

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

TARGET CORPORATION,

Petitioner,

v.

PROXICOM WIRELESS, LLC,

Patent Owner.

Case IPR2020-00903

U.S. Patent No. 9,038,129

PETITION FOR *INTER PARTES* REVIEW

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	MANDATORY NOTICES (§42.8).....	4
A.	Real Party-In-Interest	4
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.....	6
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 '129 PATENT.....	9
VI.	PROSECUTION HISTORY	11
VII.	LEVEL OF ORDINARY SKILL	14
VIII.	CLAIM CONSTRUCTION	14
IX.	GROUND OF UNPATENTABILITY.....	15
A.	Grounds 1-2.....	17
1.	Overview of Eagle	17
2.	Claim Chart—Eagle.....	25
X.	SECONDARY CONSIDERATIONS	56
XI.	CONCLUSION.....	56

LIST OF EXHIBITS

Ex. 1001	U.S. Patent No. 9,038,129 (“129”)
Ex. 1002	File History of U.S. Patent No. 9,038,129 (“129 FH”)
Ex. 1003	Declaration of David Hilliard Williams in Support of Petition for <i>Inter Partes</i> Review of U.S. Patent No. 9,038,129 (“Williams”)
Ex. 1004	U.S. Patent App. No. 2005/0250552 (“Eagle”)
Ex. 1006	U.S. Patent App. No. 2004/0243519 (“Perttila”)
Ex. 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. 1023-1025	Reserved

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, 7, 10-11, 16-20, and 25-26 (“Challenged Claims”) of U.S. Patent 8,374,129 (“’129”) (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 ’129’s purported invention is the use of a “central server” to “broker the exchange of information between” two entities associated with two wireless devices. ’129, 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.*

The ’129 admits that, prior to the alleged invention, wireless devices already were configured to use both the short-range and wide-area connections claimed in

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 '129. *Id.*, 2:12-23 (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 '129 admits that prior art systems already were using wireless devices for e-commerce and social networking applications. *Id.*, 1:56-2:1, 2:24-35. And as recognized during prosecution, the prior art already taught using a central server to broker the exchange of information between devices communicating via a short-range network by communicating with the devices using a wide-area network. *See* §VI.

The only purportedly novel elements of the '129 claims are the specific recitations of what “further information” is returned to a wireless device from the server. For example, independent claims 1 and 16 require the “further information” to be related to *any one* or more of: (1) using “current state information” and “feedback ratings” in a “multiple step electronic transaction” ('129 File History (Ex. 1002) 207-209, 304); (2) returning further information related to “a reward for participation in a loyalty program... dependent upon said stored state” (*id.* 210); *or* (3) use of “social network content ... dependent upon said stored state ... [that] comprises a friends list” that results in access to “private social network content” (*id.* 210-214). But, as discussed herein, it was already well-known to transmit such further information over a network, including a network conforming to the claimed

arrangement of two wireless devices communicating over a short-range network and a server communicating with one or both devices across a wide-area network.

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].

Thus, and as further explained below, **Eagle** anticipates claims 1-5, 7, 10-11, 16-20, and 25-26 and, at minimum, renders obvious all the Challenged Claims. At best, the Challenged Claims of the ’129 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 or any other reference providing analogous disclosures during prosecution of the '129. 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 '129, 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 '129 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
7,936,736	IPR2020-00904

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. 001008-0037-657.

IV. REQUIREMENTS FOR INTER PARTES REVIEW

A. Grounds for Standing

Pursuant to §42.104(a), Petitioner certifies that the '129 is available for IPR. Petitioner is not barred or estopped from requesting IPR challenging the claims of the '129 on the grounds identified herein.

B. Identification of Challenge

Pursuant to §42.104(b), Petitioner requests IPR of claims 1-5, 7, 10-11, 16-19, and 25-26 of the '129, and that the Board cancel the same as unpatentable. The '129 matured from U.S. Application 13/744,457 (filed 01/18/2013), and through a chain of divisional and continuation applications, claims priority to U.S. Application 12/364,897 (filed 2/3/2009, matured into U.S. Patent 7,936,736), U.S. Provisional

Application 61/095,359 (filed 9/9/2008), and U.S. Provisional Application 61/095,001 (filed 9/8/2008).² Williams ¶81.

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)

Eagle was 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 ’129. 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

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 ’129 patent. Petitioner reserves the right to challenge these priority claims.

³ Eagle issued as U.S. Patent No. 7,877,082 (prior art under §102(e)). Ex. 1022.

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 ’129; PO served its infringement contentions on 02/10/2020 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, 10-11, 16-20, and 25-26
2		§103	

3. How the Challenged Claims Are Unpatentable

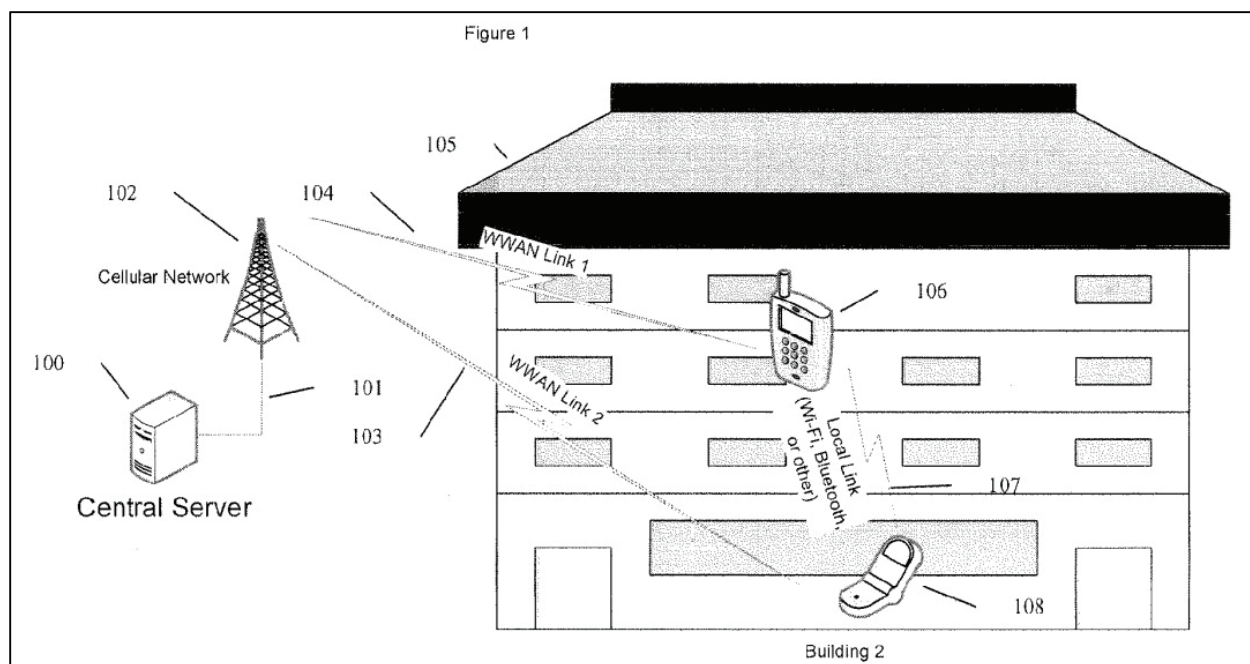
Petitioner provides the information required under §§42.104(b)(4)-(5) in §IX.

