8, 14 and 22 are rendered obvious by Eagle.

However, as further described below for particular limitations, to the extent it is argued that further evidence is required for those limitations, a POSITA would have found the limitations obvious in view of *Eagle*—rendering all Challenged Claims obvious.

1. Overview of *Eagle*

Eagle teaches a system for using a server to facilitate communications between portable wireless communication devices. *E.g.*, *Eagle* Abstract, ¶[0003]. As further discussed below, the devices exchange identifying information using Bluetooth when they are in close proximity. *E.g.*, *Eagle* ¶[0018]. The identifying information received by a requester device (a first wireless device) from an identified device (a second wireless device) is transmitted to a server using a long-range communication network, and is used to retrieve “profile” data associated with the devices, which includes privacy settings. *E.g.*, *Eagle* ¶¶[0005], [0050]. The server then uses the profile data to determine whether the server should send each device an “alert” message containing information about the owner of the other nearby device. *E.g.*, *Eagle* ¶¶[0007], [0020]. *Williams* ¶¶82-83.

As shown in Figure 2 below, **Eagle** discloses that a “first Bluetooth phone” (the requester device – blue) identifies a nearby “second Bluetooth phone” (the identified device – yellow) and receives a unique “Bluetooth device ID” via a Bluetooth link (represented in green). *E.g.*, *Eagle* ¶¶[0008], [0022]. In a preferred

embodiment, this device ID is the Bluetooth Device Address (BD_ADDR) for the device. *E.g.*, Eagle ¶¶[0003], [0031]. The first Bluetooth phone then transmits a “notification message,” which contains both its “own ID value (the Requester ID)” and “the ID value of the newly arrived other device (the Identified ID)” to a “remote server” (purple) via a “cellular phone network” (represented in red). *E.g.*, Eagle ¶¶[0004], [0020] [0048]. The server then uses the ID values to retrieve “profile data” for the requester device and the identified device, and determines whether an “alert” should be sent to one or both devices. *E.g.*, Eagle ¶¶[0005], [0020].

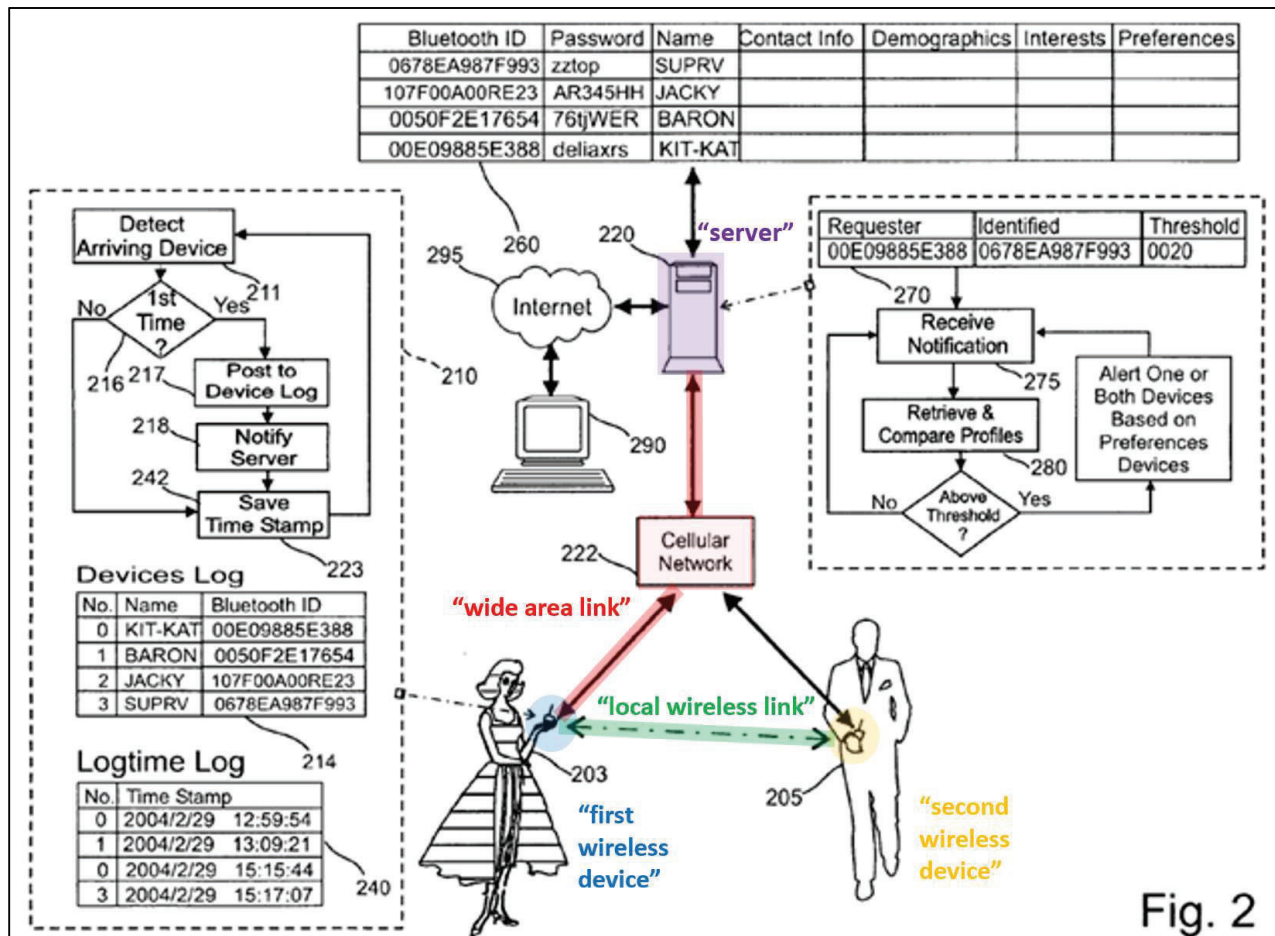


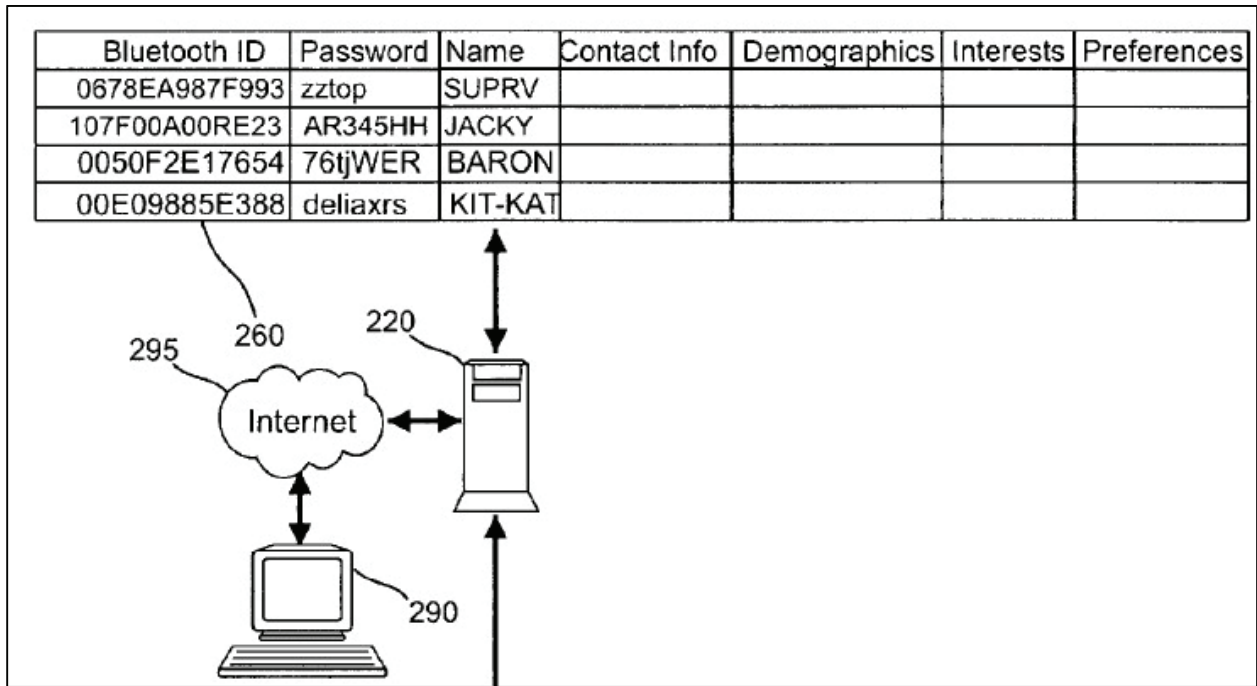
Fig. 2

Eagle, Fig. 2; Williams ¶¶84-86.

