

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

TARGET CORPORATION,

Petitioner,

v.

PROXICOM WIRELESS, LLC,

Patent Owner.

Case IPR2020-00979

U.S. Patent No. 9,161,164

PETITION FOR *INTER PARTES* REVIEW

TABLE OF CONTENTS

LIST OF EXHIBITS..... iii

I. INTRODUCTION1

II. MANDATORY NOTICES (§42.8).....5

A. Real Party-In-Interest5

B. Related Matters.....5

C. Lead and Back-Up Counsel and Service Information6

III. PAYMENT OF FEES7

IV. REQUIREMENTS FOR INTER PARTES REVIEW.....7

A. Grounds for Standing7

B. Identification of Challenge.....7

1. The Specific Art on Which the Challenge is Based8

2. Statutory Grounds on Which the Challenge is Based.....12

3. How the Challenged Claims Are Unpatentable12

V. THE '164 PATENT12

VI. PROSECUTION HISTORY14

VII. LEVEL OF ORDINARY SKILL.....15

VIII. CLAIM CONSTRUCTION.....16

IX. GROUNDS OF UNPATENTABILITY.....17

A. Grounds 1 And 2: Mgrdechian Anticipates Claims 1-7 (Ground 1) And Renders Obvious Claims 1-8 (Ground 2)18

1. Overview of Mgrdechian19

2. Claim Chart—Mgrdechian.....25

B. Ground 3: Claims 1-8 Are Rendered Obvious By Mgrdechian In View Of Kaplan53

| | | |
|------------|--|-----------|
| C. | Grounds 4 And 5: Claims 3 And 4 Are Rendered Obvious By Mgrdechian In View Of Kulakowski (Ground 4), And In Further View Of Kaplan (Ground 5)..... | 60 |
| D. | Grounds 6 And 7: Claim 7 Is Rendered Obvious By Mgrdechian In View Of Eagle (Ground 6), And In Further View Of Kaplan (Ground 7)..... | 65 |
| E. | Grounds 8 And 9: Claim 8 Is Rendered Obvious By Mgrdechian In View Of Behrens (Ground 8), And In Further View Of Kaplan (Ground 9)..... | 68 |
| X. | SECONDARY CONSIDERATIONS | 70 |
| XI. | CONCLUSION | 71 |

LIST OF EXHIBITS

| | |
|-----------------------|--|
| Ex. 1001 | U.S. Patent No. 9,161,164 (“164”) |
| Ex. 1002 | File History of U.S. Patent No. 9,161,164 |
| 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- Ex. 1012 | Reserved |
| Ex. 1013 | International App. No. WO 2007/084973 (“Kulakowski”) |
| Ex. 1014 | U.S. Patent No. 6,446,208 (“Gujar”) |
| Ex. 1015 | U.S. Patent Application Publication No. 2010/0138481 (“Behrens”) |
| 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. Leedarson 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 Application Publication No. 2005/0174975 (“Mgrdechian ’975”) |
| Ex. 1024 | U.S. Patent No. 8,295,819 (“Kaplan”) |
| Ex. 1025 | Reserved |
| Ex. 1026 | Declaration of Crena Pacheco |
| Ex. 1027 | Office Action Response in U.S. Ser. No. 11/055,310 (“Mgrdechian Office Action Response”) |
| Ex. 1028 | File History of U.S. Patent No. 8,370,955 (“’955 File History”) |
| Ex. 1029 | File History of U.S. Patent No. 9,038,129 (“’129 File History”) |
| Ex. 1030 | Reserved |
| Ex. 1031 | File History of U.S. Patent No. 8,849,698 (“’698 File History”) |
| Ex. 1032 | <i>Proxicom Wireless, LLC v. Target Corp.</i> , No. 6:19-cv-01886-RBD-LRH, Dkt. 64 (M.D. Fl. May 22, 2020) |

Pursuant to §§311-319 and §42,¹ Target Corporation (“Petitioner”) petitions for *inter partes* review (“IPR”) of claims 1-8 (“Challenged Claims”) of U.S. Patent 9,161,164 (“’164”) (Ex. 1001), assigned to Proxicom Wireless (“PO”) according to USPTO records. There is a reasonable likelihood 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 ’164’s purported invention is the “use of proximity beacons” to “facilitat[e] the exchange of information” between two entities associated with two wireless devices. ’164, 2:60-64, cl. 1. In particular, a first wireless device determines the proximity of a second wireless device by comparing identifier(s) provided by a server to the first wireless device via “a long range wireless capability” with identifier(s) received via a “short range” wireless capability. *Id.*; Williams ¶¶1-2, 39.

The ’164 admits that, prior to the alleged invention, wireless devices already were configured to use “both a short range and long range wireless capability” claimed in the ’164. *Id.*, 2:18-30 (admitting “[m]ost mobile phones on the market

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

today support at least two wireless standards; one for the cellular wireless wide area connection (WWAN) and one for a wireless personal or local area network” such as “Bluetooth”). And the ’164 admits that prior art systems already were using wireless devices for e-commerce and social networking applications. *Id.*, 2:1-4, 2:31-40; Williams ¶¶5, 7, 40-42, 60.

The only purportedly novel elements of the ’164 claims are the specific recitations of using a server to enforce a disclosure policy between a first and second wireless device. *Id.*, cl. 1. For example, independent claim 1 recites a server locating a “disclosure policy,” which “specifies...rules for privacy of information concerning the first wireless device” (or associated entity) and “the second wireless device” (or associated entity), associated with the second wireless device’s identifier or an associated entity’s account. *Id.* The server discloses information (including the second wireless device’s identifier) to the first wireless device only if permitted after “comparing the disclosure policy” to the first wireless device’s unique identifier or associated entity’s account data. *Id.* If that disclosure is permitted, the first wireless device then uses the received identifier to determine the proximity of the second wireless device. *Id.* But, as discussed herein, it was already well-known to use a server to invoke a privacy-related disclosure policy to limit disclosure of information (including identifiers) between two wireless devices, one of which then uses the information to determine the proximity of the second device. Williams ¶¶42-58.

For example, **Mgrdechian** (Ex. 1005) discloses all the claimed features of '164 claims 1-7, and renders all Challenged Claims obvious, including a server that locates privacy-related filter parameters for a target device, compares those parameters to the profile of an initiating device, and discloses the identifier and public profile information of the target device to the initiating device only as permitted by those parameters. If that disclosure is permitted, the initiating device determines the target device's proximity and lookup profile information about the target device based on the received identifier. Williams ¶¶49, 52-53, 57, 78, 80-158.

To the extent it is argued further disclosure beyond **Mgrdechian** is required for the Claims, **Kaplan, Kulakowski, Eagle, and Behrens** make express what a POSITA would have also understood from **Mgrdechian's** teachings. Williams ¶78. As to claims 1-8, **Kaplan** (Ex. 1024) discloses implementation details such as comparing incoming identifiers with stored information from a server, as discussed in §IX.B. As to claims 3-4, **Kulakowski** (Ex. 1013) discloses secure and fraud resistant application of privacy-related disclosure policies through use of changing, covert identifiers, as discussed in §IX.C. Williams ¶¶185-199. As to claim 7, **Eagle** (Ex. 1004) discloses implementation details such as disclosing information only to users within a trust network as discussed in §IX.D. Williams ¶¶48, 200-205. As to claim 8, **Behrens** (Ex. 1015) discloses beacons broadcasting MAC addresses and identifiers, as discussed in §IX.E. Williams ¶¶206-214.

Thus, as demonstrated herein, **Mgrdechian** anticipates claims 1-7 and, at minimum, renders obvious all the Challenged Claims. At best, the Challenged Claims of the '164 are directed to an obvious combination of prior art elements combined according to known methods to yield predictable results. The claimed elements and the claimed arrangement of elements were anticipated by **Mgrdechian** art and/or rendered obvious by **Mgrdechian** alone or in view of Kaplan, Kulakowski, Behrens and/or Eagle. At best, the combination amounts to nothing more than a predictable use of prior art elements according to their established functions.

The USPTO did not apply **Mgrdechian, Kaplan, Eagle, Kulakowski, or Behrens** or any other reference providing analogous disclosures during prosecution of the '164. Had such references been 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 '164, 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 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 '164 by utilizing instrumentalities provided at least in part by Acuity Brands (“Acuity”), but Acuity is not funding, controlling, directing, or otherwise involved in this petition or proceeding, nor has it been in the past.

B. Related Matters

Proxicom Wireless, LLC v. Target Corp., 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 |
| 7,936,736 | IPR2020-00904 |
| 8,090,359 | IPR2020-00931 |
| | IPR2020-00932 |
| 8,374,592 | IPR2020-00933 |
| 8,385,896 | IPR2020-00934 |
| 8,116,749 | IPR2020-00978 |

| | |
|-----------|---------------|
| 8,385,913 | IPR2020-00980 |
| 8,369,842 | IPR2020-00977 |

C. 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. 001008-0037-659.

IV. REQUIREMENTS FOR INTER PARTES REVIEW

A. Grounds for Standing

Pursuant to §42.104(a), Petitioner certifies that the '164 is available for IPR. Petitioner is not barred or estopped from requesting IPR challenging the claims of the '164 on the grounds identified herein.

B. Identification of Challenge

Pursuant to §42.104(b), Petitioner requests IPR of claims 1-8 of the '164, and that the Board cancel the same as unpatentable. The '164 matured from U.S. Application 14/472,477 (filed 08/29/2014), and claims priority to U.S. provisional applications 61/095,001 (filed on 9/8/2008) and 61/095,359 (filed on 9/9/2008).² Williams ¶¶4, 76-77.

² Petitioner takes no position as to, and reserves its right to challenge, the propriety of the priority claims because the art presented herein predates the earliest possible filing of the '164 patent.

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 |
|--------------------------|---------|------------------------------------|------------|-----------------------|-----------------------------------|
| Mgrdechian | 1005 | U.S. 7,545,784 | 2/10/2005 | 6/9/2009 | §102(e) |
| Kaplan | 1024 | U.S. 8,295,819 | 12/19/2005 | 10/23/2012 | §102(e) |
| Eagle³ | 1004 | U.S. 2005/0250552 | 5/5/2005 | 11/10/2005 | §102(b) |
| Kulakowski | 1013 | International WO 2007/084973 | 1/19/2007 | 7/26/2007 | §102(b) |
| Behrens | 1015 | U.S. 2010/0138481 | 4/30/2008 | 6/3/2010 | §102(b) |

Although U.S. Patent Application Publication No. 2005/0174975 (“Mgrdechian ’975”) (**Mgrdechian’s** pre-grant publication) (Ex.1023) (prior art under §102(b)) was cited in an Information Disclosure Statement (Ex. 1002, 73, 136 (’164 File History)), it was not applied to reject the claims during prosecution of ’164 (*id.*, 105-109). And while Mgrdechian ’975 was applied during prosecution of related U.S. Patent Nos. 8,370,955 (’955) (Ex. 1028, 91-110, 147-69, 249-72) and 9,038,129 (’129) (Ex. 1029, 141-67, 292-317), neither application warrants exercise

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

of discretion under §325(d) as '955 and '129 are not parents of '164, have different claims, and were examined by different examiners.

During prosecution of '955, the examiner thrice rejected the claims over Mgrdechian '975—twice as *anticipating* the independent claims. Ex. 1028, 91-110, 147-69, 249-72. After the second anticipation rejection, the applicant added a new claim (prosecution claim 35) reciting several features not found in the '164 Challenged Claims, such as receipt of various messages related to initiation and completion of a multistep electronic commerce transaction with a merchant. Ex. 1028, 226-27. After this new claim 35 was deemed allowable, the applicant canceled all other pending claims to which Mgrdechian '975 had been applied, tacitly conceding those claims were unpatentable over Mgrdechian '975. Ex. 1028, 327, 333. Because '955's issued claims recite features not present in the '164 Challenged Claims, the '955 prosecution is relevant to '164 only in that the applicant never succeeded in overcoming Mgrdechian '975 as to the canceled claims.

Additionally, '129 is not a parent application to '164, so the '164 examiner would not have automatically considered the '129 office actions under MPEP §609.II.A.2 and would have had reason to be aware of the office actions only if the office actions themselves were cited in an IDS. Although the applicant did cite numerous office actions in an IDS filed in the '164 prosecution (Ex. 1002, 77-79), the '129 office actions applying Mgrdechian '975 were not cited, nor were any '129

office actions. Accordingly, the '129 office actions applying '975 were not before the '164 examiner.