V. THE '129 PATENT

The '129 describes techniques for using a server to broker the exchange of information between wireless devices. '129, Abstract. The background section of the '129 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. '129, 1:27-38, 2:24-35. The '129 combines these two well-known communication methods, and describes methods for exchanging information using “both a short range and a long range wireless capability.” '129, 2:53-57. Williams ¶¶57-58.

The '129'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 some additional information that the server should communicate back to one or both devices. For example, Figure 1 of the '129 shows that “a central server 100 is connected to devices 106 and 108” through a combination of the Internet and a “cellular network 102.” '129, 5:44-53. The devices are also able to communicate directly with each other via “a short range wireless link 107 such as a Bluetooth.” '129, 6:33-37.



'129 Fig. 1. The '129 states that each wireless device searches for nearby devices and exchanges “wireless identifiers” using Bluetooth. *E.g.*, '129, 6:49-53. 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.” ’129, 3:2-7; 8:1-6. As an example of enforcing a “policy,” the ’129 states that the server returns “relevant” information that a device is “authorized to receive.” ’129, 8:6-8. Williams ¶¶59-62.

The ’129 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* ’129, 3:22-32, 4:31-48. As another example, ’129 discloses that a customer might interact with a “broadcast device” used in a store to receive “coupon[s]” or rewards from a “loyalty program.” *See* ’129, 15:4-23. Additionally, the ’129 states that its disclosures can be used to facilitate “financial transaction[s],” with the server mediating between the two devices. *See* ’129, 11:20-30. Williams ¶¶63-66.

VI. PROSECUTION HISTORY

U.S. Patent Application 13/744,457, which matured into the ’129, was filed 01/18/2013. The originally-filed claims were generally directed to “utilizing a server” to exchange information between first and second wireless devices by receiving first and second “unique identifiers” from the first wireless device, where the second “unique identifier” was previously communicated from a second wireless device to the first wireless device; comparing “data derived from the first unique identifier” with a “disclosure policy” specifying “rules for privacy” associated with

the second identifier; and communicating “further information” to the first wireless device based on a “stored state resulting from previous interactions,” wherein the information is related to one or more of “a current step of a multiple step electronic commerce transaction ... a reward for participation in a loyalty program ... and social network content.” ’129 FH (Ex. 1002), 52-53; Williams ¶¶67-68.

The Examiner issued a first Non-Final Office Action on 10/25/2013 rejecting pending independent claims 1, 16, and 31 as unpatentable over U.S. Pub. No. 2004/0030601 (“Pond”) in view of U.S. Pub. No. 2005/174975 (“Mgrdechian”). ’129 FH, 146-150, 161-162. The Applicant responded on 4/25/2014 by arguing that the cited references did not disclose various features of the independent claims, including: (1) “communicating further information to the first wireless device,” (*id.* 206-207); (2) using “current state information” in a “multiple step electronic transaction” in the same manner as claimed (*id.* 207-209); (3) returning further information related to “a reward for participation in a loyalty program... dependent upon said stored state” (*id.* 210); and (4) use of “social network content ... dependent upon said stored state ... [that] comprises a friends list” that results in access to “private social network content” (*id.* 210-214). Williams ¶¶69-70.

The Examiner issued a first Notice of Allowance and entered an Examiner amendment on 5/15/2014, following a pair of interviews conducted on 5/7/2014 and 5/8/2014. ’129 FH 234-243. The amendment required the multi-step electronic

commerce transaction to be “*related to feedback ratings by other entities for behavior of an entity associate with the second wireless device,*” and replaced the word “*or*” for the word “*and*” prior to the final limitation (*i.e.*, to require that the “further information” comprises content related to a multi step electronic transaction, a reward for participation in a loyalty program, *or* social network content). *Id.*; Williams ¶71.

The Applicant withdrew the application from issue and filed a request for continued examination on 6/13/2014. ’129 FH 280-282. On further consideration, the Examiner issued a second Non-Final Office Action on 8/25/2014 to reject the independent claims as unpatentable over Pond in view of Mgrdechian. *Id.* 297. The Applicant responded on 1/26/2015 by reiterating all of the same arguments made in response to the first office action—asserting that the pending claims “maintain each and every feature of the claims as previously allowed.” *Id.* 341-343. The Applicant also made amendments to independent claims 1 and 16 regarding the multi-step electronic transaction limitation and requiring the reward for participation in the loyalty program be “*related to past purchasing behavior of an entity associated with the first wireless device.*” *Id.* 326-333; Williams ¶¶72-73.

The Examiner issued a second Notice of Allowance on 2/17/2015, allowing claims 1-30 and cancelling claims 31 and 35 by Examiner amendment. ’129 FH 369. The Examiner did not identify specific limitations that led to allowance—

simply stating that the previous arguments “pertaining to any of claims 1-30 were found to be persuasive.” *Id.* 369-370. The ’129 patent issued 5/19/2015. Williams ¶74.

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 ¶¶35-37.

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” link/network, “local wireless link”), the prior art relied on herein discloses the ’129’s examples of those terms as shown in §IX.A below. *See, e.g.*, ’129 2:13-18 (“cellular wireless wide area network connection (WWAN) ... such as CDMA (IS-2000), GSM, W-CDMA, WiMax, etc.”), 5:61-64 (“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...”), 17:48-50 (“The device detects a broadcast device, and interacts over the internet with the server via the WWAN connection...”), 19:44-47 (“a local, or personal area network wireless protocol such as ... Bluetooth”) (emphasis added). *See Williams ¶¶77-80.*

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 ’129 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 device to a server; (3) comparing a “disclosure policy” for the second wireless device with information about the other; and (4) using a “stored state” to determine some additional information that the server should communicate back to one or more of

the devices relating to one or more of a “multi-step electronic commerce transaction ... a reward for participation in a loyalty program ... or social network content.” The claimed features are anticipated and, at minimum, obvious in view of the prior art, as explained below. Williams ¶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 the '129, 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 related to social network content. **Eagle** also describes the same additional limitations, such as the use of a friends list, applications involving business entities, or providing information based on previous interactions with the server. Williams ¶104.

As shown below, the prior art renders the Challenged Claims of the '129 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 '129. Williams ¶¶38-186.

A. Grounds 1-2: Claims 1-5, 7, 10-11, 16-20, and 25-26 are anticipated and, at minimum, rendered obvious by Eagle

As further set forth below, the Challenged Claims are anticipated 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. Williams ¶¶83-84.

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 ¶¶85-86.

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].