Eagle discloses that “[e]ach cellular phone keeps a log of other devices that have been previously detected and, whenever a new device comes within range, a notification message is transmitted to a remote server via the long-range cellular phone network.” Eagle [0004], [0023]. A POSITA would have found it to be an obvious implementation choice for the requester device to continue to transmit to the server such a notification message until an alert message is returned for the identified device. Williams ¶87. This would ensure that a user receives up-to-date information about nearby devices reflecting the user’s most current preferences. *Id.* **Eagle** teaches transmitting an alert message when a comparison of the profiles for the requester device and the identified device exceeds a threshold set by the user. Eagle ¶¶[0048]-[0049]. That threshold is reset with each notification message sent to the server. *Id.* ¶¶[0049], [0055]. A POSITA would have understood that, because each user can re-set the threshold with each notification request and can regularly update her profile, a notification request from the same requester device containing the identifier of the same identified device may not result in an alert message on a first try, but may result in an alert message on a second try if either the threshold or a profile is changed in the interim. Eagle ¶¶[0006], [0045], [0049], [0052]; Williams ¶141. Thus, a POSITA would have been motivated to continue sending notification messages, even if the first notification message had already been sent, until an alert

message is received from the server with information relating to the identified (second) device, subject to the second device's disclosure policy. Williams ¶¶141-142. A POSITA would have been further motivated to do so particularly in light of Eagle's goals of "facilitat[ing] communications between the devices *when appropriate*" and its recognition that alerts may be appropriate at some times but not at others. *Id.*; Eagle ¶¶Abstract, [0054], [0059].

Eagle discloses that "profile data" for each of the devices is stored in "database 260" accessible by the server. *E.g.*, Eagle ¶¶[0005], [0050]-[0051]. A user's profile data is set by the user through a secure website. *E.g.*, Eagle ¶[0048]. As shown in the portion of Figure 2 below, the profile data includes a device identifier, a name and password associated with the device, contact and demographic information for the owner of the device, a list of "interests," and privacy setting in the form of "preference data indicating, for example, the extent to which other information [in] the profile is sharable, and under what circumstances." Eagle ¶[0050].



Eagle, Fig. 2 (partial); Williams ¶¶88.

Eagle also discloses that the “profile data” includes a list of devices owned by “friends” or a stored list of “likely friends” automatically generated by analyzing past interactions between devices and the server. *E.g.*, Eagle ¶¶[0056], [0067]. The friends list defines a “trust network” of devices that a user is willing to share private information with, as opposed to the “public” profile accessible to anybody. *E.g.*, Eagle ¶¶[0056], [0060], [0066]-[0067]. For example, **Eagle** teaches that a device can be set to establish links with only another user’s device that is “within one degree from an individual’s social circle, i.e.: a friend-of-a-friend.” Eagle ¶[0066]. Williams ¶¶89-90.

Once the server retrieves the profiles, it “compare[s]” the profiles and determines whether to send an “alert message” to one or both devices. *E.g.*, Eagle ¶¶[0005], [0020], [0051]; Williams ¶91. As discussed above, **Eagle** discloses that certain alerts may be sent to only devices within a trust network, based on the profile data. *E.g.*, Eagle ¶¶[0056], [0060], [0066]. A POSITA would have understood that to determine whether to send an alert, the requester device’s ID (the Requester ID) is compared to the “trust network” (“a set of device IDs”) of the identified device because the Requester ID is used to identify the requester device. Eagle ¶¶[0050], [0056], [0066]; Williams ¶121. To the extent it is argued that further disclosure is required, it would have been obvious to make this determination using the device IDs to retrieve and perform this comparison based on these well-known disclosures. Williams ¶122.

A POSITA would have further understood that a data processor in the server performs these steps of retrieving profiles and performing the comparison, given Eagle’s reliance on a standard server to perform these functions. Williams ¶92. To the extent it is argued that further disclosure is required, it would have been obvious to implement the server using a “data processor” to retrieve the profiles and perform the comparison based on these well-known disclosures. *Id.* It would have been well known to a POSITA that servers make use of data processors, and it would have been an obvious design choice to include such a processor in the server. *Id.* Indeed,

the '736 specification admits that data processors were “well known in the art”: “[t]he internal structure of...server 100 includes one or more data processors (not shown in detail) that are well known in the art” ’736, 5:66-6:4.

Eagle is in the same field of art and is analogous art to the ’736—both are in the same field related to facilitating communications between wireless devices. E.g., ’736, 2:51-55 (“The present invention is generally concerned with facilitating the exchange of information and transactions between two entities associated with two wireless devices when the devices are in close proximity to each other utilizing both a short range and a long range wireless capability.”); Eagle Abstract (“Portable communication devices, such as Bluetooth enabled cellular phones, communicate with and identify like devices that are nearby, and send notification messages to a remote server ... [that] facilitates communications between the devices when appropriate.”); Williams ¶94.

In addition, Eagle is also reasonably pertinent to the alleged problem(s) identified in the ’736 of overcoming the inaccuracies of GPS systems, and avoiding the security and privacy concerns of direct peer-to-peer communications. E.g., ’736, 2:35-43 (“[A]ny policy for the delivery of locally stored content is difficult to enforce without the potential for fraud such as spoofing identities between the peers. Such fraud may lead to concerns of personal safety or privacy....”), 3:56-60 (“GPS will often not operate indoors or where the GPS signal is weak. Using a peer to peer

detection process to locate nearby devices allows for the operation of proximity detection indoors.”); Eagle ¶[0008] (“[P]ortable wireless electronic devices that incorporate Bluetooth transceivers that can be used as beacons....Such personal beacon system offer *better short range spatial resolution for proximity detection than do absolute location systems, such as GPS* and cellular phone location systems. The fact that the beacons transmit only device identification codes *avoids some privacy problems* since these codes do not contain information about the users.”); Williams ¶95.

As further discussed below, Eagle anticipates claims 1, 5-7, 10, 12, 15, 18, and 20-21 and, at minimum, renders obvious each of the Challenged Claims. Williams ¶101.

2. Claim Chart—Eagle

Claim Element	Eagle
<p>[1.pre] A method for a central server utilizing one or more wireless Wide Area Network connections to exchange information between one or more applications executing on first and second wireless devices, the central</p>	<p>Eagle discloses a method for a central server (e.g., “server”) utilizing one or more wireless Wide Area Network connections (e.g., “large area wireless network such as a cellular phone network and/or the Internet”) to exchange information between one or more applications (e.g., “BlueAware”) executing on first and second wireless devices (e.g., “Bluetooth enabled cellular phones, communicate with and identify like devices that are nearby,” a “requester” and an “identified” device).</p> <p><u>E.g., Eagle:</u></p> <p>Eagle discloses wireless “portable communication devices” that exchange information using the “BlueAware” program running on each device. E.g.,</p>

Claim Element	Eagle
server performing the steps of:	<p>Eagle Abstract, ¶[0019]. Devices (e.g., a requester device (the first wireless device) and the identified device (the second wireless device)) identify themselves by exchanging unique identification codes, which are transmitted to a “remote server” over a cellular phone network to facilitate additional communications. Eagle Abstract, ¶[0010], [0048].</p> <ul style="list-style-type: none"> • Abstract (“Portable communication devices, such as <i>Bluetooth enabled cellular phones, communicate with and identify like devices</i> that are nearby, and send notification messages to a <i>remote server</i>. When a notification message is received at the server identifying two devices that have come within range of one another, <i>the server compares the profile data associated with each of the two identified devices and facilitates communications between the devices</i> when appropriate.”) • [0010] (“<i>The preferred embodiment of the present invention described in more detail below uses personal area wireless network devices such as Bluetooth transceivers to identify social proximity and a large area wireless network such as a cellular phone network and/or the Internet, to permit interest matching functions to be performed at a remote central server and to instigate person-to-person interactions between selected devices that are near to each other and/or between their users.</i>”) • [0019] (“Each of these Bluetooth enabled cellular phones includes a processor that is specially programmed with <i>an application program, called “BlueAware,” that enable the cellular phone to identify and log the presence of other “discoverable” Bluetooth devices that are nearby, and to display an identification of those devices on the cell phone's screen as illustrated in FIG. 1a.</i>”)