Although the applicant cited Mgrdechian '975 and certain '955 office actions applying Mgrdechian '975 (cited as “Office Action; U.S. Application No. 13/015,306”) in IDSs in '164's prosecution, these citations did not identify any particular portions of the disclosures relevant to '164's claims, and the '164 examiner did not rely on **Mgrdechian** or Mgrdechian '975 during the '164 prosecution. Ex. 1002, 71-79, 105-109, 124-130, 134-142. These bare citations in IDSs do not warrant exercise of discretion under §325(d). *Vizio, Inc. v. Nichia Corp.*, IPR2017-00551, Paper 9, *7-8 (no evidence that references cited in IDS were applied against the challenged claims or that examiner considered particular disclosures cited by Petitioner); *Microsoft Corp. v. Parallel Networks, LLC*, IPR2015-00486, Paper 10, *14-15 (same).

None of the other references was cited in an IDS or otherwise identified by the Examiner, or applied in a rejection of the claims during prosecution of the '164. The Examiner never considered the grounds presented herein or the testimony of Petitioner's expert David 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). Even if Mgrdechian '975 had been considered, the Examiner would have had to err by not rejecting the Claims for the reasons explained herein and the Board should not exercise its discretion under §325(d). 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 '164, PO served its infringement contentions on 2/10/2020, identifying 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) while the challenged claims are all asserted in the litigation currently, that may change before institution; (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 applied 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 | Mgrdechian | §102 | 1-7 |
| 2 | Mgrdechian | §103 | 1-8 |
| 3 | Mgrdechian in view of Kaplan | | 3-4 |
| 4 | Mgrdechian in view of Kulakowski | | 7 |
| 5 | Mgrdechian in view of Kaplan and Kulakowski | | 8 |
| 6 | Mgrdechian in view of Eagle | | |
| 7 | Mgrdechian in view of Kaplan and Eagle | | |
| 8 | Mgrdechian in view of Behrens | | |
| 9 | Mgrdechian in view of Kaplan and Behrens | | |

3. How the Challenged Claims Are Unpatentable

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

V. THE '164 PATENT

The '164 describes techniques for using a server to exchange information between wireless devices. '164, Abstract; Williams ¶¶6, 39 59. The background section of the '164 concedes that wireless devices, such as mobile phones, had access to both a “personal or local area network” using the “Bluetooth” standard and a “wide area” cellular connection. *E.g.*, '164 1:33-37, 2:11-23, 2:33-34, 2:18-30. Using these two well-known communication methods for “both a short range and a long range wireless capability,” the '164 is directed to exchanging information

between two wireless devices using a server. *E.g.*, '164, 2:60-64; Williams ¶¶35, 40-42, 60.

The '164's embodiments discuss a variant of the same general functionality: (1) a server (a) locating a disclosure policy for a second wireless device or associated entity, comprising rule(s) for privacy of information, (b) comparing the "disclosure policy" with an identifier associated with the first wireless device or an associated entity's data; and (c) providing "first information" about the second wireless device to the first wireless device, but only "as permitted by the disclosure policy;" and (2) the first wireless device determining receipt of the second wireless device identifier via a local or personal area wireless protocol. For example, Figure 1 of the '164 shows that "a central server 100 is connected to devices 106 and 108" through a combination of the Internet and a "cellular network 102." *E.g.*, '164, 5:44-62. The devices are also able to communicate directly with each other via "a local, or personal area network wireless protocol such as...Bluetooth." *E.g.*, '164, 19:43-56.

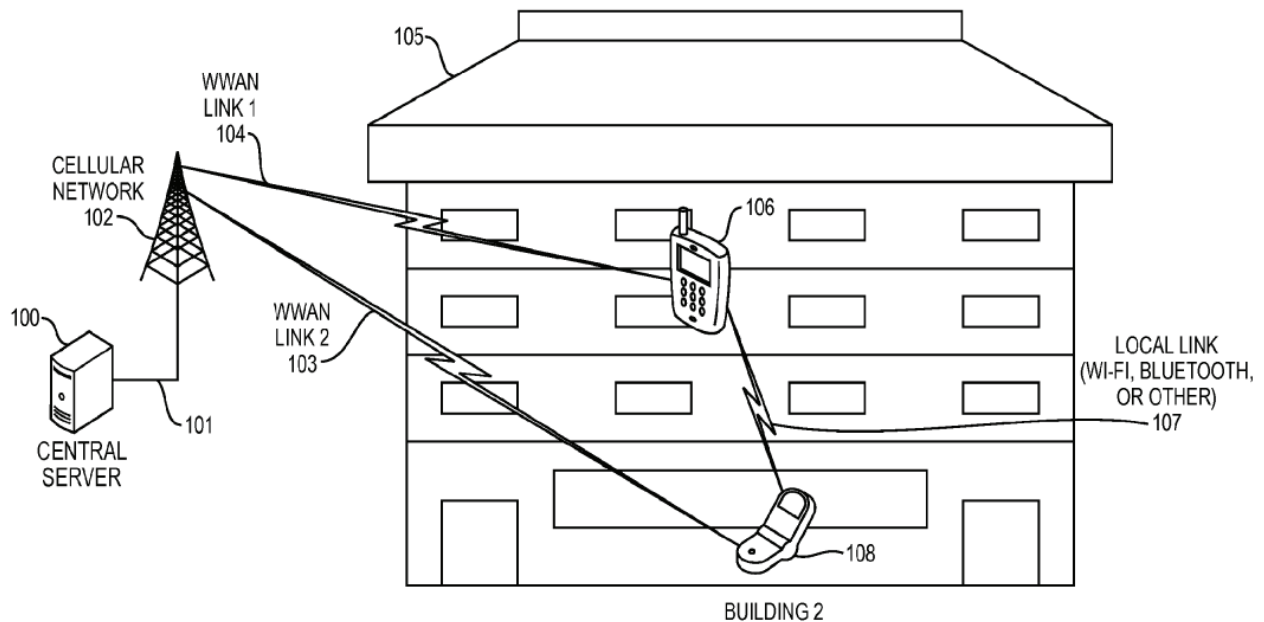


Figure 1

E.g., '164 Fig. 1. The '164 states that “[r]eliance on a central server...allows the secure and fraud resistant application of disclosure policy.” *E.g.*, '164 4:41-42; Williams ¶¶61-66.

The '164 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* '164, 3:30-40, 4:41-58; Williams ¶65.

VI. PROSECUTION HISTORY

U.S. Patent Application 14/472,477, which matured into the '164, was filed on 08/29/2014. '164, (22). The Examiner issued a Restriction Requirement on 12/05/2014. In an Amendment filed 1/16/2015, applicant elected prosecution claims

1-10 and 16-21 (issued claims 1-16). Ex. 1002, 120. A Notice of Allowance issued 06/08/2015. *Id.*, 124-130. While no reason for allowance was provided, *id.*, the prosecution of the parent shows that the '164 claims were allowed because of their required disclosure policy that specifies rules for privacy of information. Williams ¶¶3, 67-69.

To traverse prior art during prosecution of the parent (U.S. Application 13/775,435 (matured into U.S. Patent 8,849,698)), applicant both (1) amended claims to require disclosure of certain merchants and (2) added new claims with disclosure policies that included rules for privacy of information. '698 File History (Ex. 1031), 173-186. The amended claims were allowed because of added limitations not at issue here involving merchants. *Id.*, 196-203; Williams ¶70. Applicant cancelled the “new” privacy claims in the parent, and refiled them in a continuation that became the '164. *Compare, e.g., id.*, 176-178 (claim 16), *with* '164 claim 1; Williams ¶71.

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 ¶¶8-20, 36-38.

VIII. CLAIM CONSTRUCTION

Terms of claims subject to IPR are to be construed using the same claim construction standard as in district court. §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. Williams ¶¶21-24, 72.

The parties have submitted proposed constructions in the underlying litigation, which do not impact the outcome of this IPR as the prior art meets each proposed construction for the reasons discussed below. *See* Ex. 1032; Williams ¶72. While the Challenged Claims use terms of degree (e.g., “local or personal area wireless protocol”), the prior art relied on herein discloses the ’164’s examples of those terms as shown in §IX below. *See, e.g.*, ’164, 19:49-51 (“a local, or personal area network wireless protocol such as...Bluetooth”); Williams ¶¶73-75.

A district court in another proceeding has construed terms of a related patent, but these constructions do not impact the outcome of this IPR. *See* Ex. 1021; Williams ¶72.

IX. GROUNDS OF UNPATENTABILITY

The '164 is directed to a system for facilitating communications between two wireless devices through a server. At their core, the claims recite (1) a server (a) locating a disclosure policy for a second wireless device or associated entity, comprising rule(s) for privacy of information, (b) comparing the “disclosure policy” with an identifier associated with the first wireless device or an associated entity’s data; and (c) providing “first information” about the second wireless device to the first wireless device, but only “as permitted by the disclosure policy;” and (2) the first wireless device determining receipt of the second wireless device identifier via a local or personal area wireless protocol. Claims 1-7 are anticipated and, at minimum, all Challenged Claims are obvious in view of the prior art cited herein, as explained below. Williams ¶¶61, 78.

For example, **Mgrdechian** discloses a system for using a server to facilitate communications between Bluetooth-enabled devices. **Mgrdechian** discloses all the claimed features of '164 claims 1-7, and at minimum renders all Challenged Claims obvious. Williams ¶¶79-80. **Mgrdechian**'s server locates privacy-related filter parameters for device C, compares those parameters to the profile of device A, and discloses the identifier and public profile information of device C to the device A only as permitted by those parameters, such that device A can both (1) determine device C's proximity when it comes within range and (2) look up profile information

about device C, as permitted by the filter parameters, based on its received “dynamic” identifier. *See* §IX.A.

To the extent it is argued that further disclosure is required beyond **Mgrdechian**, a POSITA would have been motivated to apply **Kaplan’s** implementation detail teachings of separate Bluetooth and cellular radios as well as comparing received identifiers to previously stored information before retrieving additional information from the server; **Kulakowski’s** teachings of using dynamic identifiers to ensure secure communications between wireless devices for claims 3-4; **Eagle’s** teachings of using a trusted friends lists to limit disclosure of private information for claim 7; and **Behrens’s** teachings of sending multiple identifiers between devices including a “MAC address” for claim 8. *See* §§IX.B-E, respectively; Williams ¶79.

As shown below, the prior art renders the Challenged Claims 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 ’164. Williams ¶¶25-227.

A. Grounds 1 And 2: Mgrdechian Anticipates Claims 1-7 (Ground 1) And Renders Obvious Claims 1-8 (Ground 2)

Mgrdechian anticipates claims 1-7 and renders obvious claim 8. However, as further described below for particular limitations, to the extent it is argued that

further evidence is required, a POSITA would have found the limitations obvious in view of Mgrdechian—rendering all Challenged Claims obvious. Williams ¶¶80-158.

1. Overview of Mgrdechian

Mgrdechian discloses a “wireless communication system” that enables “exchange of information between wireless devices” using a “server” (computer system 360), *e.g.*, as illustrated in Fig. 3A. Mgrdechian, 1:32-35, 10:48-56; Williams ¶81.