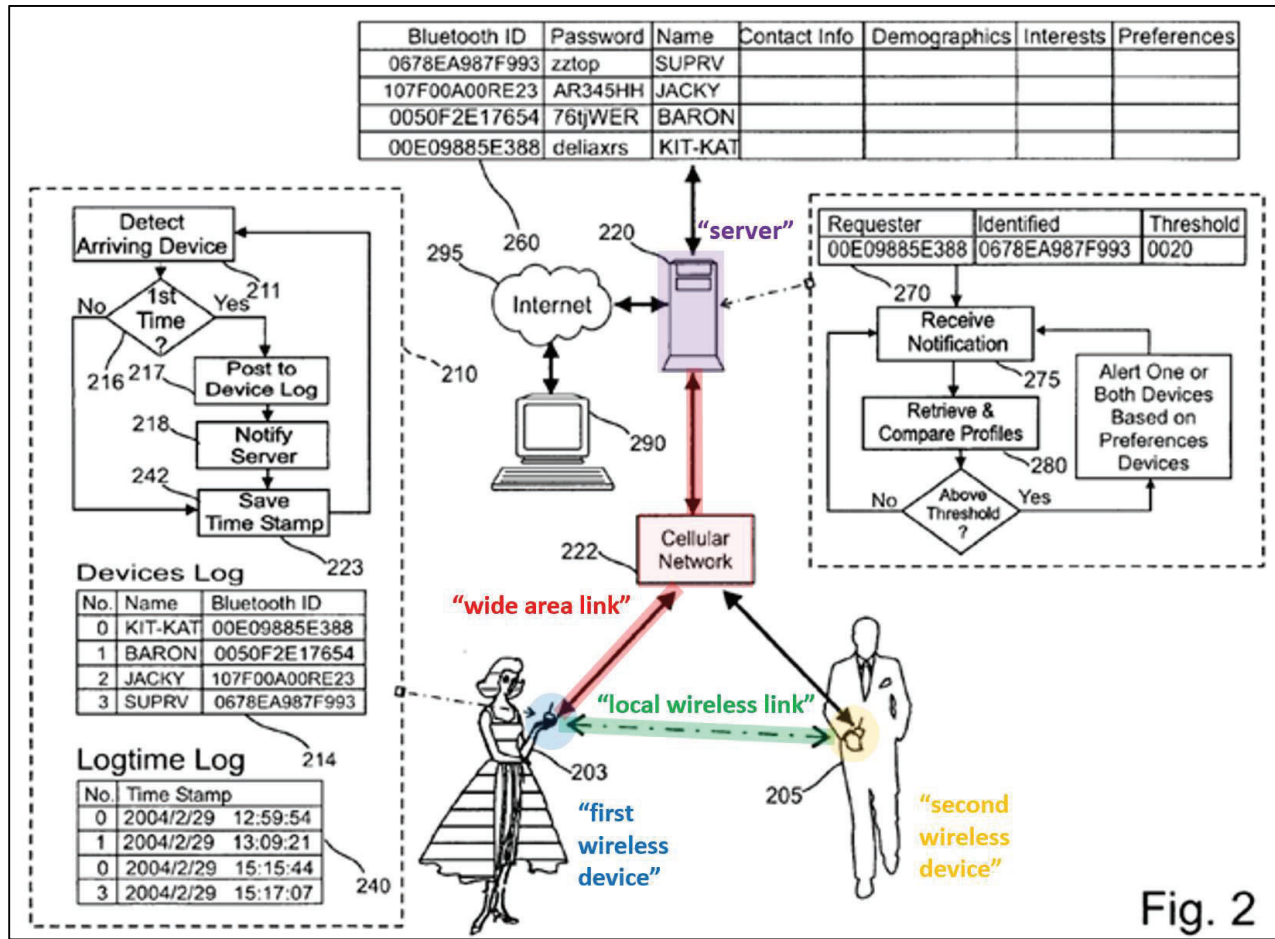
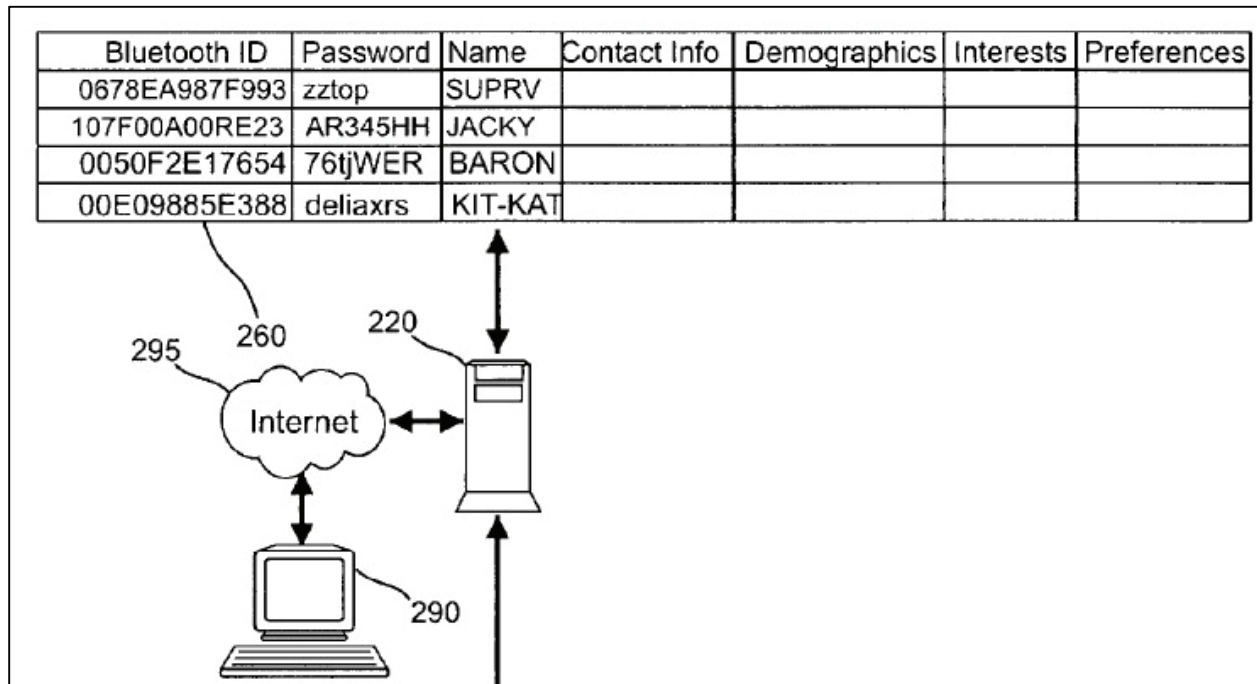


Fig. 2

Eagle, Fig. 2; Williams ¶¶87-89.

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 ¶90.

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” or “likely 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

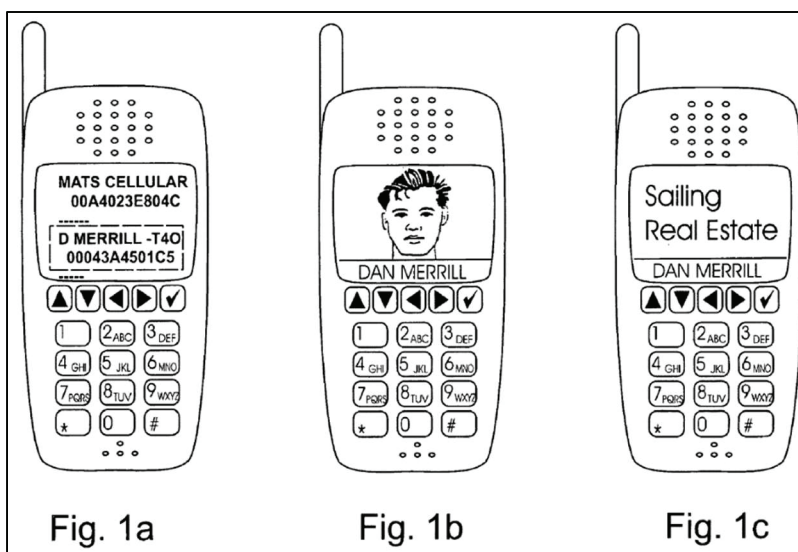
device that is “within one degree from an individual’s social circle, i.e.: a friend-of-a-friend.” Eagle ¶[0066]. Williams ¶¶91-92.