Claim Element	Eagle
	<ul style="list-style-type: none"> • [0020] (“Each of these cellular phones is further programmed to <i>generate a notification message identifying itself, and other Bluetooth devices that come within its range</i>, as well as additional status information. The application program that executes on the cellular phone processor then <i>transmits that notification message via the long-range cellular network to a remote central server.</i>”) • [0048] (“...As illustrated at 270 in FIG. 2, <i>each notification message sent from a device to the server includes not only its own ID value (the Requester ID) and the ID value of the newly arrived other device (the Identified ID).</i>...”) <p>See also Eagle ¶¶[0004], [0009]-[0010], [0022], [0049], [0051].</p> <p>Williams ¶¶104-106.</p>
<p>[1.a] receiving first identification information from the first wireless device, the first identification information communicated from the first wireless device to the server via the wireless Wide Area Network,</p>	<p>Eagle discloses the central server receiving first identification information (e.g., “Requester ID”) from the first wireless device (e.g., “each notification message sent from a device to the server includes...its own ID value (the Requester ID)...”), the first identification information communicated from the first wireless device to the server via the wireless Wide Area Network (e.g., “large area wireless network such as a cellular phone network and/or the Internet”).</p> <p><u>E.g., Eagle:</u></p> <p>Eagle discloses that, each time a requester device detects a “new device,” it communicates to a server, using a “long-range cellular network,” a notification message containing its own identifier (“Requester ID”).</p> <ul style="list-style-type: none"> • [0004] (“[W]henver a new device comes within range, <i>a notification message is transmitted to a remote server via the long-range cellular phone network. The notification message contains an</i>

Claim Element	Eagle
	<p><i>identification of both the requesting device and the nearby device whose presence has been detected.”)</i></p> <ul style="list-style-type: none"> • [0020] (“Each of these cellular phones is further programmed to <i>generate a notification message identifying itself, and other Bluetooth devices that come within its range</i>, as well as additional status information. The application program that executes on the cellular phone processor then <i>transmits that notification message via the long-range cellular network to a remote central server.</i>.”) • [0031] (“<i>Bluetooth devices are identified by a unique identification code values</i>. Each Bluetooth device is specified by a unique 48-bit Bluetooth Device Address (BD_ADDR)...”) • [0048] (“...As illustrated at 270 in FIG. 2, <i>each notification message sent from a device to the server includes not only its own ID value (the Requester ID) and the ID value of the newly arrived other device (the Identified ID).</i>...”) <p><i>See also Eagle ¶¶[0003], Claim 2, Fig. 2. Williams ¶¶107-108.</i></p>
<p>[1.b] wherein the first identification information is associated with one or more of an identifier of the first wireless device or an entity associated with the first wireless device,</p>	<p>Eagle discloses wherein the first identification information (e.g., “Requester ID”) is associated with one or more of an identifier of the first wireless device or an entity associated with the first wireless device (e.g., “the profile database contains, for each Bluetooth device: (a) the Bluetooth identification value BTID for that device ... (c) a short name for the device or its user”).</p> <p><u>E.g., Eagle:</u> See [1.a].</p> <p>In addition, Eagle discloses that each device’s identification information (e.g., a “Bluetooth identification value BTID”) is part of the device’s “profile data,” which</p>

Claim Element	Eagle
	<p>also includes a “name” for the device or its user. Eagle ¶¶[0050]. Thus, the “Requester ID” is associated with the name of the requester device or its user. <i>Id.</i>; Eagle ¶¶[0048].</p> <ul style="list-style-type: none"> • [0005] (“Profile data that describes each device and its owner is stored in a database. <i>When a notification message is received identifying two devices that have come within range of one another, the server fetches the profile data associated with each of the two identified devices and performs a comparison.</i>”) • [0031] (“<i>Bluetooth devices are identified by a unique identification code values. Each Bluetooth device is specified by a unique 48-bit Bluetooth Device Address (BD_ADDR)...</i>”) • [0050] (“As shown in FIG. 2 at 260, the profile database contains, <i>for each Bluetooth device: (a) the Bluetooth identification value BTID for that device; ... (c) a short name for the device or its user (which need not be same name as the “device name” stored in the Bluetooth device)...</i>”) <p><i>See also</i> Eagle ¶¶[0020], [0029], [0045]. Williams ¶¶109-110.</p>
<p>[1.c] receiving second identification information, as collected by the first wireless device from the second wireless device via a separate local wireless link between the first and second wireless</p>	<p>Eagle discloses receiving second identification information (e.g., “Identified ID”), as collected by the first wireless device from the second wireless device via a separate local wireless link between the first and second wireless devices (e.g., “When a device is within range of another such device, it identifies itself with unique identification value, such as a Bluetooth device address value,” using “Bluetooth”), and wherein the second identification information is communicated from the first wireless device to the server (e.g., “each notification message sent from a device to the server includes...the ID value of the newly arrived other device</p>

Claim Element	Eagle
<p>devices, and wherein the second identification information is communicated from the first wireless device to the server via the wireless Wide Area Network connection,</p>	<p>(the Identified ID)”) via the wireless Wide Area Network connection (e.g., see [1.a]).</p> <p><u>E.g., Eagle:</u></p> <p>See [1.a].</p> <p>In addition, Eagle discloses that devices exchange identification codes using a Bluetooth short-range wireless link. Eagle ¶¶[0003], [0018], [0031]. Each device receives the identification code for another device (“Identified ID”) and includes it in the notification message sent to a server using a “long-range cellular network.” Eagle ¶¶[0004], [0020], [0048]. Thus, the requester device receives the Identified ID from the identified device and sends the Identified ID to the server.</p> <p><i>Id.</i></p> <ul style="list-style-type: none"> • [0003] (“When a device is within range of another such device, <i>it identifies itself with unique identification value</i>, such as a Bluetooth device address value.”) • [0004] (“[W]henever a new device comes within range, a notification message is transmitted to a remote server via the long-range cellular phone network. <i>The notification message contains an identification of both the requesting device and the nearby device whose presence has been detected.</i>”) • [0018] (“people who use the system are provided with <i>cellular telephones which incorporate short range radio transceivers that use the Bluetooth protocol to detect other nearby Bluetooth enabled devices.</i>”) • [0020] (“Each of these cellular phones is <i>further programmed to generate a notification message identifying itself, and other Bluetooth devices that come within its range</i>, as well as additional status information. The application program that executes

Claim Element	Eagle
	<p>on the cellular phone processor <i>then transmits that notification message via the long-range cellular network to a remote central server.</i>”)</p> <ul style="list-style-type: none"> • [0048] (“...As illustrated at 270 in FIG. 2, <i>each notification message sent from a device to the server includes</i> not only its own ID value (the Requester ID) and <i>the ID value of the newly arrived other device (the Identified ID).</i>...”) <p><i>See also</i> Eagle ¶[0031], Claims 2-3, Fig. 2. Williams ¶¶111-113.</p>
<p>[1.d] wherein the second identification information is associated with one or more of an identifier of the second wireless device or an identifier of an entity associated with the second wireless device;</p>	<p>Eagle discloses wherein the second identification information (e.g., “Identified ID”) is associated with one or more of an identifier of the second wireless device or an identifier of an entity associated with the second wireless device (e.g., “the profile database contains, for each Bluetooth device: (a) the Bluetooth identification value BTID for that device ... (c) a short name for the device or its user”).</p> <p><u>E.g., Eagle:</u> See [1.b]-[1.c].</p> <p>In addition, Eagle discloses the “Identified ID” is associated with the name of the identified device or its user. Eagle ¶¶[0048], [0050]. Williams ¶¶114-115.</p>
<p>[1.e] retrieving disclosure policy data associated with the second identification information, the disclosure policy data representing rules for privacy of information</p>	<p>Eagle discloses the central server retrieving disclosure policy data associated with the second identification information (e.g., “The two BTID values [the Requester ID and the Identified ID in the notification message] are used to fetch corresponding profile data from the database 260;” “profile data” in “[p]rofile database” “contains ... the Bluetooth identification value BTID for that device”), the disclosure policy data representing rules for privacy of information concerning the second wireless device or privacy of information concerning an entity</p>

Claim Element	Eagle
<p>concerning the second wireless device or privacy of information concerning an entity associated with the second wireless device;</p>	<p>associated with the second wireless device (e.g., “the profile database contains ... preference data indicating, for example, the extent to which other information [in] the profile is sharable, and under what circumstances,” “device ... set to only establish potential links to others within a 'trust network'”).</p> <p><u>E.g., Eagle:</u></p> <p>See [1.b], [1.d].</p> <p>In addition, Eagle discloses that the server receives the notification message with the device identifiers, and retrieves the corresponding “profiles.” Eagle ¶[0005]. The “profile data” associated with each device includes “the Bluetooth identification value BTID for that device,” demographic information, a “friends” list, and user “preference[s]” dictating what information may be shared with other devices and when. Eagle ¶¶[0005], [0050], [0056], [0057]. Each device is “set to only establish potential links to others within a 'trust network.’” Eagle ¶[0066]. Thus, the identified device’s “profile” is retrieved using the Identified ID and its “preferences” and “trust network” in the profile data represent rules for privacy of information concerning the device and its user.</p> <ul style="list-style-type: none"> • [0005] (“Profile data that describes each device and its owner is stored in a database. <i>When a notification message is received identifying two devices that have come within range of one another, the server fetches the profile data associated with each of the two identified devices and performs a comparison. ...</i>”) • [0050] (“As shown in FIG. 2 at 260, the profile database contains, for each Bluetooth device: (a) the Bluetooth identification value BTID for that device; ... (f) weighting values associated with individual items of demographic or interest data indicating the level of importance that user attached to each