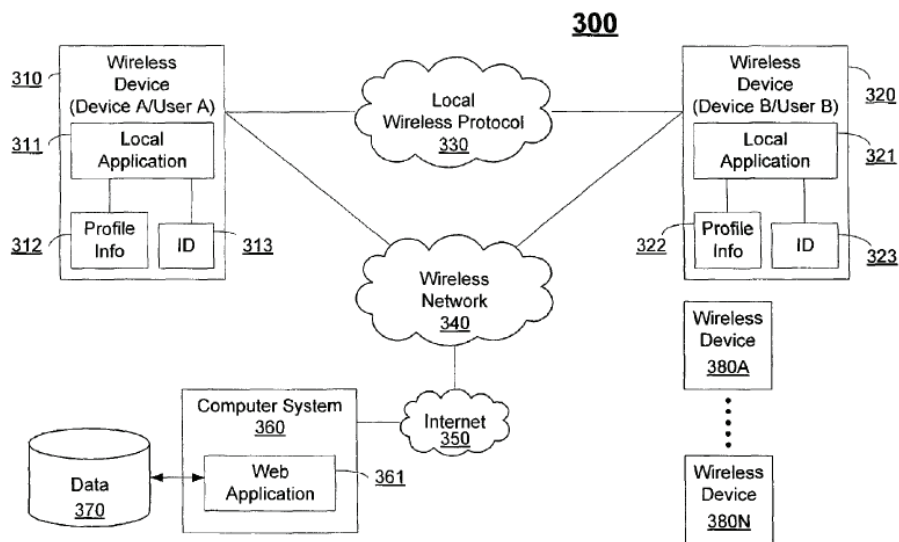


Fig. 3A

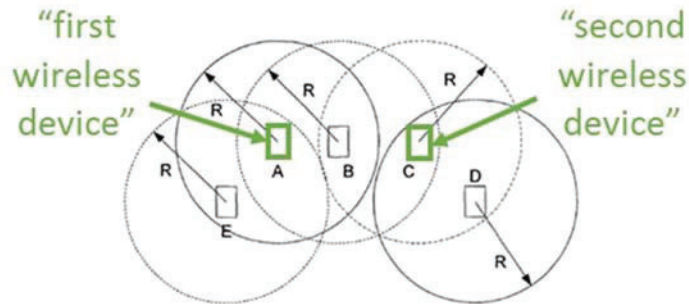
Mgrdechian discloses that each “mobile wireless device” “continuously or intermittently broadcast[s] its ID and/or other information” for detection by other wireless devices via a “local wireless protocol” (*e.g.*, “Bluetooth”), thus acting as

proximity beacon transmissions. *Id.*, 3:38-42, 6:59-61, 10:8-15, 22:26-35. These identifiers are “static, dynamic, or pseudo-random.” *Id.*, 5:1-3; Williams ¶82.

Mgrdechian discloses that an initiating wireless device (e.g., device A) receiving an identifier from a target wireless device (e.g., device B) sends the initiating device’s and the target device’s identifiers to the server to retrieve profile information for the target device. Mgrdechian, 3:13-25, 19:13-25, 20:1-47. The initiating device may receive many identifiers, such as when users congregate in an area. Mgrdechian 6:44-50, 17:51-56; Williams ¶84. The server uses the identifiers to retrieve profile information for each device. Mgrdechian, 13:50-8. Each profile contains a privacy-related disclosure policy—“filter parameters” and information designated “non-public,” such that it “may not be disclosed.” Mgrdechian, 13:50-14:8, 16:60-17:10. Before returning profile information to an initiating device, the server compares the initiating device’s and target device’s filter parameters to determine the information that it may disclose or must withhold. *Id.*, Fig. 7A, 13:50-14:8, 20:1-47. For example, the profiles each include “a list of friends,” which are compared to generate a list of “mutual friends” to send to the initiating device, in a “social networking application” if permitted by the “filter parameters.” Mgrdechian, 11:23-41, 13:50-14:8. For example, where device C’s “filter parameters” designate its “list of friends” as “non-public” for users not on that list, then the list would be

shared with device A only if device A’s user is included in device C’s “list of friends.” *Id.*, 11:23-34, 13:50-14:8, 16:60-17:10; Williams ¶85.

The server also sends to the initiating device (device A) the identifier and profile information (if permitted) of users “active within one hop.” Mgrdechian, 20:1-47. For example, as shown in the figure below, device B is “within range” of device A because it is reachable via protocol of limited range “R,” but device C is “within one hop” of device A because it is reachable by device B:



| Device | Devices in Range |
|--------|------------------|
| A | B, E |
| B | A, C |
| C | B, D |
| D | C |
| E | A |

~ 1000

Fig. 10

Id., 20:21-30, Fig. 10. Thus, the server, upon receiving device B’s identifier from device A, returns public profile information and identifiers for devices B and C (if

permitted by their filter parameters). *Id.*, 20:1-47; Williams ¶86. The wireless device saves “[s]ome or all of the [received] profile information” locally such that it can later “search for saved profiles.” *Id.*, 12:18-26, 20:56-21:6. For example, when device C, which was initially one hop away, later comes within range of device A, device A receives device C’s ID (thus detecting its proximity), compares it to the “saved profiles,” and refrains from requesting information already received from the server. Mgrdechian, 12:18-26, 20:56-21:6, Figs. 3A, 11. For example, when device A reviews profiles saved locally and decides to message now-in-range device C directly, device A directly messages device C using device C’s ID—e.g., its Bluetooth ID. Mgrdechian 5:31-35, 12:48-50, 13:32-34. A POSITA would have understood, or at minimum found it obvious, for the device ID, such as the Bluetooth ID, to be included with the profile information to facilitate the identification of saved profiles and direct communication between the wireless devices. Mgrdechian 5:31-35, 12:48-50, 13:32-34; Williams ¶87.

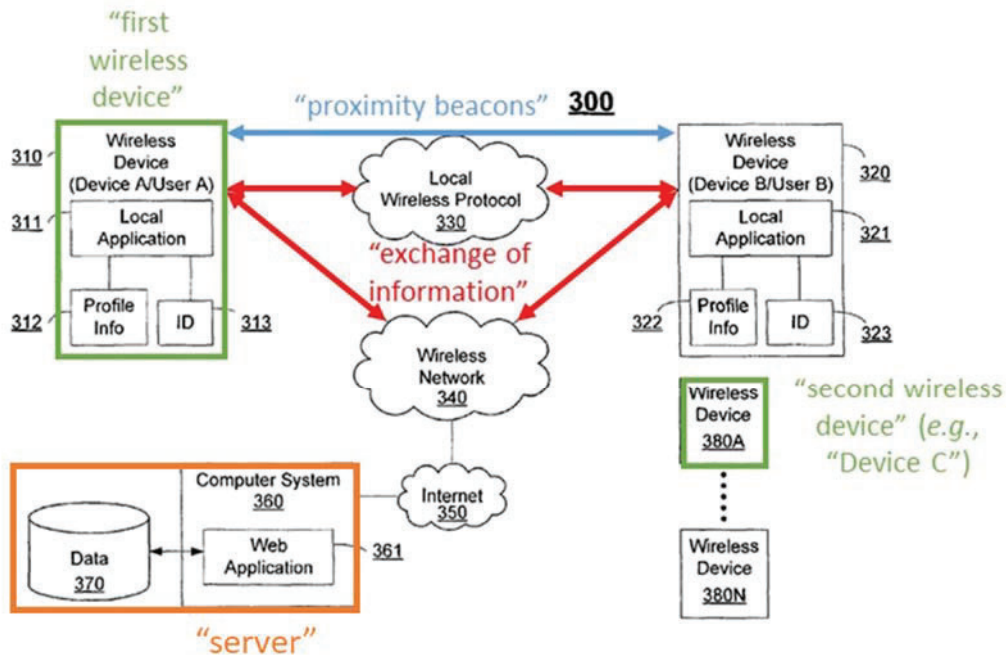


Fig. 3A

Mgrdechian further discloses that in some instances device A only receives and saves a “summary profile” of device C, but can subsequently request device C’s “complete” profile from the server, e.g., “based on the picture and initial information” in the “summary profile.” Mgrdechian, 12:18-26, 20:56-21:6, 17:28-43; Williams ¶88.

Mgrdechian discloses that the computer system 360 is either a single server or multiple servers. *Id.*, 7:23-32, 10:48-61. A POSITA would have understood or, at minimum, found it an obvious implementation choice, that the server performs its steps using a server data processor. *Id.* cl. 27; Williams ¶89. Indeed, the ’164 admits

that “[t]he internal structure of ... server 100 includes one or more data processors...that are well known in the art...” ’164, 6:10-15.

Mgrdechian further discloses that each wireless device includes “RF circuitry” for “receiv[ing]” and “transmit[ting]” “RF signals.” Mgrdechian, 21:65-22:12. A POSITA would have understood, or at minimum found it to be an obvious implementation choice, for the Bluetooth and cellular radios that perform these transmissions to be separate. *Id.*, 6:59-61, 21:65-22:12, Figs. 8, 13; Eagle (Ex. 1004), cl. 2 (e.g., “short range radio receiver” and “long range communications interface”); Williams ¶90. Indeed, the ’164 specification admits, “[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 (WPAN, WLAN).” ’164, 2:18-30, *see also* 1:33-37.

The device-to-device transmissions can include “device IDs,” “Bluetooth IDs,” a “unique ID [assigned] in the manufacturing process,” including a MAC address, and “initial profile information.” *Id.*, 15:55-62, 16:16-33; Williams ¶82. A POSITA would have also found it obvious and straightforward to include multiple identifiers in the transmission to facilitate communication between the devices. *Id.*, 4:65-5:1, 12:26-44; Behrens, ¶¶103, 122 (“[a] user may...exercise control over...how many UIDs are transmitted by his device.”); Williams ¶83.

Mgrdechian is in the same field of art and is analogous art to '164—both are in the same field related to wireless communication systems. *E.g.*, '164, 2:60-64; Mgrdechian, 1:32-35; Williams ¶91.

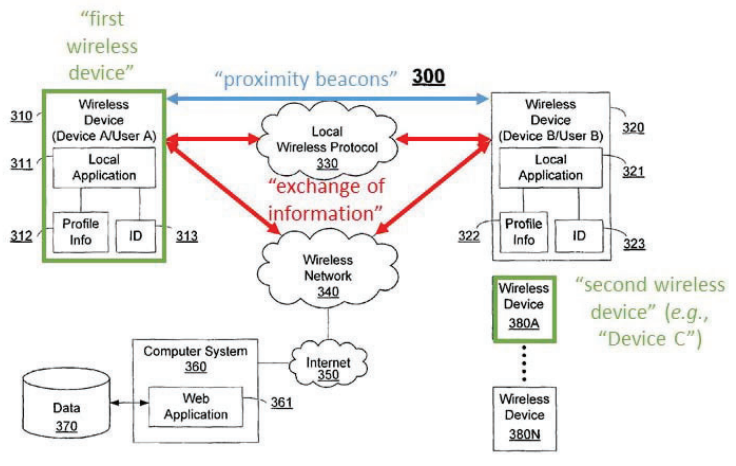
In addition, Mgrdechian is reasonably pertinent to the alleged problem(s) identified in '164 of overcoming the alleged inaccuracies of GPS systems, and avoiding the alleged security and privacy concerns of direct peer-to-peer communications. *E.g.*, '164, 2:47-52, 3:66-4:3; Mgrdechian 4:40-47, 9:56-60; Williams ¶92.

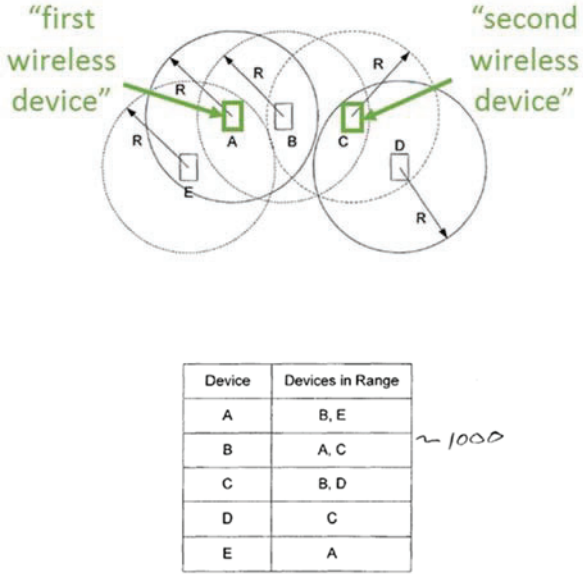
As further discussed below, Mgrdechian anticipates, and at minimum renders obvious, all Challenged Claims. Williams ¶93.