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 ¶¶93-94. 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]; Williams ¶¶92-94, 118. 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. *Id.*

A POSITA would have 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 ¶95. 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 processor, and it would have been an obvious design choice to include such a processor in the server. *Id.* Indeed, the '129 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” '129, 6:1-6.

As shown in Figures 1a-1c, the alert sent to the requester device may also include contact information, a photograph of the other user, or a list of shared interests with the identified device.



Eagle Figs. 1a-1c, ¶¶[0015], [0019]-[0021]; Williams ¶96. The alert may also contain personal details about the owner of the other device, including a list of “mutual friends” (e.g., based on the list of “friends” or “likely friends”), or demographic information such as their age, sex, and religion. *E.g.*, Eagle ¶¶[0007], [0050], [0056]. At minimum, it would have been obvious to use the list of “likely

friends” to identify “mutual friends” particularly when no friends list is available. Williams ¶97. Eagle discloses that the alert message also includes “any other information which is of use in a specific application may be of use to identify, or promote communications between, nearby devices and their owners”—which includes the identified device’s list of likely friends as it can be used by the recipient device to identify potential friends in common. Eagle ¶¶[0007], [0067].⁴ For example, particularly where the identified device’s user has not provided a friends list or the friends list may be incomplete, the user of the requester device can look at the identified device’s list of likely friends to identify potential friends in common or other mutual acquaintances. Thus, a POSITA would have understood and at least found it obvious that the list of likely friends itself is sent as part of the alert message to advantageously promote communications between nearby devices and their owners. Eagle ¶¶[0007], [0067]; Williams ¶98.

Eagle also discloses using its teachings to facilitate communications with business entities. For example, **Eagle** discloses that a device in an approaching taxi will notify users that it is available, or a device embedded into a delivery vehicle will provide notices to “more efficiently service pickup/drop-off requests.” Eagle ¶[0061]. Similarly, **Eagle** discloses that the device could be in a “greeting beacon”

⁴ See also Ex. 1022 (issued Eagle Patent 7,877,082), 1:64-2:4.

at a trade show, or that it could be used by salesmen to “publicize their products and expertise.” Eagle ¶¶[0061], [0063]. Eagle discloses users, including businesses and individuals, being included on a “friends list” and in a “trust network,” and at minimum, it would have been obvious to do so in order to enable business users to enjoy these same advantageous functionalities. Williams ¶99.

Eagle is in the same field of art and is analogous art to the ’129—both are in the same field related to facilitating communications between wireless devices. E.g., ’129, 2:53-57 (“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 ¶100.

In addition, Eagle is also reasonably pertinent to the alleged problem(s) identified in the ’129 of overcoming the inaccuracies of GPS systems, and avoiding the security and privacy concerns of direct peer-to-peer communications. E.g., ’129, 2:37-45 (“[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...”), 3:58-62 (“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 ¶101.

As further discussed below, Eagle anticipates and, at minimum, renders obvious, each of the Challenged Claims. Williams ¶102.

2. Claim Chart—Eagle

'129 Claim	Eagle
[1.pre] A method for facilitating an exchange of information between first and second wireless devices or entities, the method utilizing a server performing the steps of:	To the extent the preamble is limiting, Eagle discloses a method for facilitating an exchange of information between first and second wireless devices or entities (e.g., “Bluetooth enabled cellular phones, communicate with and identify like devices that are nearby,” a “requester” and an “identified” device), the method utilizing a server (e.g., “server”). <u>E.g., Eagle:</u> Eagle discloses wireless “portable communication devices” that exchange information. <i>E.g.</i>, Eagle Abstract.

'129 Claim	Eagle
	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” to facilitate additional communications. Eagle Abstract, ¶¶[0003], [0048]. • 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.”) • [0003] (“In its preferred form, the present invention employs body-worn personal networking devices, such as <i>Bluetooth enabled cellular phones, that are able to communicate with and identify other such devices that are nearby</i>. When a device is within range of another such device, it identifies itself with unique identification value, such as a Bluetooth device address value.”) • [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>...”) See also Eagle ¶¶[0009]-[0010]. Williams ¶¶105-107.
[1.a] receiving a first unique identifier	Eagle discloses the server receiving a first unique identifier (e.g., “Requester ID”) communicated over a wide area link (e.g., “large area wireless network such as

'129 Claim	Eagle
communicated over a wide area link from the first wireless device,	a cellular phone network and/or the Internet”) 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)...”). <u>E.g., Eagle:</u> 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”). • [0004] (“Each cellular phone keeps a log of other devices that have been previously detected and, whenever a new device comes within range, <u>a notification message is transmitted to a remote server via the long-range cellular phone network. The notification message contains an identification of both the requesting device</u> and the nearby device whose presence has been detected.”) • [0010] (“The preferred embodiment ... uses personal area wireless network devices such as Bluetooth transceivers to identify social proximity <u>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</u> and to instigate person-to-person interactions between selected devices.”) • [0020] (“Each of these cellular phones is further programmed to <u>generate a notification message identifying itself, and other Bluetooth devices that come within its range,</u> as well as additional status information. The application program that executes on the cellular phone processor then <u>transmits that notification message via the long-range cellular network to a remote central server.</u>”)

'129 Claim	Eagle
	• [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), which is typically displayed as 12 hexadecimal digits as seen in Table 1 above...”) • [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>”) See also Eagle ¶¶[0003], Claim 2, Fig. 2. Williams ¶¶108-109.
[1.b] receiving a second unique identifier associated with the second wireless device, the second unique identifier associated with the second wireless device being communicated to the first wireless device over a local wireless link, and then from the first wireless device to the server over the wide area link,	Eagle discloses the server receiving a second unique identifier associated with the second wireless device (e.g., “Identified ID”), the second unique identifier associated with the second wireless device being communicated to the first wireless device over a local wireless link (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 then from the first wireless device to the server over the wide area link (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)”). <u>E.g., Eagle:</u> Eagle discloses that devices exchange identification codes using a short-range wireless link, such as Bluetooth. Eagle ¶¶[0003], [0018], [0031]. Each device receives the identification code for another device (the “Identified ID”) via Bluetooth, and includes it in the notification message sent to a server using a “long-range cellular network.” Eagle ¶¶[0004], [0020], [0048]. Thus, the requester