Claim Element	Eagle
	<p>category of data; and (f) [sic] <u>other preference data indicating, for example, the extent to which other information [in] the profile is sharable and under what circumstances.</u>")</p> <ul style="list-style-type: none"> • [0056] (“The profile data for each user may advantageously include data specifying a set of device IDs for devices owned by “friends.” ... <u>A given user may then request that alert messages be sent only when such a “trusted” person having common interests is nearby.</u> ...”) • [0057] (“<u>Each user may also set the extent to which information will be provided to requesters.</u> For example, a user may indicate that interest categories may be revealed to others, but not name and address information. The degree to which information is revealed by be varied by transmitting a threshold value which contains not only an indication of the extent to which profiles should match but which also contains a “mode” value for the device. <u>The mode value may indicated vary the content of the profile data which is communicated to others in alert messages or requested from the server by a device which has another device’s Bluetooth ID in its devices log...</u>”) • [0066] (“<u>The system allows for a large variation in the privacy constraints for these applications. ... A device can also be set to only establish potential links to others within a ‘trust network’.</u>”) <p>See also Eagle ¶¶[0004], [0007], [0012], [0041], [0051]. Williams ¶¶116-118.</p>
[1.f] comparing the information disclosure policy data and the first	<p>Eagle discloses the central server comparing the information disclosure policy data and the first identification information (e.g., “device ... set to only establish potential links to others within a 'trust network'”).</p>

Claim Element	Eagle
identification information; and	<p><u>E.g., Eagle:</u> <i>See [1.e].</i></p> <p>In addition, Eagle discloses that when determining what information in the identified device’s “profile is sharable, and under what circumstances,” the server determines whether the requester device is within the identified device’s “trust network.” Eagle ¶¶[0050], [0056], [0066]. A POSITA would have understood that to make this determination the requester device’s ID (the Requester ID) is compared to the “trust network” (“a set of device IDs”) of the identified device because the Requester ID is used to identify the requester device, and, at minimum, would have found it obvious to do so for this same reason as discussed in §IX.A.1. Eagle ¶¶[0050], [0056], [0066]; Williams ¶123.</p> <ul style="list-style-type: none"> • [0050] (“As shown in FIG. 2 at 260, <i>the profile database contains, for each Bluetooth device: (a) the Bluetooth identification value BTID for that device...</i>”) • [0056] (“<i>The profile data for each user may advantageously include data specifying a set of device IDs for devices owned by “friends.”</i> The server may then identify persons who are “friends of friends” or “friends of friends of friends”. <i>A given user may then request that alert messages be sent only when such a “trusted” person having common interests is nearby.</i> Moreover, the alert message may contain an identification of mutual friends, providing an easy way to start a conversation...”) • [0066] (“<i>The system allows for a large variation in the privacy constraints for these applications. ... A device can also be set to only establish potential links to others within a ‘trust network’. Users become part of a trust network when they are within</i>”)

Claim Element	Eagle
	<p><i>one degree from an individual's social circle, i.e.: a friend-of-a-friend. ...[A] user can have the option of setting his or her profile to 'public'. ...")</i></p> <ul style="list-style-type: none"> • [0067] (“...[B]y processing proximity data, <i>a given user’s profile may be further populated with inferred data, such as one or more automatically created lists of likely friends and acquaintances that can be used to create a trust network</i> as noted above.”) <p>See also Eagle, ¶[0005]. Williams ¶¶119-123.</p>
<p>[1.g] providing further information to the first wireless device concerning the entity associated with second wireless device, but only to the extent that it is consistent with the step of comparing the information disclosure policy data.</p>	<p>Eagle discloses the central server providing further information to the first wireless device concerning the entity associated with second wireless device (e.g., “the remote server sends an alert message to one or both of the two identified nearby devices,” “alert messages ... sent only when such a “trusted” person having common interests is nearby”), but only to the extent that it is consistent with the step of comparing the information disclosure policy data (e.g., “user may also set the extent to which information will be provided to requesters”; “Certain trusted devices may have profile information attributes set that entitle them to receive profile data from the server relating to a nearby individual that would not be available to the general public.”).</p> <p><u>E.g., Eagle:</u> See [1.f].</p> <p>In addition, Eagle discloses that the “server” compares the profile data for the requester and identified devices to determine whether to communicate an “alert message” to the requester device, which contains information about the entity associated with the identified device such as contact information, a photograph, or a list of mutual interests. <i>E.g., Eagle ¶¶[0007], [0020]. Whether an alert message is</i></p>

Claim Element	Eagle
	<p>sent, and the content of the alert message, is based on whether the requester device is in the “trust network” of the identified device. Eagle ¶¶[0056]-[0057], [0060], [0066]-[0067].</p> <ul style="list-style-type: none"> • [0007] (“<u>The alert message sent to each device from the server may contain information describing the nearby device</u> to the extent the owner of that device has consented to its being revealed.... The alert message may include information identifying an encountered device or its owner, such as <u>name, address or other contact information, a photograph or other descriptive image, demographic data, data indicating the interests of the owner of the device, or any other information which is of use in a specific application may be of use to identify, or promote communications</u> between, nearby devices and their owners.”) • [0020] (“When the remote server receives a notification message indicating that two identified devices are within Bluetooth range of one another, and <u>further determines that the profile data associated with these two devices satisfies a specified matching criteria, the remote server sends an alert message to one or both of the two identified nearby devices.</u>”) • [0057] (“<u>Each user may also set the extent to which information will be provided to requesters.</u> For example, a user may indicate that interest categories may be revealed to others, but not name and address information. The degree to which information is revealed by be varied by transmitting a threshold value which contains not only an indication of the extent to which profiles should match but which also contains a “mode” value for the device. <u>The mode value may indicated vary the content of the profile data which is communicated to others in</u>

Claim Element	Eagle
	<p><u>alert messages or requested from the server by a device which has another device’s Bluetooth ID in its devices log...</u>)</p> <ul style="list-style-type: none"> • [0060] (“<u>Certain trusted devices may have profile information attributes set that entitle them to receive profile data from the server relating to a nearby individual that would not be available to the general public.</u> These devices can act as remote extensions of the server....”) <p>Williams ¶¶124-127.</p>
<p>[5] The method of claim 1 wherein the disclosure policy data defines communication preferences for the entity associated with the second wireless device that comprise one or more of:</p> <p>... disclose my name/do not disclose my name; disclose age/do not disclose age; or do or do not disclose personal details.</p>	<p>See [1].</p> <p>Eagle discloses that the disclosure policy data defines communication preferences for the entity associated with the second wireless device (e.g., “user may also set the extent to which information will be provided to requesters”) that comprise one or more of: ... disclose my name/do not disclose my name (e.g., “a short name for ... its user”); disclose age/do not disclose age (e.g., “age”); or do or do not disclose personal details (e.g., “demographic information;” “interests”).</p> <p><u>E.g., Eagle:</u></p> <p>See [1.e].</p> <p>In addition, Eagle discloses that the profile database includes “preference data” specifying when to disclose information about the user associated with the identified device, including the user’s name, contact information, age, sex, religion, ethnicity, “interests,” or other personal details.</p> <ul style="list-style-type: none"> • [0012] (“<u>The user can also vary the mode of operation of the cellular phone to control the frequency and content of the alert messages that are transmitted</u> by the server when different devices come within range of one another.”)