2. Claim Chart—Mgrdechian

| Claim Element | <u>Mgrdechian</u> |
|--|--|
| [1.pre] A system for facilitating use of proximity beacons for the exchange of information between a first wireless device or a first entity associated with the first wireless device and a second wireless device or a second entity associated with the second wireless | <p>Mgrdechian discloses a system (<i>e.g.</i>, “wireless communication system”) for facilitating use of proximity beacons (<i>e.g.</i>, “a device may continuously or intermittently broadcast its ID and/or other information without having received an inquiry”) for the exchange of information (<i>e.g.</i>, “exchange of information between wireless devices”) between a first wireless device or a first entity associated with the first wireless device (<i>e.g.</i>, “first wireless device,” “device A”) and a second wireless device or a second entity associated with the second wireless device (<i>e.g.</i>, “other wireless device[],” “device C”).</p> <p><u>E.g., Mgrdechian:</u></p> <p>Mgrdechian discloses a “wireless communication system” that enables “exchange of information between</p> |

| Claim Element | <u>Mgrdechian</u> |
|--------------------------------|--|
| device, the system comprising: | <p>wireless devices” (e.g., “device A,” “device C”). Mgrdechian, 1:32-35, 20:1-47. Such information includes unique “wireless device identifications” and “information associated” with those identifiers, such as profile information. <i>Id.</i>, 3:34-35, 3:59-67, 11:57-58. Each wireless device may “continuously or intermittently broadcast its ID and/or other information”—e.g., allowing device A to detect device B because it is “within range.” <i>Id.</i>, 6:59-61, 9:65-10:5. Device A sends device A’s and B’s unique IDs to a server. <i>Id.</i>, 20:1-47. In response, the “server” “return[s]” profile “information associated with” “all users active within one hop,” including devices B and C. <i>Id.</i></p> <ul style="list-style-type: none"> • 1:32-35 (“The present invention relates to...<u>a wireless communication system and method that provides an exchange of information between wireless devices.</u>”) • 3:59-67 (“<u>[R]eceiving in a first wireless device one or more wireless device identifications associated with one or more other wireless devices...and receiving information associated with the one or more wireless device identifications from the remote computer system in the first wireless device.</u>”) • 6:59-61 (“<u>[A] device may continuously or intermittently broadcast its ID and/or other information without having received an inquiry.</u>”) • 9:65-10:5 (“<u>[F]irst wireless device 310 may wirelessly communicate with wireless devices 390A-N that are within range of device 310...communication using protocol 301 is dynamic because as users of the wireless devices move, new devices may be detected as they come within range and other devices may become undetectable as they move out of range.</u>”) |

| Claim Element | <u>Mgrdechian</u> |
|---------------|--|
| | <ul style="list-style-type: none"> <li data-bbox="586 317 1416 737"> <p>20:1-47 (“<i>[W]hen device A initiates an identification request, devices B and E return their device IDs, which are subsequently sent to the remote computer....[T] remote computer can further determine that device C is in range of device B. If the system is programmed to return all users active within one hop, the system may automatically use device C's ID and return information associated with device C's ID to device A.</i>”)</p> <li data-bbox="586 758 764 800"> <p>Fig. 3A:</p>  <p>The diagram illustrates a network system. On the left, a 'first wireless device' (310) contains a 'Wireless Device (Device A/User A)' (310), a 'Local Application' (311), and 'Profile Info' (312) and 'ID' (313) components. On the right, a 'Wireless Device (Device B/User B)' (320) contains a 'Local Application' (321) and 'Profile Info' (322) and 'ID' (323) components. A 'Local Wireless Protocol' (330) is shown between these two devices, with a blue double-headed arrow labeled 'proximity beacons' (300) and red double-headed arrows labeled 'exchange of information'. Both devices are connected to a 'Wireless Network' (340). The network is connected to the 'Internet' (350). A 'Computer System' (360) with a 'Web Application' (361) and 'Data' (370) is connected to the Internet. A 'second wireless device' (380A) is also shown, along with other devices (380N).</p> <li data-bbox="586 1381 756 1423"> <p>Fig. 10:</p> |

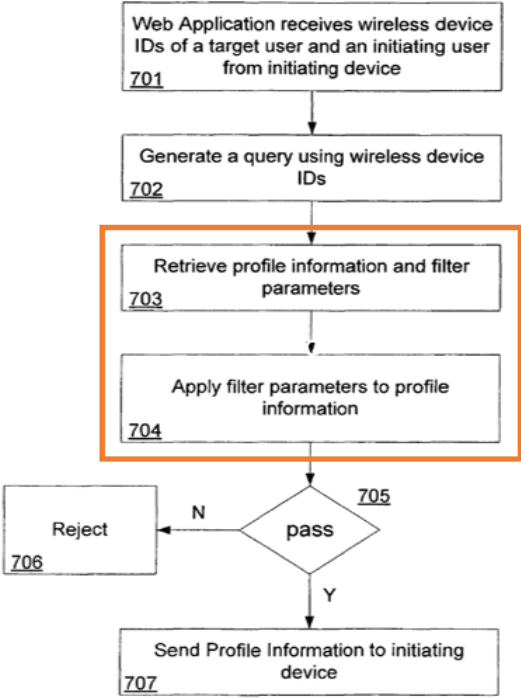
| Claim Element | <u>Mgrdechian</u> |
|--|---|
| |  <p style="text-align: center;"><i>Fig. 10</i></p> <ul style="list-style-type: none"> • <i>See also</i> 3:34-35, 9:40-55, 10:48-56, 11:57-58, 19:34-39, Fig. 4. <p>Williams ¶¶94-97.</p> |
| <p>[1.a] at least one server for providing a second unique identifier associated with an account associated with the second entity comprising:</p> | <p>Mgrdechian discloses the system comprising at least one server (e.g., “server”) for providing a second unique identifier associated with an account associated with the second entity (e.g., “return all users active within one hop, the system may automatically use device C’s [unique] ID and return information associated with device C’s ID to device A”).</p> <p><u>E.g., Mgrdechian:</u></p> <p>See [1.pre].</p> <p>In addition, Mgrdechian discloses that part of the profile information for devices B and C “return[ed]” by the server includes the “unique” identifier for device C (the second unique identifier), such that device C’s profile can be “saved” on device A and accessed based on its identifier, and such that device A uses the identifier to message</p> |

| Claim Element | <u>Mgrdechian</u> |
|---------------|---|
| | <p>device C directly once device C comes into range. Mgrdechian, 3:34-35, 12:18-26, 13:32-34, 20:1-47. At minimum, it would have been obvious to do so for this same reason as discussed in §IX.A.1. <i>Id.</i>; Williams ¶102; <i>see also</i> discussion of [1.g].</p> <ul style="list-style-type: none"> • 3:34-35 (“<u>the one or more wireless device identifications are unique identifications</u>”) • 7:19-21 (“[t]he response [of the server] will be in the form of images or other identifiers of users within a specified range of User A.”) • 8:5-14 (“(e.g., as part of the server) a web-based user interface for registration and profile management. Information provided by users...would include,...the <u>Bluetooth ID of their mobile device</u>,...”) • 10:48-56 (“[R]emote computer system 360...may be an Internet <u>server</u> computer....”) • 12:18-26 (“[C]omputer system 360 may send some or all of the <u>profile information associated with each device ID back to the initiating wireless device (e.g., Device A)</u>,...Profile information for one or more targets may be stored internally on a wireless device.... <u>Some or all of the profile information may be saved</u> (e.g., as a complete profile or as a summary profile).”) • 13:32-34 (“At 503, the user of the initiating device reviews the profile information (e.g., the images or pictures). At 504 <u>the initiating device transmits information, such as a message</u> or the initiating user's profile, <u>directly to the target device using the local wireless protocol</u>.”) • 16:16-19 (“[W]ireless device IDs 813 and 823 are <u>unique</u> identifications.”) |

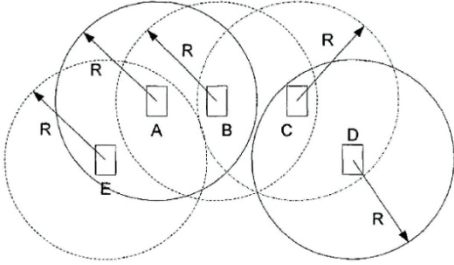
| Claim Element | <u>Mgrdechian</u> |
|--|--|
| | <ul style="list-style-type: none"> • 20:1-47 (“...[U]sing the positional database 1000, the remote computer can further determine that <u>device C is in range of device B</u>. If the system is programmed to <u>return all users active within one hop, the system may automatically use device C's ID and return information associated with device C's ID to device A.</u>”) • See also 5:31-35, 10:48-61, 12:48-50, 13:32-34, 19:54-57, 26:39-67, Figs. 3A, 6, 10. <p>Williams ¶¶98-102.</p> |
| <p>[1.b] a server data processor, for locating a disclosure policy associated with the second unique identifier or associated with the account associated with the second entity, and for comparing the disclosure policy to a first unique identifier associated with the first wireless device or other data associated with an account associated with the first entity associated with the first wireless device, wherein the disclosure policy specifies data</p> | <p>Mgrdechian discloses the at least one server comprising a server data processor (e.g., “processor” of “server”), for locating a disclosure policy associated with the second unique identifier or associated with the account associated with the second entity (e.g., “target user’s filter parameters,” “filter parameters associated with the device IDs [e.g., device C’s ID] are retrieved”), and for comparing the disclosure policy to a first unique identifier (e.g., “unique” “device ID[] of ... the initiating device[]”—device A) associated with the first wireless device or other data associated with an account associated with the first entity associated with the first wireless device (e.g., “the profile information of an initiating user may be compared to the target’s filter parameters”; “individual users...can set limitations such that users removed from direct contact beyond a certain number of hops (e.g. more than twice removed) are not included in any query”), wherein the disclosure policy specifies data representing one or more rules for privacy of information concerning the first wireless device or the entity associated with the first wireless device and the second wireless device or the entity associated with the second wireless device (e.g., “the initiating user [device A] may be denied access to the target's [device C’s] profile if the initiating user's profile</p> |

| Claim Element | <u>Mgrdechian</u> |
|---|---|
| representing one or more rules for privacy of information concerning the first wireless device or the entity associated with the first wireless device and the second wireless device or the entity associated with the second wireless device; and | <p>information does not satisfy the target user's filter parameters”).</p> <p><u>E.g., Mgrdechian:</u></p> <p><i>See [1.pre]-[1.a].</i></p> <p>In addition, Mgrdechian discloses that before the server “return[s]” “information associated with” “all users active within one hop,” including devices B and C, the server retrieves profile information for these devices. Mgrdechian, Fig. 7A, 13:50-14:8, 20:1-47. Each profile stored by the server contains a disclosure policy—“filter parameters” and information designated “non-public,” such that it “may not be disclosed.” <i>Id.</i>, 13:50-14:8, 16:60-17:10. Thus, if device A’s profile information (which is retrieved using device A’s unique ID) does not meet device B’s “filter parameters” (i.e., rules for privacy of information), then device A is denied access to device B’s profile as the target device. <i>Id.</i> Similarly, if device A’s profile information does not meet device C’s “filter parameters” then device A is denied access to device C’s profile and does not receive its information—and at minimum it would have been obvious to do so to protect device C’s information. <i>Id.</i>; Williams ¶106.</p> <p>Mgrdechian discloses that its server(s) performs these functions using a “processor,” and at minimum it would have been obvious to use one as discussed in §IX.A.1. Mgrdechian, cl. 27; Williams ¶¶89, 107.</p> <ul style="list-style-type: none"> • 13:50-14:8 (“FIGS. 7A-B illustrate <i>filtering based on profile information....</i> Some applications <i>may use the device IDs of both the target and the initiating devices to perform filtering.</i> For example,...a <i>query using the device IDs is generated,</i> and at 703 profile information and <i>filter parameters associated with the device IDs are retrieved.</i> At 704, the filter parameters are applied to the profile information.... Alternatively, <i>the</i> |

| Claim Element | <u>Mgrdechian</u> |
|---------------|--|
| | <p><i>profile information of an initiating user may be compared to the target's filter parameters, and the initiating user may be denied access to the target's profile if the initiating user's profile information does not satisfy the target user's filter parameters.”)</i></p> <ul style="list-style-type: none"> • 16:16-19 (“[W]ireless device IDs 813 and 823 are unique identifications.”) • 16:60-17:10 (“...<i>The profile information returned in reply 806 depends in part on how User B has configured his/her profile information. For example, User B may store some information that is designated non-public (i.e., information that may not be disclosed...).</i>...[N]on-public information may be filtered out when generating reply 806.”) • 20:1-47 (“If the system is programmed to <i>return all users active within one hop, the system may automatically use device C's ID and return information associated with device C's ID to device A...individual users or the system itself can set limitations such that users removed from direct contact beyond a certain number of hops (e.g. more than twice removed) are not included in any query.</i>”) • Claim 27 (“computer system-comprising... <i>processor</i>”) • Fig. 7A: |