'129 Claim	Eagle
	device receives the Identified ID from the identified device and sends the ID to the server. <i>Id.</i> In addition, each device's identification information ("a Bluetooth identification value BTID") is part of the device's "profile data," which also includes a "name" for the device or its user. ¶[0050]. Thus, the "Identified ID" is associated with the name of the identified device or its user. <i>Id.</i>; Eagle ¶[0048]. • [0003] ("When a device is within range of another such device, <u>it identifies itself with unique identification value</u>, such as a Bluetooth device address value.") • [0004] ("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.</u>") • [0018] ("In the illustrative embodiment of the invention described in detail below, people who use the system are provided with <u>cellular telephones which incorporate short range radio transceivers that use the Bluetooth protocol to detect other nearby Bluetooth enabled devices.</u>") • [0020] ("Each of these cellular phones is <u>further programmed to generate a notification message identifying itself, and other Bluetooth devices that come within its range</u>, as well as additional status information. The application program that executes on the cellular phone processor <u>then transmits that notification message via the long-range cellular network to a remote central server.</u>")

'129 Claim	Eagle
	• [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), which is typically displayed as 12 hexadecimal digits as seen in Table 1 above...”) • [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>...”) • [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; ... (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)....”) See also Eagle Claims 2-3, Fig. 2. Williams ¶¶110-113.
[1.c] comparing a disclosure policy associated with the second unique identifier with the first unique identifier from the first wireless device or with an identifier or other data derived from the first unique identifier, wherein the disclosure policy specifies data	Eagle discloses the server comparing a disclosure policy associated with the second unique identifier (e.g., “profile data” in “[p]rofile database” “contains ... the Bluetooth identification value BTID for that device”) with the first unique identifier from the first wireless device or with an identifier or other data derived from the first unique identifier (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;” “the server fetches the profile data associated with each of the two identified devices and performs a comparison”), wherein the disclosure policy specifies data representing one or more rules for privacy of information concerning the second wireless device or privacy of information concerning an entity

'129 Claim	Eagle
representing one or more rules for privacy of information concerning the second wireless device or privacy of information concerning an entity associated with the second wireless device; and	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'”). <u>E.g., Eagle:</u> See [1.b] In addition, Eagle discloses that 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]. For example, each device is “set to only establish potential links to others within a ‘trust network.’” Eagle ¶[0066]. Thus, the “preference[s]” and “trust network” in the identified device’s “profile” represent rules for privacy of information concerning the device and its user. Eagle ¶¶[0050], [0066]. Once the server receives the notification message with the device identifiers, the server retrieves the corresponding “profiles” for the requester device and the identified device and compares them. Eagle ¶[0005]. The Requester ID is compared to the identified device’s “trust network” in order to determine whether the requester device can receive information about the identified device. Eagle ¶¶[0050], [0066]. To the extent it is argued that any further disclosure of such a comparison is required, it would have been an obvious implementation choice to do so in order to determine if the requester device is in the trust network. Williams ¶118. • [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,</i>

'129 Claim	Eagle
	<u>the server fetches the profile data associated with each of the two identified devices and performs a comparison.</u> The comparison generates a calculated value indicating the extent to which the two profiles match. This comparison operation may use different weighting schemes depending on the mode of the requesting device to determine the type of interaction to enable.”) • [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 category of data; and (f) [sic] <u>other preference data indicating, for example, the extent to which other information is the profile is sharable and under what circumstances.</u>”) • [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> ... Like other profile attributes, a user may assign a weight to the “friend list” data to indicate the relative importance that should be assigned to the fact that an encountered person may be a friend of one or more friends.”) • [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

'129 Claim	Eagle
	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.</u> Phones can be set in invisible mode so that they will never be contacted, but they can still see other people's 'public profiles' and view information indicating what they have in common. <u>A device can also be set to only establish potential links to others within a ‘trust network’.</u>”) See also Eagle ¶¶[0004], [0007], [0012], [0041], [0051]. Williams ¶¶114-118.
[1.d] communicating further information to the first wireless device as permitted by a result of comparing the disclosure policy, and wherein said further information is based, at least in part, upon a stored state resulting from previous interactions utilizing said server between the entities associated with the	Eagle discloses the server communicating further information to the first wireless device as permitted by a result of comparing the disclosure policy (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”), and wherein said further information is based, at least in part, upon a stored state (e.g., “lists of likely friends”) resulting from previous interactions utilizing said server between the entities associated with the first and second unique identifiers (e.g., “by processing proximity data, 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 as noted above”). <u>E.g., Eagle:</u>

'129 Claim	Eagle
first and second unique identifiers, and	See [1.c]. In addition, Eagle discloses that the “server” compares the profile data for the devices to determine whether to communicate an “alert message” to the requester device. <i>E.g.</i>, Eagle ¶¶[0005], [0020]. The profile data includes “inferred data” generated from previous “interaction[s]” between the devices monitored by the server, including a list of “likely friends” (a stored state) which is used to create a “trust network.” Eagle ¶[0067]. The information contained in the “alert message” is based in part on whether the recipient (the requester device) is part of the identified device’s “trust network”—otherwise, no information is sent. Eagle ¶¶[0056], [0066], [0067]. Thus, the content of the “alert message” is based, in part, on “inferred data” generated from previous interactions monitored by the server between the requester device and the identified device. Eagle ¶¶[0056], [0066], [0067]. In addition, the alert message identifies “mutual friends.” Eagle ¶[0056]. A POSITA would have understood that the list of “likely friends” is used to generate the list—thus, the further information sent in the alert message is again based on the stored state of the list of likely friends, and at minimum it would have been obvious to do so to advantageously identify additional individuals beyond a friends list as discussed in §IX.A.1. Eagle ¶[0067]; Williams ¶¶119-125. In addition, even if it were argued that the stored state itself must be sent as part of the further information, a POSITA would have understood and at least found it obvious that the list of likely friends itself is sent as part of alert message. Williams ¶¶122-125. Eagle discloses that the alert message includes “information which is of use in a specific application may be of use to identify, or promote communications between, nearby devices and their owners”—which includes the identified device’s list

'129 Claim	Eagle
	of likely friends as it can be used by the recipient device to identify potential friends in common as discussed in §IX.A.1. Eagle ¶¶[0007], [0067]. • [0007] (“The alert message may include ... any other information which is of use in a specific application may be of use to identify, or promote communications 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>”) • [0021] (“As illustrated by FIG. 1b, the alert message may advantageously include a picture of the owner of the matching nearby device that is displayed on the cellular phone's screen after the alert message is received, facilitating a personal contact between the two nearby device owners. <u>In addition, as illustrated in FIG. 1c, the alert message may include displayable data indicating common interests of the two nearby users.</u>”) • [0056] (“<u>The profile data for each user may advantageously include data specifying a set of device IDs for devices owned by “friends.”</u> The server may then identify persons who are “friends of friends” or “friends of friends of friends”. A given user may then request that alert messages be sent only when such a “trusted” person having common interests is nearby. <u>Moreover, the alert message may contain an identification of mutual friends, providing an easy way to start a</u>