Claim Element	Eagle
	<ul style="list-style-type: none"> • [0050] (“As shown in FIG. 2 at 260, the profile database contains, for each Bluetooth device:... (c) <i>a short name for the device or its user</i> (which need not be same name as the “device name” stored in the Bluetooth device); (d) <i>contact information such as mailing address, email address</i>, web site URL, fax numbers, and importantly, the cellular phone number of the device, etc.; (e) <i>demographic information describing the device or user, such as age, sex, religion, ethnicity, height, weight, or any other values</i> which are of use in performing desired matching functions; ... and (f) <i>other preference data indicating, for example, the extent to which other information [in] the profile is sharable and under what circumstances.</i>”) <p>See also Eagle ¶¶[0007], [0056]-[0057]. Williams ¶¶128-130.</p>
<p>[6] The method of claim 5 wherein the step of providing further information to the first wireless device concerning the entity associated with second wireless device is based on at least one of:</p> <p>... a list the second wireless identifier is included on;</p>	<p>See [5].</p> <p>Eagle discloses that providing further information to the first wireless device concerning the entity associated with second wireless device (e.g., “the remote server sends an alert message to one or both of the two identified nearby devices”) is based on at least one of: ... a list the second wireless identifier is included on (e.g., “A given user may then request that alert messages be sent only when such a “trusted” person having common interests is nearby;” “A device can also be set to only establish potential links to others within a 'trust network'.”)....</p> <p><u>E.g., Eagle:</u></p> <p>See [1.f]-[1.g].</p> <p>In addition, Eagle discloses sending alert messages to the requester device only if the identified device is included in a “trust network” for the requester device. Eagle ¶¶[0056],</p>

Claim Element	Eagle
	<p>[0066]. A POSITA would have understood that to make this determination the Identified ID is compared to the “trust network” of the requester device because the Identified ID is used to identify the identified device, and, at minimum, would have found it obvious to do so for this same reason as discussed in §IX.A.1. Eagle ¶¶[0050], [0056], [0066]; Williams ¶133.</p> <p>Williams ¶¶131-133.</p>
<p>[7] The method of claim 1 wherein the step of providing further information to the first wireless device concerning the entity associated with second wireless device is based on at least one of:</p> <p>... a list the second wireless identifier is included on;</p>	<p><i>See</i> [1], [6].</p> <p>Williams ¶¶134-135.</p>
<p>[8] The method of claim 1 additionally comprising: returning information to the first wireless device, as a result of the step of comparing the information disclosure policy</p>	<p><i>See</i> [1].</p> <p>Eagle renders obvious returning information to the first wireless device (e.g., “the remote server sends an alert message to” the requester device), as a result of the step of comparing the information disclosure policy data (e.g., “A given user may then request that alert messages be sent only when such a ‘trusted’ person having common interests is nearby;” “A device can also be set to only establish potential links to others within a 'trust network'.”), which causes the first wireless device to limit re-sending of identifiers already reported by the first wireless device (e.g., “[i]f it is determined at 216 that</p>

Claim Element	Eagle
<p>data, which causes the first wireless device to limit re-sending of identifiers already reported by the first wireless device.</p>	<p>a detected nearby device has newly come within range and [is] not currently identified in the Devices [Log] 214, ... a request message is sent as indicated at 218 to a remote server, seen at 220 in FIG. 2, via the cellular phone network 222”; “whenever a new device comes within range, a notification message is transmitted to a remote server via the long-range cellular phone network”).</p> <p><u>E.g., Eagle:</u></p> <p>See [1.g].</p> <p>In addition, Eagle discloses that the requester device will send a notification message to the remote server when a “new” device not on the requester device’s devices log comes within range. <i>E.g.</i>, Eagle [0023]. An alert message containing the identified device’s profile information is not sent to the requester device unless the profile data for the two devices satisfies a matching criteria. <i>E.g.</i>, Eagle ¶¶[0020]. As discussed in §IX.A.1, at minimum, it would have been an obvious implementation choice to stop sending notification messages requesting a new device’s profile information only once an alert message has been received. Williams ¶¶138-140. This would have advantageously enabled the requester device to still receive an alert with the identified device’s information if, subsequent to the two devices’ first encounter, the requester or the identified device’s profile settings or thresholds are updated, such that an alert would be triggered (and the profile information sent) if a second notification message for the same device was received by the server. Williams ¶¶141-142. For example, a first device could have the maximum threshold set when it originally detects a second device, such that it does not receive any alert messages, but may subsequently lower the threshold and encounter the second device again such that a notification message would result in an alert message being returned. <i>Id.</i></p>

Claim Element	Eagle
	<ul style="list-style-type: none"> • [0004] (“<u>Each cellular phone keeps a log of other devices that have been previously detected and, whenever a new device comes within range, a notification message is transmitted to a remote server via the long-range cellular phone network.</u> The notification message contains an identification of both the requesting device and the nearby device whose presence has been detected....”) • [0020] (“.... When the remote server receives a notification message indicating that two identified devices are within Bluetooth range of one another, <u>and further determines that the profile data associated with these two devices satisfies a specified matching criteria, the remote server sends an alert message</u> to one or both of the two identified nearby devices.”) • [0023] (“<u>If it is determined at 216 that a detected nearby device has newly come within range and not currently identified in the Devices Long 214, its Bluetooth ID is posted at 217 as a new Devices Log entry and a request message is sent as indicated at 218 to a remote server, seen at 220 in FIG. 2, via the cellular phone network 222. ...</u>”) • [0024] (“Using the mechanism described above, a sequence of timestamp values may be recorded for each device encountered, and the BlueAware application may process this data to determine whether the detection of a given device warrants the transmission of a notification message to the server. To conserve memory space, <u>the BlueAware application may periodically remove identification and timestamp data for devices which have been out of range for an extended time.</u>”) <p>See also Eagle ¶¶[0048], [0054]–[0055] Williams ¶¶136-142.</p>

Claim Element	Eagle
<p>[10] The method of claim 1 wherein the information disclosure policy data specifies what portions of and/or the circumstances under which the further information is disclosed to the first wireless device.</p>	<p><i>See</i> [1].</p> <p>Eagle discloses that the information disclosure policy data specifies what portions of and/or the circumstances under which the further information is disclosed to the first wireless device (e.g., “the profile database contains ... preference data indicating, for example, the extent to which other information [in] the profile is sharable, and under what circumstances”).</p> <p><u>E.g., Eagle:</u></p> <p><i>See</i> [1.e]; Eagle ¶[0050].</p> <p>Williams ¶¶143-144.</p>
<p>[12] The method of claim 1 wherein the second identification information is received as part of detecting a proximity of a neighboring wireless device.</p>	<p><i>See</i> [1].</p> <p>Eagle discloses that the second identification information is received as part of detecting a proximity of a neighboring wireless device (e.g., “to identify social proximity”; “presence of a nearby device is detected”).</p> <p><u>E.g., Eagle:</u></p> <p><i>See</i> [1.c].</p> <p>Additionally, Eagle discloses that the system is used to detect the “proximity” of neighboring devices by the requester device receiving the Identified ID from the identified device via a Bluetooth “short range” communication.</p> <ul style="list-style-type: none"> • [0008] (“The present invention can exploit the growing availability of portable wireless electronic devices that incorporate Bluetooth transceivers that can be used as beacons to identify a device to other nearby devices. <i>Such personal beacon system offer better short range spatial resolution for proximity detection than do absolute location systems, such as GPS and cellular phone location systems. ...</i>”) • [0010] (“<i>The preferred embodiment of the present invention described in more detail below uses</i>

Claim Element	Eagle
	<p><i>personal area wireless network devices such as Bluetooth transceivers to identify social proximity ... to instigate person-to-person interactions between selected devices that are near to each other and/or between their users.”)</i></p> <p>Williams ¶¶145-147.</p>
<p>[14] The method of claim 1 additionally comprising: returning information to the first wireless device, as a result of the step of comparing the information disclosure policy data, which causes the first wireless device to limit other actions previously performed by the first wireless device.</p>	<p>See [1].</p> <p>Eagle renders obvious returning information to the first wireless device (e.g., see [8]), as a result of the step of comparing the information disclosure policy data (e.g., see [8]), which causes the first wireless device to limit other actions previously performed by the first wireless device (e.g., see [8] (discussing “which causes the first wireless device to limit re-sending of identifiers already reported by the first wireless device”)).</p> <p>See [8].</p> <p>Williams ¶¶148-149.</p>
<p>[15.pre] A central server utilizing one or more wireless Wide Area Network connections to exchange information between one or more applications executing on first and second wireless</p>	<p>Eagle discloses a central server (e.g., “server”) utilizing one or more wireless Wide Area Network connections (e.g., “large area wireless network such as a cellular phone network and/or the Internet”) to exchange information between one or more applications (e.g., “BlueAware”) executing on first and second wireless devices (e.g., “Bluetooth enabled cellular phones, communicate with and identify like devices that are nearby,” a “requester” and an “identified” device).</p> <p>See [1.pre].</p>

Claim Element	Eagle
devices, the central server comprising:	Williams ¶¶150-151.
[15.a] a first receiver, for receiving first identification information from the first wireless device, the first identification information communicated from the first wireless device to the server via the wireless Wide Area Network;	<p>Eagle discloses the central server comprising a first receiver (e.g., “message receiver” for the “Internet”), for receiving first identification information (e.g., “Requester ID”) from the first wireless device (e.g., “each notification message sent from a device to the server includes...its own ID value (the Requester ID)...”), the first identification information communicated from the first wireless device to the server via the wireless Wide Area Network (e.g., via a “large area wireless network such as a cellular phone network and/or the Internet”).</p> <p><u>E.g., Eagle:</u></p> <p>See [1.a].</p> <p>In addition, Eagle discloses that the server includes a “receiver” for receiving the notification messages from the “Internet.”</p> <ul style="list-style-type: none"> • [0010] (“uses personal area wireless network devices such as Bluetooth transceivers to identify social proximity and <i>a large area wireless network such as a cellular phone network and/or the Internet</i>, to permit interest matching functions to be performed at a remote central server....”) • Claim 2 (“Apparatus comprising ... a plurality of portable electronic devices, each given one of said devices comprising: a short range radio transmitter for transmitting a unique identification code value that identifies said given one of said devices,... and a server connected to a long range communication network, said <i>server comprising: ... a message receiver coupled to said long range communications network for receiving one or more notification messages from said devices...</i>”) <p>Williams ¶¶152-154.</p>