| Claim Element | <u>Mgrdechian</u> |
|---|---|
| |  <pre> graph TD 701[Web Application receives wireless device IDs of a target user and an initiating user from initiating device] --> 702[Generate a query using wireless device IDs] 702 --> 703[Retrieve profile information and filter parameters] 703 --> 704[Apply filter parameters to profile information] 704 --> 705{pass} 705 -- N --> 706[Reject] 705 -- Y --> 707[Send Profile Information to initiating device] style 703 stroke:#f96,stroke-width:2px style 704 stroke:#f96,stroke-width:2px </pre> <p style="text-align: center;">Fig. 7A</p> <ul style="list-style-type: none"> • <i>See also</i> 5:51-65, 6:44-57, 10:48-56, 14:9-45, 26:39-67, Fig. 7B. <p>Williams ¶¶103-107.</p> |
| <p>[1.c] a network interface, for communicating first information to the first wireless device as permitted by the disclosure policy, wherein at least a portion of the first information</p> | <p>Mgrdechian discloses the at least one server comprising a network interface (e.g., server’s interface with the “Internet”), for communicating first information to the first wireless device as permitted by the disclosure policy, wherein at least a portion of the first information includes the second unique identifier (e.g., “return all users active within one hop, the system may automatically use device C’s ID and return information associated with device C’s ID to device A”).</p> <p><u>E.g., Mgrdechian:</u></p> <p><i>See</i> [1.pre]-[1.b].</p> |

| Claim Element | <u>Mgrdechian</u> |
|--|--|
| includes the second unique identifier; | <p>In addition, Mgrdechian discloses that the server is an “Internet server computer,” such that it has a network interface to the Internet and, at minimum, it would have been obvious to use such an interface in order to communicate with the Internet and the rest of the system as taught in Mgrdechian. Mgrdechian, 10:48-61; Williams ¶110. As discussed in [1.a]-[1.b], if permitted by device C’s filter parameters, the device C profile information, including its ID, is returned to device A. <i>Id.</i>, 13:50-14:8, 16:60-17:10, 20:1-47.</p> <ul style="list-style-type: none"> • 10:48-61 (“Computer system 360 may be an <u>Internet server computer and may include multiple computers coupled to the Internet...</u>”) • 12:18-26 (“<u>[C]omputer system 360 may send some or all of the profile information associated with each device ID back to the initiating wireless device (e.g., Device A),...</u>”) • 20:1-47 (“<u>...return all users active within one hop, the system may automatically use device C's ID and return information associated with device C's ID to device A.</u>”) |

| Claim Element | <u>Mgrdechian</u> | | | | | | | | | | | | |
|--|--|--------|------------------|---|------|---|------|---|------|---|---|---|---|
| | <ul style="list-style-type: none"> Fig. 10  <table border="1" data-bbox="867 764 1130 1003"> <thead> <tr> <th>Device</th> <th>Devices in Range</th> </tr> </thead> <tbody> <tr> <td>A</td> <td>B, E</td> </tr> <tr> <td>B</td> <td>A, C</td> </tr> <tr> <td>C</td> <td>B, D</td> </tr> <tr> <td>D</td> <td>C</td> </tr> <tr> <td>E</td> <td>A</td> </tr> </tbody> </table> <p style="text-align: right; margin-right: 50px;">~ 1000</p> <p style="text-align: center;">Fig. 10</p> <ul style="list-style-type: none"> <i>See also</i> 8:5-14, 13:39-49, 20:1-47, Fig. 6. <p>Williams ¶¶108-113.</p> | Device | Devices in Range | A | B, E | B | A, C | C | B, D | D | C | E | A |
| Device | Devices in Range | | | | | | | | | | | | |
| A | B, E | | | | | | | | | | | | |
| B | A, C | | | | | | | | | | | | |
| C | B, D | | | | | | | | | | | | |
| D | C | | | | | | | | | | | | |
| E | A | | | | | | | | | | | | |
| <p>[1.d] a mobile device for operating as the first wireless device and for receiving information related to the second wireless device or the entity associated with the second wireless device further comprising:</p> | <p>Mgrdechian discloses the system comprising a mobile device (e.g., “mobile wireless device”) for operating as the first wireless device (e.g., “device A”) and for receiving information related to the second wireless device or the entity associated with the second wireless device (e.g., “return all users active within one hop, the system may automatically use device C’s ID and return information associated with device C’s ID to device A”).</p> <p><u>E.g., Mgrdechian:</u></p> <p>See [1.pre], [1.b]-[1.c].</p> <p>In addition, Mgrdechian discloses that a wireless device (e.g., device A) is a “mobile wireless device” that receives “information associated” with other wireless devices</p> | | | | | | | | | | | | |

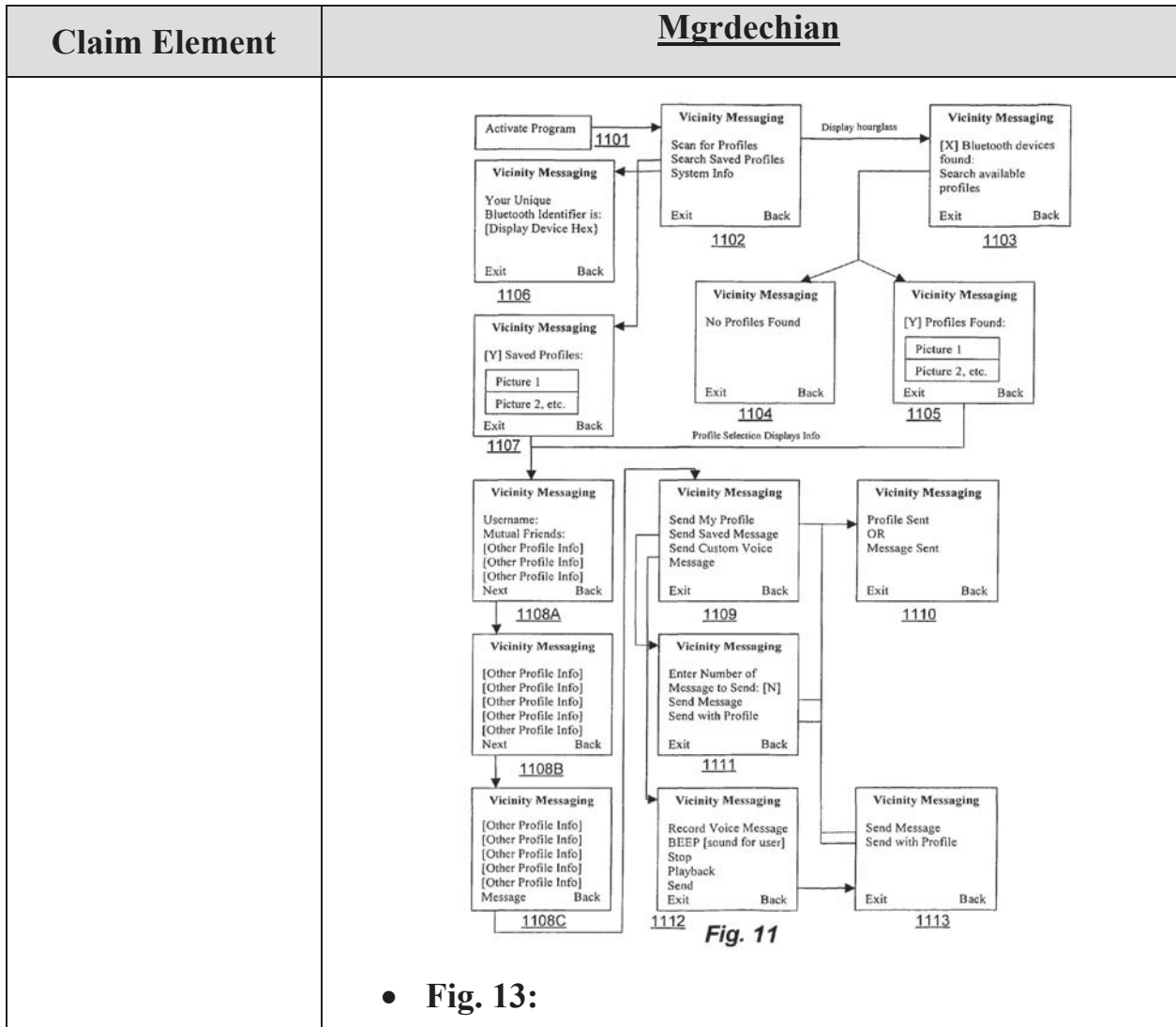
| Claim Element | <u>Mgrdechian</u> |
|--|---|
| | <p>within a certain number of communication hops, including device C’s profile information. Mgrdechian, 20:1-47, 22:26-35.</p> <ul style="list-style-type: none"> • 22:26-35 (“<i>Embodiments of wireless devices 1300 may include ...mobile wireless device.</i>”) • <i>See also</i> 8:1-4, 16:6-10, 20:1-47, Fig. 8. <p>Williams ¶¶114-116.</p> |
| <p>[1.e] a first radio for communicating with the server and receiving the first information including the second unique identifier;</p> | <p>Mgrdechian discloses the mobile device comprising a first radio (e.g., “circuits for implementing multiple wireless technologies such as...a wireless phone technology”) for communicating with the server and receiving the first information including the second unique identifier (e.g., see [1.c]-[1.d]).</p> <p><u>E.g., Mgrdechian:</u></p> <p>See [1.c]-[1.d].</p> <p>In addition, Mgrdechian discloses that the server is an “Internet server” that communicates with the wireless device “over a cellular network” using a “circuit[.]” Mgrdechian, 10:48-56, 16:34-42, 21:65-22:12. As discussed in §IX.A.1, a POSITA would have understood, or at minimum found it an obvious implementation choice, that device A uses a radio to receive the first information as discussed in [1.c]-[1.d] from the server. Williams ¶¶90, 119.</p> <ul style="list-style-type: none"> • 10:48-56 (“Computer system 360 may be an <i>Internet server computer and may include multiple computers coupled to the Internet ...</i>”) • 16:34-42 (“Device A sends a request 803 to web application 861 on server 860...<i>over a cellular network.</i> ... Device A may...contact web application 861...<i>over the Internet.</i>”) • 21:65-22:12 (“<i>Wireless device 1300 includes...an antenna...coupled to RF circuitry 1302. RF</i>”) |