'129 Claim	Eagle
	<u>conversation</u>: “So, I guess we both know Alice Green ...” Like other profile attributes, a user may assign a weight to the “friend list” data to indicate the relative importance that should be assigned to the fact that an encountered person may be a friend of one or more friends.”) • [0066] (“<u>The system allows for a large variation in the privacy constraints for these applications.</u> Phones can be set in invisible mode so that they will never be contacted, but they can still see other people's 'public profiles' and view information indicating what they have in common. <u>A device can also be set to only establish potential links to others within a 'trust network'.</u>”) • [0067] (“<u>Being able to infer relationships between people based on proximity and interaction behaviors</u> will augment a variety of existing services that currently require users to manually quantify existing relationships.... By continually monitor [sic] proximity data, <u>the phones and the server which connects them can begin to learn patterns in an individual's behavior.</u> This enables inferences to be made regarding whom the user knows and the type of relationship between everyone in their social network.... <u>Thus, by processing proximity data, 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 as noted above.</u>”) See also Eagle ¶¶[0015]-[0016], [0050], Figs. 1-2. Williams ¶122-125.
[1.e] wherein said further information	Eagle discloses that said further information (e.g., an “alert message”) additionally comprises content relating

'129 Claim	Eagle
additionally comprises content relating to one or more of the following: ... or social network content wherein said social network content is dependent upon said stored state, wherein said stored state comprises a friends list associated with the entity associated with the second wireless device, and wherein said disclosure policy utilized in said step of comparing comprises the inclusion of an entity associated with the first wireless device being included in said friends list and resulting in access to the otherwise private social network content of the entity associated	to one or more of the following: ... social network content (e.g., the alert message includes “contact information, a photograph ..., demographic data,... interests..., or any other information... [to] promote communications”) wherein said social network content is dependent upon said stored state, wherein said stored state comprises a friends list associated with the entity associated with the second wireless device (e.g., see [1.d], “lists of likely friends and acquaintances that can be used to create a trust network” associated with the profile of the identified device), and wherein said disclosure policy utilized in said step of comparing comprises the inclusion of an entity associated with the first wireless device being included in said friends list and resulting in access to the otherwise private social network content of the entity associated with the second wireless device (e.g., “alert messages...sent only when such a “trusted” person having common interests is nearby”; “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>E.g., Eagle:</u> See [1.d]. In addition, Eagle discloses that the alert message received by the requester device includes social networking content such as contact information, photographs, a list of interests, or other information of the person associated with the identified device in order to “promote communications.” Eagle ¶[0007]. The profile data for each user includes a list of “likely friends” (the “stored state” as discussed in [1.d]). The social content information included in the alert message is based on the stored state for at least the reasons discussed in [1.d]—e.g., because the alert message is shared with only devices

'129 Claim	Eagle
with the second wireless device.	in a “trust network” for the identified device created from the list of “likely friends” and the list of likely friends is sent as part of the social content information. Eagle ¶¶[0066]-[0067]. Thus, inclusion of the requester device on the “likely friends” list for the identified device results in access to otherwise private social network content of the person associated with the identified device. Eagle ¶¶[0007], [0056], [0060], [0067]. • [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.”) • [0056] (“<u>The profile data for each user may advantageously include data specifying a set of device IDs for devices owned by “friends.”</u> The server may then identify persons who are “friends of friends” or “friends of friends of 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> Moreover, the alert message may contain an identification of mutual friends, providing an easy way to start a conversation...”) • [0060] (“<u>Certain trusted devices may have profile information attributes set that entitle them to receive profile data from the server relating to a</u>

'129 Claim	Eagle
	<u>nearby individual that would not be available to the general public.</u> These devices can act as remote extensions of the server. By way of example, the invention might be used to encourage communications between attendees and exhibitors at a trade show, and a device at a registration desk may be used to automatically obtain bibliographic data from the server that describes an arriving attendee in order to facilitate the registration process.”) • [0066] (“<u>The system allows for a large variation in the privacy constraints for these applications.</u> Phones can be set in invisible mode so that they will never be contacted, but they can still see other people's ‘public profiles’ and view information indicating what they have in common. <u>A device can also be set to only establish potential links to others within a ‘trust network’.</u> Users become part of a <u>trust network when they are within one degree from an individual's social circle, i.e.: a friend-of-a-friend.</u> Trust networks can be expanded to incorporate several degrees should the user desire. Finally, a user can have the option of setting his or her profile to ‘public’. This will allow other service participants to view this person's information. <u>The public profile can be different from the main profile</u> and can be viewed as a type of proximity webpage.”) • [0067] (“Being able to infer relationships between people based on proximity and interaction behaviors will augment a variety of existing services that currently require users to manually quantify existing relationships. Devices can be implemented that are not only aware of each other, but are also infused with a sense of social curiosity. ... Thus, by

'129 Claim	Eagle
	processing proximity data, <u>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</u> as noted above.”) See also Eagle ¶[0011]. Williams ¶¶126-131.
[2] The method of claim 1 wherein the first unique identifier is associated with a person and the second unique identifier is associated with a business entity.	See [1]. Eagle discloses that the first unique identifier is associated with a person (e.g., “attendee,” “human users”) and the second unique identifier is associated with a business entity (e.g., “exhibitor at a trade show,” “greeting beacon,” “physical infrastructure,” “trucks, busses, ... or delivery vehicles,” “salesmen”). <u>E.g., Eagle:</u> Eagle discloses associating the requester device with specific people, such as the attendees at a trade show, and associating the identified device with various business entities, such as trade show organizers, delivery vehicles, or salesmen publicizing products in “professional encounters.” Eagle ¶¶[0060]-[0061], [0063]. As discussed in §IX.A.1, to the extent it is argued further disclosure is required, at minimum, it would have been obvious to extend the concept of a “friends” list and a “trust network” to include devices associated with trusted businesses. • [0060] (“By way of example, the invention might be used to encourage communications between <u>attendees and exhibitors at a trade show</u>, and a device at a registration desk may be used to automatically obtain bibliographic data from the server that describes an arriving attendee in order to facilitate the registration process.”)

'129 Claim	Eagle
	• [0061] (“Thus, for example, <u>attendees at a trade show</u> may receive special instructions or announcements whenever they come within range of a <u>greeting beacon</u> near the entrance to the show.... <u>By equipping physical infrastructure with embedded computing and a Bluetooth transceiver, human users can be notified of nearby resources</u> or facilities, such as an approaching free taxi, or a nearby public restroom. <u>Devices might also be carried by mobile platforms with embedded computers (e.g., trucks, buses. For instance, busses could wait until passengers from other busses had gotten on-board, or delivery vehicles could more efficiently service pickup/drop-off requests.</u>”) • [0063] (“For example, <u>a device carried by an attendee at trade show</u> may specify profile data designed to put the attendee in contact with experts in a particular field. <u>Salesmen can create a public profile to publicize their products and expertise.</u> Similarly, people attending a gathering of “singles” may seek a person of the opposite sex of a particular age having common interests....Thus, <u>the same user may supply profile data for use in professional encounters, and other profile data for use in social encounters.</u>”) Williams ¶¶132-135.
[3] The method of claim 1 wherein at least one of the first or second unique identifiers further comprises one or more of	See [1]. Eagle discloses that at least one of the first or second unique identifiers further comprises one or more of ... a Bluetooth Device Address (BD_ADDR) (e.g., “BD_ADDR”).... <u>E.g., Eagle:</u> See [1.a]-[1.b].