Claim Element	Eagle
<p>[15.b] wherein the first identification information is associated with one or more of an identifier of the first wireless device or an entity associated with the first wireless device;</p>	<p>Eagle discloses wherein the first identification information (e.g., “Requester ID”) is associated with one or more of an identifier of the first wireless device or an entity associated with the first wireless device (e.g., “the profile database contains, for each Bluetooth device: (a) the Bluetooth identification value BTID for that device ... (c) a short name for the device or its user”).</p> <p><i>See [1.b].</i></p> <p>Williams ¶¶155-156.</p>
<p>[15.c] a second receiver, for receiving second identification information, as collected by the first wireless device from the second wireless device via a separate local wireless link between the first and second wireless devices, and the second identification information communicated from the first wireless device to the server via the wireless Wide Area Network connection;</p>	<p>Eagle discloses the central server comprising a second receiver (e.g., “message receiver” for the “cellular phone network”), for receiving second identification information (e.g., “Identified ID”), as collected by the first wireless device from the second wireless device via a separate local wireless link between the first and second wireless devices (e.g., “When a device is within range of another such device, it identifies itself with unique identification value, such as a Bluetooth device address value,” using “Bluetooth”), and the second identification information communicated from the first wireless device to the server (e.g., “each notification message sent from a device to the server includes...the ID value of the newly arrived other device (the Identified ID)”) via the wireless Wide Area Network connection (e.g., via a “large area wireless network such as a cellular phone network and/or the Internet”).</p> <p><u><i>E.g., Eagle:</i></u></p> <p><i>See [1.c].</i></p> <p>In addition, because the wide area network connected to the server is “a cellular phone network and/or the Internet,” Eagle discloses that the server also includes a second “receiver” from a “cellular phone network,” which thus also receives a second notification message containing the same Requester ID and Identified ID — e.g., after the requester device’s device log has been</p>

Claim Element	Eagle
	<p>cleared and the identified ID is again detected Eagle ¶[0010], [0019], [0023]-[0024], Claim 2. To the extent it is argued further disclosure is required, at minimum, it would have been an obvious implementation choice for the server to use multiple receivers for receiving information from the devices such that information may be received either via the “cellular phone network and/or the Internet” as disclosed in Eagle. Williams ¶159.</p> <ul style="list-style-type: none"> • [0010] (“The preferred embodiment of the present invention described in more detail below uses personal area wireless network devices such as Bluetooth transceivers to identify social proximity and <u>a large area wireless network such as a cellular phone network and/or the Internet</u>, to permit interest matching functions to be performed at a remote central server”) • [0019] (“Each of these Bluetooth enabled cellular phones includes a processor that is specially programmed with an application program, called “BlueAware,” that enable the cellular phone to identify and log the presence of other “discoverable” Bluetooth devices that are nearby...”) • [0023] (“If it is determined at 216 that a detected nearby device has newly come within range and not currently identified in the Devices Long 214, its Bluetooth ID is posted at 217 as a new Devices Log entry and a request message is sent as indicated at 218 to a remote server, seen at 220 in FIG. 2, via the cellular phone network 222.”) • [0046] (“... As will be understood, <u>the functions performed by the remote server may be performed by a plurality of different server processes which execute on one or several different computes and</u>

Claim Element	Eagle
	<p><u>would typically include a web server, an application server and a database server. ...”</u>)</p> <ul style="list-style-type: none"> • Claim 2 (“Apparatus comprising ... a plurality of portable electronic devices, each given one of said devices comprising: a short range radio transmitter for transmitting a unique identification code value that identifies said given one of said devices,... and a server connected to a long range communication network, said <u>server comprising: ... a message receiver coupled to said long range communications network for receiving one or more notification messages from said devices...</u>”) <p>Williams ¶¶157-159.</p>
<p>[15.d] wherein the second identification information is associated with one or more of an identifier of the second wireless device or an identifier of an entity associated with the second wireless device; and</p>	<p>Eagle discloses wherein the second identification information (e.g., “Identified ID”) is associated with one or more of an identifier of the second wireless device or an identifier of an entity associated with the second wireless device (e.g., “the profile database contains, for each Bluetooth device: (a) the Bluetooth identification value BTID for that device ... (c) a short name for the device or its user”).</p> <p><i>See</i> [1.d].</p> <p>Williams ¶¶160-161.</p>
<p>[15.e] a data processor for</p>	<p>Eagle discloses the central server comprising a data processor (e.g., the “remote server processes these incoming notification messages”).</p> <p><u>E.g., Eagle:</u></p> <p><i>See</i> [1.e], [1.f].</p> <p>In addition, a POSITA would have understood that the “server” comprises a data processor to “process[]” the incoming notification messages and perform the</p>

Claim Element	Eagle
	<p>comparison, and, at minimum, it would have been obvious for the server to have one for the same reason, as discussed in §IX.A.1.</p> <ul style="list-style-type: none"> • [0020] (“<i>The remote server processes these incoming notification messages by consulting a database of profile information about each participating device and its owner...</i>”) • [0046] (“<i>...As will be understood, the functions performed by the remote server may be performed by a plurality of different server processes which execute on one or several different computers and would typically include a web server, an application server and a database server....</i>”) • Claim 2 (“...said server comprising: ... <i>processing means coupled to said message receiver</i> and to said database for generating an new alert message when the profile data for two nearby ones of said devices satisfy a predetermined [sic] matching criteria...”) <p>Williams ¶¶162-163.</p>
<p>[15.f] storing and retrieving disclosure policy data associated with the second identification information, the disclosure policy data representing rules for privacy of information concerning the second wireless device or privacy of an entity associated</p>	<p>Eagle discloses storing and retrieving disclosure policy data associated with the second identification information (e.g., “user accesses a secure web site ... for entering and editing profile information;” “The two BTID values [the Requester ID and the Identified ID in the notification message] are used to fetch corresponding profile data from the database 260;” “profile data” in “[p]rofile database” “contains ... the Bluetooth identification value BTID for that device”), the disclosure policy data representing rules for privacy of information concerning the second wireless device or privacy of an entity associated with the second wireless device (e.g., “the profile database contains ... preference data indicating, for example, the extent to which other information [in] the profile is sharable, and under what</p>

Claim Element	Eagle
<p>with the second wireless device;</p>	<p>circumstances,” “device ... set to only establish potential links to others within a 'trust network'”).</p> <p><u>E.g., Eagle:</u></p> <p>See [1.e].</p> <p>In addition, Eagle discloses that the disclosure policy is stored and retrieved using the same Identified ID in both notification messages, and that the profile data is set by the user of the identified device, and stored by the server. Eagle ¶[0012].</p> <ul style="list-style-type: none"> • [0045] (“Participating Bluetooth device users provide profile information along with the Bluetooth identification values (BTIDs) to populate a profile database illustrated at 260 in FIG. 2.... <i>Using an assigned user name and password, a user accesses a secure web site which provides a forms based interface for entering and editing profile information</i> the describes a Bluetooth enabled cellular phone (typically including its cellular phone number and its 48 bit Bluetooth device address)...”) <p><i>See also</i> Eagle ¶[0057].</p> <p>Williams ¶¶164-166.</p>
<p>[15.g] comparing the information disclosure policy data and the first identification information; and</p>	<p>Eagle discloses the data processor for comparing the information disclosure policy data and the first identification information (e.g., “device ... set to only establish potential links to others within a 'trust network'”).</p> <p><u>E.g., Eagle:</u></p> <p>See [1.f].</p> <p>In addition, Eagle discloses that, for both notification messages, the data processor of the “server” compares the profile data for the requester and identified IDs/devices (which are the same for both messages) to determine whether to communicate an “alert message” to the requester device. <i>E.g.</i>, Eagle ¶¶[0007], [0020].</p>