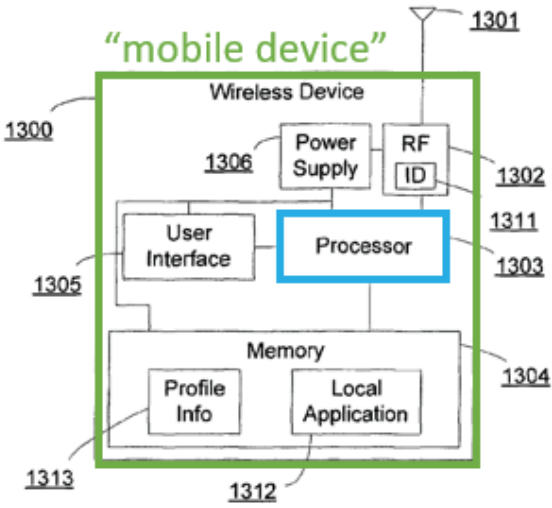
| Claim Element | <u>Mgrdechian</u> |
|---|---|
| | <p><i>circuitry 1302 receives...the RF signals...RF circuitry 1302 may include analog and digital circuits for implementing multiple wireless technologies such as...a wireless phone technology (e.g., an analog or digital cellular technology...).</i>”</p> <ul style="list-style-type: none"> • <i>See also</i> Fig. 13. <p>Williams ¶¶117-119.</p> |
| <p>[1.f] a second radio for receiving proximity beacon transmissions utilizing a local or personal area wireless protocol, and for providing received proximity beacon information derived from the proximity beacon transmissions; and</p> | <p>Mgrdechian discloses the mobile device comprising a second radio (e.g., “circuits for implementing multiple wireless technologies such as a local wireless protocol,” “Bluetooth” radio) for receiving proximity beacon transmissions utilizing a local or personal area wireless protocol, and for providing received proximity beacon information derived from the proximity beacon transmissions (e.g., “each target wireless device transmits the device ID to the initiating device using the local wireless protocol...the initiating device receives the wireless device IDs from the other wireless devices”).</p> <p><u>E.g., Mgrdechian:</u></p> <p>See [1.pre], [1.d].</p> <p>In addition, Mgrdechian discloses that the mobile device acting as device A receives “Bluetooth” transmissions from the other devices that are within the “effective range of the local wireless protocol.” Mgrdechian, 15:44-16:2, 16:6-15, 19:34-39. Each of the wireless devices “continuously or intermittently broadcast[s] its ID,” thus acting as beacon transmitters and allowing device A to detect other devices that are “within range.” <i>Id.</i>, 6:59-61, 9:56-10:8. A POSITA would have understood that a separate “Bluetooth” radio is used to receive the Bluetooth transmissions, or at minimum it would have been an obvious implementation choice to do so as discussed in §IX.A.1. Williams ¶¶90, 124. Device A’s Bluetooth radio then provides the received beacon proximity information, including the IDs of the other devices, to device A’s</p> |

| Claim Element | <u>Mgrdechian</u> |
|---------------|--|
| | <p>processor for processing. <i>Id.</i>, 13:3-18, 21:65-22:12, Fig. 13.</p> <ul style="list-style-type: none"> • 6:59-61 (“[A] <u>device may continuously or intermittently broadcast its ID and/or other information without having received an inquiry.</u>”) • 9:56-10:8 (“[F]irst wireless device 310 may <u>wirelessly communicate with wireless devices 390A-N that are within range of device 310....</u>”) • 13:3-18 (“<u>each target wireless device transmits the device ID to the initiating device using the local wireless protocol. At 406, the initiating device receives the wireless device IDs from the other wireless devices and transmits the device IDs to a remote computer over a wireless network.</u>”) • 15:44-16:2 (“[I]n addition to providing their device IDs, the queried devices may also provide various forms of initial profile information,...”) • 16:6-15 (“[W]ireless devices such as PDA 880A and wireless ID tag 880N all capable of <u>communicating using a Bluetooth Protocol 830...a request (i.e., a query) 801 and reply 802 are made using Bluetooth.</u>”) • 19:34-39 (“Each circle represents <u>the effective range of the local wireless protocol....</u>”) • 21:65-22:12 (“<u>Wireless device 1300 includes...an antenna...coupled to RF circuitry 1302. RF circuitry 1302 receives...the RF signals...RF circuitry 1302 may include analog and digital circuits for implementing multiple wireless technologies such as a local wireless protocol (e.g., Bluetooth, 802.11 or Zigbee)...</u>”) • See also 20:1-47, 22:54-55, Figs. 11, 13. <p>Williams ¶¶120-125.</p> |

| Claim Element | <u>Mgrdechian</u> |
|---|---|
| <p>[1.g] a mobile device data processor for receiving the proximity beacon information from the second radio and performing an action function to detect the proximity of a device associated with the second unique identifier, wherein the action function compares the proximity beacon information with the second unique identifier to determine if the proximity beacon information corresponds to the second unique identifier to determine said proximity of the device associated with the second unique identifier.</p> | <p>Mgrdechian discloses the mobile device comprising a mobile device data processor (<i>e.g.</i>, “processor” of the “mobile wireless device”) for receiving the proximity beacon information from the second radio (<i>e.g.</i>, see [1.f]) and performing an action function to detect the proximity of a device associated with the second unique identifier, wherein the action function compares the proximity beacon information with the second unique identifier to determine if the proximity beacon information corresponds to the second unique identifier to determine said proximity of the device associated with the second unique identifier (<i>e.g.</i>, “a user may scan for profiles in the vicinity..., search for saved profiles” such that when device A receives device C’s ID, the device C ID is compared against the “saved profile[]” information for device C).</p> <p><u>E.g., Mgrdechian:</u></p> <p>See [1.pre]-[1.a], [1.d], [1.f].</p> <p>In addition, Mgrdechian discloses that wireless devices include a “processor” for “processing” and “controlling” information. Mgrdechian, 21:65-22:26, FIG. 13. When device C later comes within range of device A, the processor receives device C’s ID from device A’s radio, and compares device’s C ID to the “saved profiles” to determine whether device A already has device C’s profile. <i>Id.</i>, 12:18-26, 20:56-21:6, Fig. 11. As discussed in §IX.A.1, at minimum it would have been obvious for device A’s processor to do this to advantageously reduce the amount of information requested by device A from the server (consistent with Mgrdechian’s goal to do so). <i>Id.</i>, 15:44-16:2; Williams ¶¶87, 130.</p> <ul style="list-style-type: none"> • 12:18-26 (“<u>Profile information for one or more targets may be stored internally on a wireless device....</u> Some or all of the profile information may |

| Claim Element | <u>Mgrdechian</u> |
|---------------|--|
| | <p>be saved (e.g., as a complete profile or as a summary profile).”)</p> <ul style="list-style-type: none"> • 15:44-16:2 (“[I]n addition to providing their device IDs, the <i>queried devices may also provide various forms of initial profile information</i>, such as a picture of User B or text, <i>so that User A can select other users to communication [sic] with from the available users on the local network</i>... Thus, rather than automatically retrieving profile information for all device IDs within range, <i>computing resources may be saved by narrowing the list to profiles of interest to be retrieved from the remote computer system</i>.”) • 20:56-21:6 (“At 1102, <i>a user may scan for profiles in the vicinity (e.g., by transmitting a identification request), search for saved profiles</i> or obtain system information....”) • 21:65-22:26 (“FIG. 13 is an example of a wireless device... <i>Information is processed and controlled by processor 1303... Processor 1303 may execute instructions for controlling the flow and processing of information between RF circuitry 1302, memory 1304 and user interface 1305... Processor 1303 may access and execute local application 1312 during ‘run-time’</i> to execute the wireless device portions of the methods and processes described herein.”) • Fig. 11: |



| Claim Element | <u>Mgrdechian</u> |
|---|--|
| |  <p style="text-align: center;">Fig. 13</p> <p>Williams ¶¶126-130.</p> |
| <p>[2] The system of claim 1, wherein said proximity beacon transmissions are transmitted utilizing a local or personal area wireless protocol by the second wireless device and include information corresponding to the second unique identifier.</p> | <p><i>See</i> [1].</p> <p>Mgrdechian discloses that said proximity beacon transmissions are transmitted utilizing a local or personal area wireless protocol (e.g., “Bluetooth”) by the second wireless device and include information corresponding to the second unique identifier (e.g., device C’s unique ID, “each target wireless device transmits the device ID to the initiating device using the local wireless protocol...,” “may also provide various forms of initial profile information”).</p> <p><u>E.g., Mgrdechian:</u></p> <p><i>See</i> [1.pre], [1.d], [1.f].</p> <p>In addition, Mgrdechian discloses that each wireless device (including device C) “continuously or intermittently broadcast its ID and/or other information” using a “local wireless protocol” such as “Bluetooth” protocol for detection by other proximate wireless devices. Mgrdechian, 6:59-61, 10:10-15, 15:44-60.</p> |

| Claim Element | <u>Mgrdechian</u> |
|---------------|-------------------|
|---------------|-------------------|

- **6:59-61** (“[A] *device may continuously or intermittently broadcast its ID and/or other information without having received an inquiry.*”)
- **10:10-15** (“[W]ireless technologies that may be used as a *local wireless protocol include Bluetooth, an 802.11 protocol, Zig bee or equivalent wireless technology* for establishing a peer-to-peer or ad hoc network or *detecting the presence of other wireless devices and exchanging device IDs.*”)
- **15:44-60** (“[W]ireless devices 310 and 320 may include *initial profile information 312 and 322 stored locally* on the wireless devices ... *in addition to providing their device IDs, the queried devices may also provide various forms of initial profile information, such as a picture of User B or text*”)

• **Fig. 3A:**

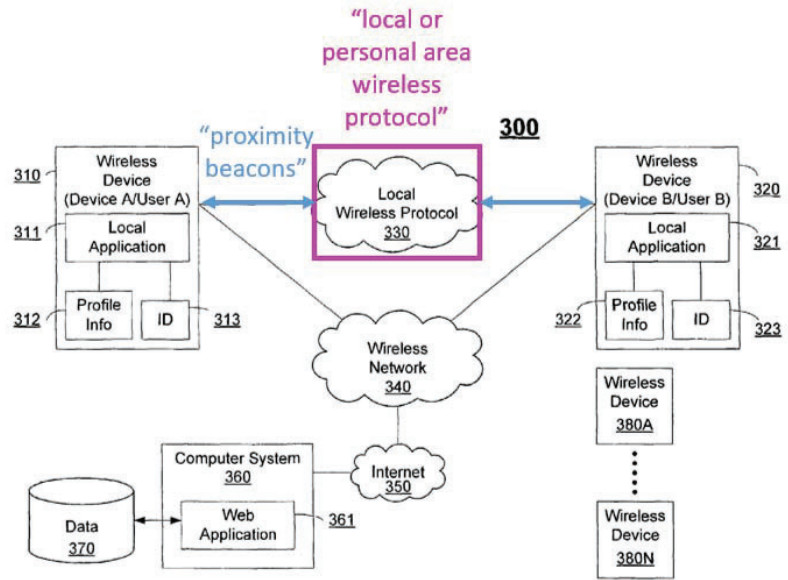


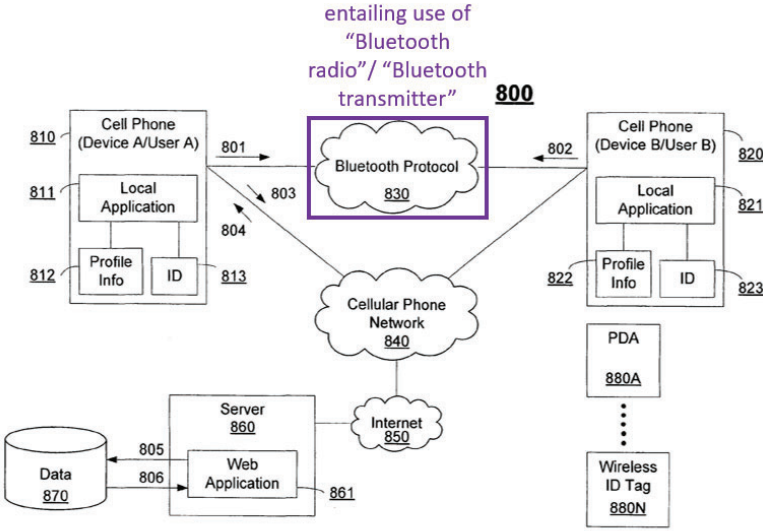
Fig. 3A

See also 13:38-42

| Claim Element | <u>Mgrdechian</u> |
|--|---|
| | Williams ¶¶131-133. |
| <p>[3] The system of claim 1, wherein the disclosure policy associated with the second unique identifier or associated with the account associated with the second entity allows for secure and fraud resistant application of policies for the disclosure of information and content.</p> | <p>See [1].</p> <p>Mgrdechian discloses that the disclosure policy associated with the second unique identifier or associated with the account associated with the second entity allows for secure and fraud resistant application of policies for the disclosure of information and content (e.g., “profile information returned in reply 806 depends in part on how User [C] has configured his/her profile information...non-public information may be filtered out”; “the ID’s are...dynamic or pseudo-random”).</p> <p><u>E.g., Mgrdechian:</u></p> <p>See [1.b]-[1.c].</p> <p>To the extent the “wherein” clause merely recites an intended result and is not limiting, Mgrdechian anticipates and renders obvious [3] for the reasons discussed in [1]. <i>See</i> MPEP §2111.04.I; <i>Minton v. Nat’l Ass’n of Securities Dealers, Inc.</i>, 336 F.3d 1373, 1381 (Fed. Cir. 2003).</p> <p>To the extent the “wherein” clause is limiting, as discussed in [1.b], “filter parameters” associated with User C’s account limit access to User C’s profile information. Mgrdechian 13:50-14:8. User C’s “filter parameters” are applied to User A’s profile information. If User A’s profile information does not satisfy User C’s “filter parameters,” User A does not receive User C’s profile. Mgrdechian, 13:50-14:8, 16:60-17:10. Because “filtering” is performed at the server using users’ filter parameters and profile information, the filtering allows for secure and fraud resistant application of policies for the disclosure of information and content. <i>Id.</i>, 5:1-3, 16:60-17:10,. Similarly, the use of “dynamic or pseudo-random” IDs to retrieve the profile provides these same benefits. <i>Id.</i> For example, a POSITA would have understood or, at minimum it would have been obvious, that when a</p> |