'129 Claim	Eagle
... a Bluetooth Device Address (BD_ADDR);....	In addition, Eagle discloses that the requester device and the identified device exchange unique identifiers in the form of a “Bluetooth Device Address (BD_ADDR).” • [0003] (“When a device is within range of another such device, <i>it identifies itself with unique identification value, such as a Bluetooth device address value.</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> which is typically displayed as 12 hexadecimal digits as seen in Table 1 above. Each Bluetooth device further stores and can reveal a “user friendly” displayable Bluetooth Device Name which can be up to 248 bytes long, although external devices are not expected to be able to handle or display more than 40 characters....”) <i>See also</i> Eagle ¶¶[0045], [0050]-[0051]. Williams ¶¶136-138.
[4] The method of claim 1 wherein the data in the disclosure policy specifies one or more of the following for an entity or person associated with the second device: ... disclose personal name/do not	<i>See [1].</i> Eagle discloses that the data in the disclosure policy specifies one or more of the following for an entity or person associated with the second device (e.g., “user may also set the extent to which information will be provided to requesters”): ... disclose personal name/do not disclose personal name (e.g., “a short name for ... its user”); disclose age/do not disclose age (e.g., “age”); or do or do not disclose other personal details (e.g., “demographic information,” “interests”);.... <u>E.g., Eagle:</u>

'129 Claim	Eagle
disclose personal name; disclose age/do not disclose age; or do or do not disclose other personal details; or	See [1.c]. 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. • [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.”) • [0050] (“As shown in FIG. 2 at 260, the profile database contains, for each Bluetooth device:... (c) <u>a short name for the device or its user</u> (which need not be same name as the “device name” stored in the Bluetooth device); (d) <u>contact information such as mailing address, email address</u>, web site URL, fax numbers, and importantly, the cellular phone number of the device, etc.; (e) <u>demographic information describing the device or user, such as age, sex, religion, ethnicity, height, weight, or any other values</u> which are of use in performing desired matching functions; data describing the “interests” of the device user, which can be used both to describe the user and/ or to describe the attributes of interest in another participating user;... and (f) <u>other preference data indicating, for example, the extent to which other information is the profile is sharable and under what circumstances.</u>”) See also Eagle ¶¶[0007], [0056]-[0057]. Williams ¶¶139-141.
[5] The method of claim 1 wherein the	See [1].

'129 Claim	Eagle
data in the disclosure policy specifies disclosure of information as a function of the identifier of the first wireless device as a requesting entity.	Eagle discloses that the data in the disclosure policy (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”) specifies disclosure of information as a function of the identifier of the first wireless device as a requesting entity (e.g., “alert messages...sent only when such a “trusted” person having common interests is nearby”; “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>E.g., Eagle:</u> See [1.a], [1.e]. In addition, Eagle discloses that certain profile information is shared with only certain devices in a “trust network” created from a list of “likely friends.” Eagle ¶¶[0056], [0066]-[0067]. Whether the requester device is in the “trust network” of the identified device is a function of the identifier (the “Requester ID”) of the requester device. <i>Id.</i>; Eagle ¶[0048]. Williams ¶¶142-143.
[7] The method of claim 1 additionally comprising, before the step of receiving a second identifier: setting data in the disclosure policy by an entity associated with the second wireless device.	See [1]. Eagle discloses, before the step of receiving a second identifier: setting data in the disclosure policy by an entity associated with the second wireless device (e.g., “user accesses a secure web site ... for entering and editing profile information;” “user may also set the extent to which information will be provided to requesters”). <u>E.g., Eagle:</u> See [1.b], [1.c]. In addition, Eagle discloses that the profile information for the identified device includes “preference data” set by

'129 Claim	Eagle
	the user of the identified device to indicate when information in the profile should be shared. • [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)...”) • [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 category of data; and (f) <i>other preference data indicating, for example, the extent to which other information is the profile is sharable and under what circumstances.</i>”) • [0057] (“<i>Each user may also set the extent to which information will be provided to requesters.</i> 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....”) Williams ¶¶144-146.
[10] The method of claim 1 wherein the	See [1].

'129 Claim	Eagle
further information provided to the first wireless device is dependent upon: ... a list the second wireless identifier is included on; and/or 	Eagle discloses the further information provided to the first wireless device is dependent upon: ... 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”).... <u>E.g., Eagle:</u> <i>See [1.d].</i> In addition, Eagle discloses that both the requester device and the identified device can be set to establish links only within a “trust network.” Eagle ¶[0066]. Even if the requester device is permitted to receive information by being part of the “trust network” for the identified device, the requester device will not receive an alert unless the identified device also belongs in a “trust network” created from a list of “friends” or “likely friends” for the requester device. Eagle ¶¶[0056], [0066], [0067]. • [0066] (“...The system allows for a large variation in the privacy constraints for these applications. Phones can be set in invisible mode so that they will never be contacted, but they can still see other people's ‘public profiles’ and view information indicating what they have in common. <u>A device can also be set to only establish potential links to others within a ‘trust network’.</u> Users become part of a trust network when they are within one degree from an individual's social circle, i.e.: a friend-of-a-friend....”). Williams ¶¶147-150.
[11] The method of claim 1 wherein the further information provided to the first	<i>See [1].</i> Eagle discloses the method of claim 1 wherein the further information provided to the first wireless device further comprises at least one of: a visual identifier of a service or individual (e.g., “alert message

'129 Claim	Eagle
wireless device further comprises at least one of: a visual identifier of a service or individual; information about an available service; ... a content type field specifying one or more of a picture, a media file, XML/AJAX;	may advantageously include a picture of the owner of the matching nearby device”); information about an available service (e.g., “publicize their products and expertise;” “nearby resources or facilities, such as an approaching free taxi”); ... a content type field specifying one or more of a picture (e.g., “picture”).... <u>E.g., Eagle:</u> See [1.d]. In addition, Eagle discloses that the alert message contains a photograph identifying the owner of the identified device, and/or information about products and services offered by the owner of the identified device. • [0007] (“<i>The alert message may include information identifying an encountered device or its owner, such as 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 between, nearby devices and their owners.</i>”) • [0021] (“As illustrated by FIG. 1b, <i>the alert message may advantageously include a picture of the owner of the matching nearby device</i> that is displayed on the cellular phone's screen after the alert message is received, facilitating a personal contact between the two nearby device owners. In addition, as illustrated in FIG. 1c, the alert message may include displayable data indicating common interests of the two nearby users.”) • [0061] (“Similarly, it may be desirable to transmit an alert message to users containing certain information whenever they come within range of a

'129 Claim	Eagle
	particular beacon device.... <u>By equipping physical infrastructure with embedded computing and a Bluetooth transceiver, human users can be notified of nearby resources or facilities, such as an approaching free taxi, or a nearby public restroom.</u> Devices might also be carried by mobile platforms with embedded computers (e.g., trucks, buses. For instance, busses could wait until passengers from other busses had gotten on-board, or delivery vehicles could more efficiently service pickup/drop-off requests.”) • [0063] (“The invention may be used to allow attendees at a particular event who have common interests to more easily find each other and communicate face-to-face.... For example, a device carried by an attendee at trade show may specify profile data designed to put the attendee in contact with experts in a particular field. <u>Salesmen can create a public profile to publicize their products and expertise.</u> Similarly, people attending a gathering of “singles” may seek a person of the opposite sex of a particular age having common interests....”) <i>See also</i>, Eagle Figs. 1a-1c. Williams ¶¶151-154.
[16.pre] A server apparatus for facilitating an exchange of information between first and second wireless devices or entities,	To the extent the preamble is limiting, Eagle discloses a server apparatus (e.g., “server”) for facilitating an exchange of information between first and second wireless devices or entities (e.g., “Bluetooth enabled cellular phones, communicate with and identify like devices that are nearby,” a “requester” and an “identified” device). <i>See</i> [1.pre]. Williams ¶¶155-156.