Claim Element	Eagle
<p>[15.h] providing further information to the first wireless device concerning the entity associated with second wireless device, but only to the extent that it is consistent with the step of comparing the information disclosure policy data.</p>	<p>Williams ¶¶167-169.</p> <p>Eagle discloses the data processor for providing further information to the first wireless device concerning the entity associated with second wireless device (e.g., “the remote server sends an alert message to one or both of the two identified nearby devices,” “alert messages ... sent only when such a “trusted” person having common interests is nearby”), but only to the extent that it is consistent with the step of comparing the information disclosure policy data (e.g., “user may also set the extent to which information will be provided to requesters”; “Certain trusted devices may have profile information attributes set that entitle them to receive profile data from the server relating to a nearby individual that would not be available to the general public.”).</p> <p><u><i>E.g., Eagle:</i></u></p> <p><i>See [1.g].</i></p> <p>In addition, Eagle discloses that in response to both notification messages, the server compares the identified device’s disclosure policy with the Requester ID, which is the same in both notification messages, to determine if the requester device is included in a “trust network” for the identified device. Eagle ¶[0048], [0066].</p> <ul style="list-style-type: none"> • [0048] (“...As illustrated at 270 in FIG. 2, <u>each notification message</u> sent from a device to the server includes not only its own ID value (the Requester ID) and the ID value of the newly arrived other device (the Identified ID)...”) <p>Williams ¶¶170-172.</p>
<p>[18] The server of claim 15 wherein the preferences comprise one or more of:</p>	<p><i>See [5], [15].</i></p> <p>Williams ¶¶173-174.</p>

Claim Element	Eagle
<p>... disclose my name/do not disclose my name; disclose age/do not disclose age; or do or do not disclose personal details.</p>	
<p>[20] The server of claim 15 additionally comprising: a processor, for making a decision based upon the detected identifiers, the decision depending upon a policy for a selected wireless device regarding privacy for communication with other wireless devices.</p>	<p><i>See</i> [15].</p> <p>Eagle discloses a processor (e.g., [15.e], the “remote server processes these incoming notification messages”; “the functions performed by the remote server may be performed by a plurality of different server processes which execute on one or several different compute[r]s and would typically include a web server, an application server and a database server.”), for making a decision based upon the detected identifiers (e.g., the server “determines that the profile data associated with these two devices satisfies a specified matching criteria” and “sends an alert message”), the decision depending upon a policy for a selected wireless device regarding privacy for communication with other wireless devices (e.g., “A given user may then request that alert messages be sent only when such a “trusted” person having common interests is nearby;” “A device can also be set to only establish potential links to others within a 'trust network'.”).</p> <p><u><i>E.g., Eagle:</i></u></p> <p><i>See</i> [1.f], [15.e].</p> <p>In addition, Eagle discloses that the server decides whether to send an alert message in response to each notification message based on whether the identified device’s ID (the Identified ID) is included in a “trust network” for the requester device. Eagle ¶¶[0056], [0066].</p>

Claim Element	Eagle
	<p>As discussed in §IX.A.1, to the extent it is argued further disclosure of a separate processor from that recited in [15.e] is required, Eagle discloses using multiple separate processors on different computers that are part of the server. Eagle ¶[0046]. At minimum, it would have been an obvious implementation choice for the server to use multiple processors to divide the workload, such that a separate processor decides whether to send alert messages based on whether the identified device is included in a “trust network” for the requester device. Eagle ¶[0046], [0066]; Williams ¶179.</p> <ul style="list-style-type: none"> • [0005] (“Profile data that describes each device and its owner is stored in a database. <i>When a notification message is received identifying two devices that have come within range of one another, the server fetches the profile data associated with each of the two identified devices and performs a comparison....</i>”) • [0009] (“The robust capabilities of web servers, applications servers and database servers may be used to advantage to provide better performance from the individual devices, as well as functions such as improved privacy protection....”) • [0046] (“As shown in FIG. 2, the user may use an available personal computer 290 connected to a web server via the Internet 295 to populate the profile database. <i>As will be understood, the functions performed by the remote server may be performed by a plurality of different server processes which execute on one or several different computers and would typically include a web server, an application server and a database server....</i>”) <p>Williams ¶¶175-179.</p>
[21] The server of claim 20 wherein	<i>See [20].</i>

Claim Element	Eagle
<p>the decision is based on at least one of: ... a list the identifier is included on....</p>	<p>Eagle discloses that the decision is based on at least one of: ... a list the identifier is included on (e.g., “A given user may then request that alert messages be sent only when such a “trusted” person having common interests is nearby;” “A device can also be set to only establish potential links to others within a 'trust network'.”)....</p> <p><u>E.g., Eagle:</u> See [1.f], [7], [20].</p> <p>Additionally, Eagle discloses that the decision discussed in [20] is based on whether the identified device’s ID (the Identified ID) is included in a “trust network” for the requester device. Eagle ¶¶[0050], [0056], [0066].</p> <p>Williams ¶¶180-181.</p>
<p>[22] The server of claim 15 additionally comprising: a transmitter, for returning information to the first wireless device, to cause the first wireless device to limit re-sending of identifiers already reported by the first wireless device.</p>	<p>See [15].</p> <p>Eagle renders obvious the server comprising a transmitter (e.g., “message transmitter”), for returning information to the first wireless device, to cause the first wireless device to limit re-sending of identifiers already reported by the first wireless device (e.g., see [8]).</p> <p><u>E.g., Eagle:</u> See [8].</p> <p>In addition, Eagle discloses that the server includes a “message transmitter” for sending the alert messages.</p> <ul style="list-style-type: none"> • Claim 2 (“...said server comprising: ... <u>a message transmitter for transmitting said new alert message via said long range communications network to one or both of said two nearby ones of said devices...</u>”) <p>Williams ¶¶182-184.</p>

B. Ground 3: Claims 8, 14, 22

To the extent it is argued that further disclosure beyond Eagle is required for claims 8, 14, and 22, Eagle in view of Mgrdechian renders these claims obvious.

1. Overview of Mgrdechian and Motivation to Apply Its Teachings to Eagle

Mgrdechian teaches a system for using a “remote computer system” to facilitate communications between wireless devices. Mgrdechian, 1:32-35, 3:13-25. As with '736 and **Eagle**, **Mgrdechian** discloses that a first wireless device receives “wireless device identifications,” such as “a Bluetooth identification or an RFID,” from a second wireless device when the two are in proximity, and transmits this identification information to the remote computer system. Mgrdechian, 3:13-25, 3:34-37, 9:46-10:29. The remote computer system accesses information about the second device, such as profile information, and returns “some or all of the profile information” of the second device to the first device, and the requester device can store this information “internally.” *E.g.*, Mgrdechian, 3:13-25, 12:18-44. As Mgrdechian teaches, having a portion of the profile information available on the requester device prevents “automatically retrieving profile information” by sending additional requests to the server. *E.g.*, Mgrdechian, 15:46-16:2. Williams ¶96.

While **Eagle** discloses sending an Identified ID from a requester device to the server to request an alert message containing information about the identified device

when the Identified ID is detected for the first time after the requester device's device log is cleared (*e.g.*, Eagle ¶¶[0023]-[0024]; *see* §IX.A.1), **Mgrdechian** discloses a first device not “automatically retrieving profile information” about a second device from a server when the information is already available to the first device. *E.g.*, Mgrdechian, 15:46-16:2. Indeed, **Mgrdechian** discloses the first device saving profile information received from the server about the second device for later use. Mgrdechian, 12:23-28; Williams ¶97.

A POSITA would have been motivated, and would have found it advantageous, to apply **Mgrdechian**'s teachings of preventing the automatic retrieval of profile information in implementing **Eagle**'s communications system such that a requester device does not send an Identified ID to the server if the requester device has previously received and saved an alert message in response to sending the Identified ID at an earlier time. Williams ¶97. Like Eagle, **Mgrdechian** is in the same field and is analogous art to the '736, namely facilitating communications between wireless devices using a server. *E.g.*, Mgrdechian, Abstract; Williams ¶97.

A POSITA would have recognized that **Mgrdechian**'s teachings of preventing the “automatic[] retriev[al of] profile information” by a first device from a server once the first device already has some information for a second device stored locally would have improved **Eagle**'s system by limiting unnecessary transmissions

after the receipt of an alert message and saving computer resources while ensuring that users still get the most relevant information about entities and devices in proximity. *Mgrdechian*, 15:46-16:2; Williams ¶98. Indeed, it was well-known as of the priority date of the '736 to limit the request to a server for information that may already be cached locally. *See, e.g.*, U.S. 8,295,819 (“Kaplan”), Fig. 4, 3:58-4:8 (a device requests “picture and contact information” for another device from a server only if the “data is not locally available”); U.S. 9,734,198 (“Taylor”), Abstract, 2:42-51 (client requests for duplicate information are suppressed to avoid “unnecessary queries against the underlying database”); Williams ¶99.⁵ Indeed, **Eagle** itself recognizes the benefits of limiting transmissions, for example, to those that have “newly come within range,” and teaches processing detected identifier data “to determine whether the detection of a given device *warrants the transmission of a notification message to the server.*” *Eagle* ¶¶[0023]-[0024]. **Eagle** further recognizes the benefits of battery-saving measures and suggests implementations to conserve battery life. *Id.* ¶[0026]. A POSITA would have recognized that **Mgrdechian**’s teachings provide implementation details for determining whether

⁵ Kaplan was filed 12/19/2005, and is prior art under §102(e). Ex. 1024. Taylor was filed 11/30/2007, and is prior art under §102(e). Ex. 1025.

the detection of a new device warrants the transmission of a message to the server and for conserving battery life by minimizing unnecessary transmissions after an alert has been received. Williams ¶¶99.