| Claim Element | <u>Mgrdechian</u> |
|--|---|
| | <p>dynamic identifier or pseudo-random identifier is used to determine whether a server is permitted to disclose target user’s information (including its identity), a malicious device cannot gain access to this information by reusing a superseded ID. <i>Id.</i>; Williams ¶136.</p> <ul style="list-style-type: none"> • 13:50-14:8 (“FIGS. 7A-B illustrate <u>filtering based on profile information...</u>. Some applications <u>may use the device IDs of both the target and the initiating devices to perform filtering.</u> For example,...a <u>query using the device IDs is generated,</u> and at 703 profile information and <u>filter parameters associated with the device IDs are retrieved.</u> At 704, the filter parameters are applied to the profile information.... Alternatively, <u>the profile information of an initiating user may be compared to the target's filter parameters, and the initiating user may be denied access to the target's profile if the initiating user's profile information does not satisfy the target user's filter parameters.</u>”) • 5:1-3 (“[D]evices can include cases where the <i>ID's</i> are static, <u>dynamic or pseudo-random.</u>”) • 16:60-17:10 (“The <u>profile information returned in reply 806 depends in part on how User B has configured his/her profile information...</u> Database 870 may differentiate public information from non-public information. Thus, <u>non-public information may be filtered out...</u>”) • <i>See also</i> Mgrdechian, 17:19-27, 19:13-25. <p>Williams ¶¶134-136.</p> |
| <p>[4] The system of claim 1, wherein the system or a component of the system causes the</p> | <p><i>See</i> [1].</p> <p>Mgrdechian discloses that the system or a component of the system causes the change of at least one unique identifier from time to time such that disclosure of the at least one unique identifier by one device to another</p> |

| Claim Element | <u>Mgrdechian</u> |
|---|--|
| <p>change of at least one unique identifier from time to time such that disclosure of the at least one unique identifier by one device to another does not compromise the identity of that device once the unique identifier has changed.</p> | <p>does not compromise the identity of that device once the unique identifier has changed (<i>e.g.</i>, “the [unique] ID's are...dynamic”).</p> <p><u>E.g., Mgrdechian:</u></p> <p>Mgrdechian discloses that the system updates the “unique” device IDs “dynamic[ally].” Mgrdechian, 5:1-3, 3:34-35. To the extent the “such that” clause merely recites an intended result and is not limiting, no further disclosure is required. MPEP §2111.04.I; <i>Minton</i>, 336 F.3d at 1381. To the extent the “such that” clause is limiting, a POSITA would have understood, or at minimum found it obvious, that, because the unique IDs are changed dynamically, disclosure of a device’s ID to another device does not compromise the identity of that device once the unique identifier has changed. Williams ¶138.</p> <ul style="list-style-type: none"> • 3:34-35 (“<i>wireless device identifications are unique identifications</i>”) • 5:1-3 (“[D]evices can include cases where the <i>ID's are static, dynamic or pseudo-random.</i>”) <p>Williams ¶¶137-138.</p> |
| <p>[5] The system of claim 1 wherein said the second radio is a Bluetooth radio and said second wireless device utilizes a Bluetooth transmitter to provide the proximity beacon transmissions.</p> | <p>See [1].</p> <p>Mgrdechian discloses that the second radio is a Bluetooth radio (<i>e.g.</i>, see [1.f]) and said second wireless device utilizes a Bluetooth transmitter (<i>e.g.</i>, “Bluetooth” transmitter) to provide the proximity beacon transmissions (<i>e.g.</i>, see [1.f]).</p> <p><u>E.g., Mgrdechian:</u></p> <p>See [1.f].</p> <p>In addition, a POSITA would have understood, or at minimum found obvious, that device A’s radio (see [1.f]) is a Bluetooth radio and that each device’s Bluetooth radio (including device C’s) includes a transmitter to</p> |

| Claim Element | <u>Mgrdechian</u> |
|-----------------------------------|---|
| | <p>“transmit[]” “Bluetooth” signals to the other devices. Mgrdechian, 16:6-15, 21:65-22:12, Figs. 8, 13; Williams ¶¶90, 141.</p> <ul style="list-style-type: none"> • 16:6-15 (“System 800 includes cellular phones 810 and 820 and other wireless devices...all capable of communicating using a <i>Bluetooth Protocol 830</i>...a <i>request (i.e., a query) 801</i> and <i>reply 802</i> are made using <i>Bluetooth</i>.”) • 21:65-22:12 (“<i>Wireless device 1300</i> includes...an antenna...coupled to RF circuitry 1302. <i>RF circuitry 1302</i> receives, transmits and processes the <i>RF signals</i> <i>RF circuitry 1302</i> may include analog and digital <i>circuits for implementing multiple wireless technologies such as...Bluetooth...</i>”) • Fig. 8:  <p style="text-align: center;"><i>Fig. 8</i></p> <ul style="list-style-type: none"> • <i>See also</i> Mgrdechian, 10:8-15, Fig. 13. Williams ¶¶139-142. |
| [6] The system of claim 1 wherein | <i>See [1].</i> |

| Claim Element | <u>Mgrdechian</u> |
|---|--|
| <p>upon the detection of the proximity of the second wireless device, the mobile device data processor utilizes the first radio to communicate with a second server to receive further information based upon the second unique identifier, 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.</p> | <p>Mgrdechian discloses that upon the detection of the proximity of the second wireless device, the mobile device data processor (e.g., see [1.g]) utilizes the first radio (e.g., see [1.e]) to communicate with a second server (e.g., a second server of the “one or more central servers”) to receive further information based upon the second unique identifier (e.g., “display a list of previously saved profiles at 1107, from which a user may select the complete profile and obtain profiles 1108A-C” where the “saved profile[]” is “summary profile”; “complete profiles retrieved from a backend system such as an Internet server”), 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 (e.g., “Profile information may include... a list of friends,” see [7]).</p> <p><u>E.g., Mgrdechian:</u></p> <p>See [1.c], [1.e], [1.g], [7].</p> <p>In addition, as previously discussed in [1.c], [1.e], and [1.g], Mgrdechian also discloses device A saving only “[s]ome” of profile information for device C as a “summary profile.” Mgrdechian, 12:18-26. The user selects the device C “summary profile” to retrieve the “complete profile” from “backend system such as an Internet server.” <i>Id.</i>, 20:56-21:6. The “complete profile[]” includes “a list of friends” (a stored state) that is based on previous interactions with other users (e.g., between users associated with Devices A and C—<i>i.e.</i>, whether the two are friends). <i>Id.</i>, 11:25-34. Consistent with Mgrdechian’s disclosures that the system includes “one or more central servers,” the request for device C’s “complete profile[]” is received by and responded to by a different server than the server sending the “summary profile” ([1.c]), or at minimum it would have been an obvious implementation choice to do so in light of Mgrdechian’s disclosures as</p> |

| Claim Element | <u>Mgrdechian</u> |
|--|--|
| | <p>discussed in §IX.A.1. <i>Id.</i>, 7:23-32, 10:48-61; Williams ¶148.</p> <ul style="list-style-type: none"> • 7:23-32 (“[W]hen the identity of the users of these devices may or may not be known to each other and communication of any form between devices is initiated by the <u>wireless exchange of one or more IDs that are uploaded to one or more central servers which then enable, authorize or facilitate information to be conveyed between the devices either directly or through one or more central servers.</u>”) • 11:25-34 (“<u>Profile information may include...a list of friends.</u>”) • 12:18-26 (“Profile information for one or more targets may be stored internally on a wireless device.... <u>Some or all of the profile information may be saved (e.g., as a complete profile or as a summary profile).</u>”) • 20:56-21:6 (“A <u>user may search available profiles,</u> which may be pictures, initial profiles (i.e., summary or “portable profiles”) or <u>complete profiles retrieved from a backend system such as an Internet server...</u>If a user is interested in a listed profile, the user may select the profile to view the complete profile...The system may <u>display a list of previously saved profiles at 1107, from which a user may select the complete profile and obtain profiles 1108A-C.</u>”) • See also 15:48-51, 16:10-14 <p>Williams ¶¶143-148.</p> |
| [7] The system of claim 6 wherein said further information | <p>See [6].</p> <p>Mgrdechian discloses that said further information (e.g., see [6]) additionally comprises content relating to...social network content (e.g., “social networking</p> |

| Claim Element | <u>Mgrdechian</u> |
|---|--|
| <p>additionally comprises content relating to one or more of the following:</p> <p>...</p> <p>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</p> | <p>application where the information is profile information”) 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 [6], device C’s “Profile information may include...a list of friends”), 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., “...construct lists of...mutual friends...by accessing and comparing profiles of two users. The list of mutual acquaintances may then be sent to the initiating wireless device,” “Profile information may include...a list of friends,” “profile information returned in reply 806 depends in part on how User B has configured his/her profile information...non-public information may be filtered out”).</p> <p><u>E.g., Mgrdechian:</u></p> <p>See [1.b], [6].</p> <p>In addition, Mgrdechian discloses sharing “profile information,” including “a list of friends” (stored state – see [6]) of a “target user[]” (device C) with an “initiating user” of device A for a “social networking application.” Mgrdechian, 11:23-34, 13:50-14:8. In addition, Mgrdechian discloses that a list of mutual friends is constructed by comparing the profiles of device A’s and C’s users. <i>Id.</i>, 11:25-48. Thus, where a friends list is not otherwise public, Mgrdechian discloses sharing whether device C’s user considers device A’s user a friend only if device A and device C each include one another as a friend on their respective “lists of friends.” <i>Id.</i>; Williams ¶152. Additionally, as discussed in [1.b], only the profile information of device C that is permitted by device C’s</p> |

| Claim Element | <u>Mgrdechian</u> |
|----------------------------------|--|
| with the second wireless device. | <p>filter parameters is returned to device A. Accordingly, if device C’s “filter parameters” designate its “list of friends” as “non-public” information for users not on its “list of friends,” then that information would be shared with device A only if device A’s user is included in device C’s “list of friends.” <i>Id.</i>, 11:23-34, 16:60-17:10. As discussed in §IX.A.1, at minimum it would have been obvious to filter on the basis of a list of friends to advantageously block “unwanted, repetitive, overwhelming or otherwise undesirable messages” (consistent with Mgrdechian’s goal to do so). <i>Id.</i>, 17:62-18:5; Williams ¶153.</p> <ul style="list-style-type: none"> • 11:23-48 (“[P]resent invention are particularly advantageous in an <i>on-line dating or social networking application</i>...Profile information may include a...list of friends. In one embodiment, users may specify a list of friends. The web application on the remote computer may then construct lists of mutual acquaintances (e.g., mutual friends or other people that are known by both users) of a given pair of users (e.g., an initiator and target) by accessing and comparing profiles of two users. The list of mutual acquaintances may then be sent to the initiating wireless device....”) • 13:50-14:8 (“[T]he profile information of an <i>initiating user may be compared to the target's filter parameters, and the initiating user may be denied access to the target's profile if the initiating user's profile information does not satisfy the target user's filter parameters.</i>”) • 16:60-17:10 (“The <i>profile information returned in reply 806 depends in part on how User B has configured his/her profile information.</i> For example, <i>User B may store some information that is designated non-public</i> (i.e., information that may not be disclosed in response to a request 805), and |