'129 Claim	Eagle
the server comprising:	
[16.a] a receiver, for receiving a first unique identifier communicated over a wide area network from the first wireless device, and for receiving a second unique identifier associated with the second wireless device, the second unique identifier associated with the second wireless device having been prior communicated to the first wireless device over a local wireless link, and then received from the first wireless device by the server over the wide area network;	Eagle discloses the server comprising a receiver (e.g., “message receiver”), for receiving a first unique identifier communicated over a wide area network from the first wireless device (e.g., “Requester ID”), and for receiving a second unique identifier (e.g., “Identified ID”) associated with the second wireless device (e.g., “a notification message is transmitted to a remote server via the long-range cellular phone network” and contains “an identification of both the requesting device and the nearby device whose presence has been detected”), the second unique identifier associated with the second wireless device having been prior communicated to the first wireless device over a local wireless link, and then received from the first wireless device by the server over the wide area network (e.g., “When a device is within range of another such device, it identifies itself with unique identification value,” using “Bluetooth,” prior to the requesting device receiving the identifier and sending it in the “notification message” to the server); <u>E.g., Eagle:</u> <i>See [1.a], [1.b].</i> In addition, Eagle discloses that the requester device sends a notification message to a server using a “long-range cellular network” that includes its own unique identifier (“Requester ID”), and the identifier received from the identified device (“Identified ID”). Eagle ¶¶[0004], [0020], [0048]. The server includes a “receiver” for receiving the notification messages. • 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

'129 Claim	Eagle
	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>") Williams ¶¶157-159.
[16.b] a data processor, for locating a disclosure policy associated with the second unique identifier and comparing the disclosure policy to the first unique identifier received from the first wireless device or with an identifier or other data derived from the first unique identifier, wherein the disclosure policy specifies data representing one or more rules for privacy of information concerning the first and second wireless devices; and	Eagle discloses the server comprising a data processor (e.g., the “remote server processes these incoming notification messages”), for locating a disclosure policy associated with the second unique identifier (e.g., “profile data” in “[p]rofile database” “contains ... the Bluetooth identification value BTID for that device”) and comparing the disclosure policy to the first unique identifier received from the first wireless device or with an identifier or other data derived from the first unique identifier (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;” “the server fetches the profile data associated with each of the two identified devices and performs a comparison”), wherein the disclosure policy specifies data representing one or more rules for privacy of information concerning the first and second wireless devices (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'”). <u>E.g., Eagle:</u> See [1.c]-[1.d]. In addition, Eagle discloses “profile data” associated with the identified device, including “preference[s] dictating what information may be shared with a requester device.

'129 Claim	Eagle
	Eagle ¶¶[0005], [0050], [0056]-[0057]. Once the server receives the notification message with the device identifiers, the server retrieves the corresponding “profiles” and compares them. Eagle ¶[0005]. The identified device’s profile must list the requester device as a “trusted” person before an alert message is sent. Eagle ¶¶[0056], [0066]-[0067]. As discussed in §§IX.A.1, a POSITA would have understood that the server comprises, and, at minimum, it would have been obvious for the server to comprise, a data processor to “process[]” the incoming notification message and perform the comparison. • [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] (“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 computes 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 matching criteria...”) Williams ¶¶160-163.
[16.c] a transmitter, for communicating further information	Eagle discloses the server comprising a transmitter (e.g., “message transmitter”), for communicating further information to the first wireless device as permitted by

'129 Claim	Eagle
to the first wireless device as permitted by the disclosure policy, and wherein said further information is based, at least in part, upon a stored state resulting from previous interactions between the entities associated with the first and second unique identifiers, and	the disclosure policy (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”), and wherein said further information is based, at least in part, upon a stored state (e.g., “lists of likely friends”) resulting from previous interactions between the entities associated with the first and second unique identifiers (e.g., “by processing proximity data, 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 as noted above”). <u>E.g., Eagle:</u> See [1.d]. In addition, Eagle discloses that the server includes a “message transmitter” for sending the alert messages. • 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>”) Williams ¶¶164-166.
[16.d] wherein said further information additionally comprises content relating to one or more of the following: ... social network content wherein said social network	See [1.e]. Williams ¶¶167-168.

'129 Claim	Eagle
content is dependent upon said stored state, wherein said stored state comprises a friends list associated with the entity associated with the second wireless device, and wherein said disclosure policy utilized in said step of comparing comprises the inclusion of an entity associated with the first wireless device being included in said friends list and resulting in access to the otherwise private social network content of the entity associated with the second wireless device.	
[17] The apparatus of claim 16 wherein the first unique identifier is associated with a person and the second unique identifier is	<i>See</i> [2], [16]. Williams ¶¶169-170.

'129 Claim	Eagle
associated with a business entity.	
[18] The apparatus of claim 16 wherein at least one of the first or second unique identifiers further comprises one or more of ... a Bluetooth Device Address (BD_ADDR);	<i>See</i> [3], [16]. Williams ¶¶171-172.
[19] The apparatus of claim 16 wherein the data in the disclosure policy specifies one or more of the following for an entity or person associated with the second device: ... disclose personal name/do not disclose personal name; disclose age/do not disclose age; or do or do not disclose other personal details; or	<i>See</i> [4], [16]. Williams ¶¶173-174.

'129 Claim	Eagle
[20] The apparatus of claim 16 wherein the data in the disclosure policy specifies disclosure of information as a function of the identifier of the first wireless device as a requesting entity.	<i>See</i> [5], [16]. Williams ¶¶175-176.
[25] The apparatus of claim 16 wherein the further information provided to the first wireless device is dependent upon: ... a list the second wireless identifier is included on; and/or 	<i>See</i> [10], [16]. Williams ¶¶177-178.
[26] The apparatus of claim 16 wherein the further information provided to the first wireless device comprises at least one of: a visual identifier of a service or individual;	<i>See</i> [11], [16]. Williams ¶¶179-180.

'129 Claim	Eagle
information about an available service; ... a content type field specifying one or more of a picture, a media file, XML/AJAX;	

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 ¶¶181-182. Indeed, as demonstrated by the prior art referenced herein, any purported problems, solutions or unexpected results in the '129 were already well known. Williams ¶182. 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 '129. Claims 1-5, 7, 10-11, 16-20, and 25-26 are anticipated or, at minimum, rendered obvious for the reasons set forth above.

Williams ¶¶183-184. There is a reasonable likelihood that Petitioner will prevail as to each of those claims. *Inter Partes* review of claims 1-5, 7, 10-11, 16-20, and 25-26 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 12,726 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 '129 patent:

VLP Law Group
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.