In light of the foregoing, a POSITA would have found it obvious and straightforward to apply **Mgrdechian**'s teachings of limiting requests to the server, in implementing **Eagle**'s communications system, and would have known that such a combination (yielding the claimed limitations) would predictably work and provide the expected functionality. Williams ¶¶100, 185-186.

2. Claim Chart—Eagle in view of Mgrdechian

Claim Element	<u>Eagle in view of Mgrdechian</u>
[8] The method of claim 1 additionally comprising: returning information to the first wireless device, as a result of the step of comparing the information disclosure policy data, which causes the first wireless device to limit re-sending of identifiers already reported by the first wireless device.	<p><i>See</i> §XI.A.2.[8].</p> <p>To the extent further information is required, Mgrdechian discloses returning information to the first wireless device (e.g., “computer system 360 may send some or all of the profile information associated with each device ID back to the initiating wireless device;” “the profile information may be saved ... as a complete profile or as a summary profile”) which causes the first wireless device to limit re-sending of identifiers already reported by the first wireless device (e.g., “rather than automatically retrieving profile information for all device IDs within range, computing resources may be saved by narrowing the list to profiles of interest to be retrieved.”).</p> <p><u>E.g., Mgrdechian:</u></p> <p>To the extent that PO may argue Eagle does not expressly disclose that the server will return information to the device to limit re-sending identifiers, Mgrdechian discloses that a remote computer system returns “some or</p>

Claim Element	<u>Eagle in view of Mgrdechian</u>
	<p>all of the profile information” of an identified device to the requester device, and the requester device can store this information “internally.” <i>E.g.</i>, Mgrdechian, 12:18-44. Additionally, having a portion of the profile information available on the requester device prevents “automatically retrieving profile information” by sending additional requests to the server. <i>E.g.</i>, Mgrdechian, 15:46-16:2.</p> <p>As discussed in §IX.B.2, a POSITA would have been motivated to apply Mgrdechian’s known teachings of storing profile information retrieved from the server and preventing the requesting device from trying to retrieve duplicate information from the server, in implementing Eagle’s “portable communication devices” such that the communication device does not send an Identified ID to the server if the communication device has previously received and saved an alert message in response to sending the Identified ID at an earlier time. Mgrdechian, 12:18-44, 15:46-16:2; Williams ¶¶189-191. Limiting the requester device from sending unnecessary notification messages would advantageously save system resources, and avoid unnecessary queries to the profile database. Williams ¶191.</p> <ul style="list-style-type: none"> • 12:18-44 (“As mentioned above, <u>computer system 360 may send some or all of the profile information associated with each device ID back to the initiating wireless device</u> (e.g., Device A), and the profile information (e.g., an image or picture of the target user) may be displayed to the user of the initiating wireless device. Profile information for one or more targets may be stored internally on a wireless device or selectively deleted. <u>Some or all of the profile information may be saved (e.g., as a complete profile or as a summary profile)</u>. Such profile information may be useful if the initiating user desires to contact such target at a later time. The user of the initiating device may review the profiles

Claim Element	<u>Eagle in view of Mgrdechian</u>
	<p>and may subsequently interact with other selected users depending on interest by sending message information to selected users....”)</p> <ul style="list-style-type: none"> • 15:46-16:2 (“In some embodiments, wireless devices 310 and 320 may include initial profile information 312 and 322 stored locally on the wireless devices. <u>Initial profile information 312 and 322 may be pictures and/or profile summaries (i.e., “thumbnails”) that require less memory than a full profile so that profiles may become “portable.”</u> Initial profile information may contain short textual statements and a picture.... Device A may then display the initial profile information (e.g., a picture) to User A using a display or other interface. User A may then select specific target devices for further and subsequent queries. <u>Thus, rather than automatically retrieving profile information for all device IDs within range, computing resources may be saved by narrowing the list to profiles of interest to be retrieved from the remote computer system.”)</u> <p>See also 20:51-21:21. Williams ¶¶187-191.</p>
<p>[14] The method of claim 1 additionally comprising: returning information to the first wireless device, as a result of the step of comparing the information disclosure policy data, which causes</p>	<p>See §XI.A.2.[14].</p> <p>To the extent further information is required, Mgrdechian discloses returning information to the first wireless device (e.g., “computer system 360 may send some or all of the profile information associated with each device ID back to the initiating wireless device;” “the profile information may be saved ... as a complete profile or as a summary profile”), which causes the first wireless device to limit other actions previously performed by the first wireless device (e.g., “rather than automatically retrieving profile information for all device IDs within range, computing resources may be saved by narrowing the list to profiles of interest to be retrieved.”).</p>

Claim Element	<u>Eagle in view of Mgrdechian</u>
the first wireless device to limit other actions previously performed by the first wireless device.	<p><u>E.g., Mgrdechian:</u> <i>See [8].</i></p> <p>Williams ¶¶192-194.</p>
[22] The server of claim 15 additionally comprising: a transmitter, for returning information to the first wireless device, to cause the first wireless device to limit re-sending of identifiers already reported by the first wireless device.	<p><i>See §XI.A.2.[22].</i></p> <p>To the extent further information is required, Mgrdechian discloses returning information to the first wireless device (e.g., “computer system 360 may send some or all of the profile information associated with each device ID back to the initiating wireless device;” “the profile information may be saved ... as a complete profile or as a summary profile”) which causes the first wireless device to limit re-sending of identifiers already reported by the first wireless device (e.g., “rather than automatically retrieving profile information for all device IDs within range, computing resources may be saved by narrowing the list to profiles of interest to be retrieved.”).</p> <p><i>See [8].</i></p> <p>Williams ¶¶195-196.</p>

X. SECONDARY CONSIDERATIONS

There is no evidence in the prosecution history of this or any related application that any arguments regarding secondary considerations exist, let alone that there is a sufficient nexus to any of the challenged claims. *See generally*, Ex. 1002; *see also* Williams ¶¶197-198. Indeed, as demonstrated by the prior art referenced herein, any purported problems, solutions or unexpected results in the

'736 were already well known. *Id.* To the extent PO asserts the existence of any secondary considerations in its responses, Petitioner reserves the right to address any such evidence.

XI. CONCLUSION

Substantial, new, and noncumulative technical teachings have been presented for the Challenged Claims of the '736. Claims 1, 5-7, 10, 12, 15, 18, and 20-21 are anticipated and all Challenged Claims are rendered obvious for the reasons set forth above. Williams ¶¶199-200. There is a reasonable likelihood that Petitioner will prevail as to each of those claims. *Inter Partes* review of claims 1, 5-8, 10, 12, 14-15, 18, and 20-22 is accordingly requested.

Dated: May 8, 2020

/James L. Davis, Jr./
James L. Davis, Jr.

CERTIFICATE OF COMPLIANCE

Pursuant to 37 CFR §42.24(a) and (d), the undersigned hereby certifies that this Petition for Inter Partes Review complies with the type-volume limitation of 37 CFR §42.24(a)(i) because, exclusive of the exempted portions, it contains 13,986 words as counted by the word processing program used to prepare the paper.

Dated: May 8, 2020

/James L. Davis, Jr./

James L. Davis, Jr.

CERTIFICATE OF SERVICE

The undersigned certifies service pursuant to 37 C.F.R. §§ 42.6(e) and 42.105(b) on the Patent Owner by FedEx of a copy of this Petition for *Inter Partes* Review and supporting materials at the correspondence address of record for the '736 patent:

VLP Law Group LLP
555 Bryant Street, Suite 820
Palo Alto, CA 94301

Courtesy copies of the same documents were also served at the following email addresses of record for Proxicom's litigation counsel for the subject patent in the district court litigation at the U.S. District Court for the Middle District of Florida, Case No. 6:19-cv-01886-RBD-LRH:

KING, BLACKWELL, ZEHNDER & WERMUTH, P.A.
Taylor F. Ford - tford@kbzwlaw.com
Dustin Mauser-Claassen - dmauser@kbzwlaw.com

BUNSOW DE MORY LL
Denise M. De Mory - ddemory@bdiplaw.com
Chris J. Coulson - ccoulson@bdiplaw.com

Dated: May 8, 2020

/James L. Davis, Jr./
James L. Davis, Jr.