| Claim Element | <u>Mgrdechian</u> |
|---|---|
| | <p>may store other information that may be designated public (i.e., information may be disclosed in response to a request 805)...<u>non-public information may be filtered out</u> when generating reply 806.”)</p> <ul style="list-style-type: none"> • 17:62-18:5 (“Additionally, users may configure the system...for <u>filtering out unwanted, repetitive, overwhelming or otherwise undesirable messages (e.g., spam).</u>”) <p>Williams ¶¶149-153.</p> |
| <p>[8] The system of claim 2 where the proximity beacons transmitted by the second wireless device comprise a MAC address and the second unique identifier.</p> | <p>See [2].</p> <p>Mgrdechian renders obvious that the proximity beacons transmitted by the second wireless device (e.g., see [1.pre]) comprise a MAC address (e.g., “in addition to providing their device IDs, the queried devices may also provide various forms of initial profile information”; “each communication device is provided with a unique ID in the manufacturing process”) and the second unique identifier (e.g., “device ID[],” “Bluetooth ID[]” of device C).</p> <p><u>E.g., Mgrdechian:</u></p> <p>See [1.pre], [2].</p> <p>In addition, Mgrdechian discloses device C transmitting “its ID and/or other” “initial profile information” in the same message. Mgrdechian, 6:59-61, 15:55-62.</p> <p>Mgrdechian discloses that the device may also have a “unique ID [assigned] in the manufacturing process,” which includes the known concept of a MAC address. <i>Id.</i>, 15:55-62, 16:16-33; Williams ¶¶82, 157. As discussed in §IX.A.1, at minimum it would have been obvious to a POSITA to send a MAC address as part of the initial profile information as an additional form of identification to the Bluetooth ID. Williams ¶¶83, 158.</p> |

| Claim Element | <u>Mgrdechian</u> |
|---------------|--|
| | <ul style="list-style-type: none"> • 6:59-61 (“<u>[A] device may continuously or intermittently broadcast its ID and/or other information....</u>”) • 15:55-62 (“<u>[In addition to providing their device IDs, the queried devices may also provide various forms of initial profile information, ...initial profile information...is received with the device IDs directly from the other wireless devices.]</u>”) • 16:16-33 (“<u>[W]ireless device IDs 813 and 823 are unique identifications...wherein the unique identifications are Bluetooth IDs...an RFID or another equivalent identification for uniquely identifying the wireless device...A device manufacturer, in coordination with the other device manufacturers, may have policies for assigning such unique IDs such that each communication device is provided with a unique ID in the manufacturing process.]</u>”) <p>Williams ¶¶154-158.</p> |

B. Ground 3: Claims 1-8 Are Rendered Obvious By Mgrdechian In View Of Kaplan

To the extent further disclosure is required beyond Mgrdechian for [1.e]-[1.f]’s requirement of two separate Bluetooth and cellular radios and [1.g]’s requirement of comparing information received via local wireless protocol with information received from a server (*see* §§IX.A.2.[1.e]-[1.g]), **Kaplan** provides these teachings and the Challenged Claims are obvious in further view of **Kaplan**. *See* §§IX.A.2, IV.B.2 (listing grounds).

Kaplan describes “a communication system...that enables automated retrieval of caller ID picture information and associat[ed]...contact information, while still allowing security control over information or images that are sent to the requesting device.” Kaplan, Abstract, 2:16-20. **Kaplan’s** communication system comprises wireless devices and a server as illustrated in Fig. 1. Kaplan, 3:47-53, Fig. 1. A typical wireless device includes a “[c]ommunication subsystem 31” comprising components sufficient for device-to-device and device-to-network communication including, but not limited to, “call sending and receiving, MMS and SMS message sending and receiving, and World Wide Web access.” Kaplan, 6:3-11. Communication with the network “is established wirelessly through radio frequency or radio channel between communication subsystem 31, antenna 14 and the subscriber’s network,” which is “operating through mobile or cellular networks.” Kaplan, 6:37-58. The wireless device further includes “[d]evice to device connection subsystem 33 compris[ing] those components necessary to establish non-network based direct connection between the wireless telecommunications device and any other device...made using short-range radio frequency (RF) transmission...includ[ing]...Bluetooth.” Kaplan, 6:12-28. A POSITA would have understood that the “components necessary to establish...Bluetooth” include wireless radio transceivers that are designed to operate at the frequency band used by the particular technology. Williams ¶¶159-163.

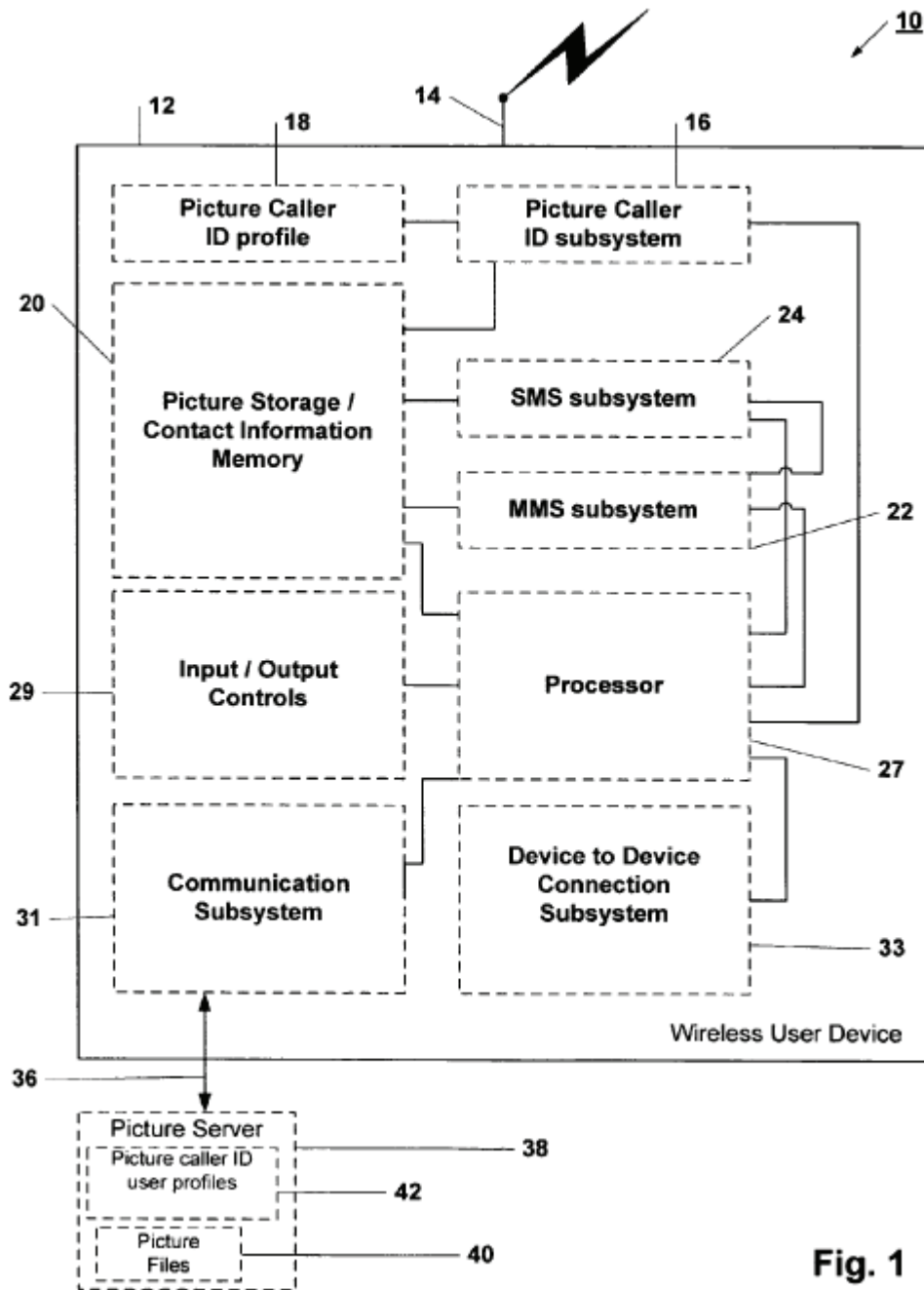


Fig. 1

Kaplan teaches the device-to-device communication includes receipt of contact information directly from another telecommunication device. Kaplan, 6:17-21. When a wireless device receives contact information, “processor 27” of the

wireless device first checks whether “the caller ID contact information” exists in “locally stored contact information” (previously received from the server) and whether “there is a locally stored picture associated with the locally stored contact information.” Kaplan, 3:58-4:8, 11:40-12:12, Fig. 4. If there is an associated locally stored picture, “then wireless device displays both the caller ID contact information and [the associated] picture on wireless device display....However, if the wireless device finds no locally stored contact information...or...no locally stored image associated with locally stored contact[, the] wireless device requests download of remotely stored caller ID contact image data and picture” from “picture server 38.” Kaplan, 3:53-55, 3:58-4:8, 11:40-12:12, Figs. 1, 4. “Upon receiving...the requested caller ID data or image files [from picture server 38], the wireless device updates the locally stored contacts...and the newly received information is ready for display either during the current call, or the next time a call carrying the same caller ID message is received....” *Id.*; Williams ¶¶164-166.

A POSITA would have found it advantageous to apply **Kaplans’s** teachings in implementing **Mgrdechian’s** system of facilitating communication between two devices via remote server. Williams ¶167. Like Mgrdechian, **Kaplan** is in the same field and is analogous art to the ’164, namely wireless communication systems. *E.g.*, Kaplan, Abstract, 2:16-31; Williams ¶167. Kaplan is also pertinent to the alleged problem(s) identified in the ’164 of a “lack of an independent third party to facilitate

the services required for a secure proximity based mobile electronic transaction.” *E.g.*, ’164, 2:52-56; Kaplan, 4:9-37, 7:7-15, 12:26-48, cl. 1; Williams ¶168. For example, Kaplan discloses that “a user may set security and distribution rules on his or her own picture and contact information,” “applied [by] picture server...to engage security measures to prevent unauthorized downloading.” Kaplan, 4:9-37, 12:26-48.

While a POSITA would have understood that **Mgrdechian** discloses that each wireless device has separate cellular and Bluetooth radios to communicate with the server and each other, respectively (see §IX.A.[1.e]-[1.f]), **Kaplan** discloses the well-known implementation choice of including separate radios to communicate over the “cellular network” and “Bluetooth” protocols. Kaplan, 6:37-58, 6:12-28; Williams ¶169. A POSITA would have been motivated to apply Kaplan’s teachings of two radios in implementing **Mgrdechian**’s wireless devices as an obvious design choice that would predictably yield a standard cell phone capable of communicating via cellular and Bluetooth protocols. Williams ¶170. Thus, with respect to [1.e]-[1.f], a POSITA would have been motivated to apply **Kaplan’s teachings of the mobile device comprising a first radio** (*e.g.*, “radio...operating through mobile or cellular networks”) **and a second radio** (*e.g.*, “components necessary to establish...short range RF...transmission ...include[ing]...Bluetooth”). *E.g.*, Kaplan 6:37-58, 6:12-28, Fig. 1. In applying these teachings, **Mgrdechian**’s wireless device (*e.g.*, device A) includes a first radio for communicating with the server via cellular phone

network and a separate “Bluetooth” radio to receive Bluetooth transmissions from other wireless devices (*e.g.*, device B and C), which includes a Bluetooth transmitter for “broadcast[ing] its ID and/or other information.” *See* Mgrdechian, 6:59-61; §IX.A.2.[1.e]-[1.f], [5]; Williams ¶¶170, 173-178.

While a POSITA would have understood that **Mgrdechian** discloses a first wireless device comparing a received identifier from another device via Bluetooth with saved profiles on the first wireless device to avoid requesting the profile information from the server to save computing resources (see §IX.A.[1.g]), **Kaplan** expressly discloses a device processor comparing received identifier information from another device to “locally stored” information in the device (previously received from the server) to determine whether there is a need to request information from the server. Kaplan, 3:53-55, 3:58-4:8, 11:61-12:12, Figs. 1, 4. A POSITA would have been motivated to apply **Kaplan’s** teaching of searching for a new ID in locally stored information before requesting the information from a server in implementing Mgrdechian’s wireless device to advantageously achieve a goal described in Mgrdechian: saving computing resources by requesting only profiles not already saved to the device. Mgrdechian, 12:18-26, 20:56-21:6, Fig. 11; *see* §IX.A.2.[1.g]; Williams ¶¶171-172.

With respect to [1.g], a POSITA would have been motivated to apply **Kaplan’s teachings of a mobile device data processor comparing proximity**

beacon information with a second unique identifier to determine if the proximity beacon information corresponds to a second unique identifier to determine said proximity of the device associated with the second unique identifier (e.g., “processor 27” of the “wireless device” checking whether the “[received] caller ID contact information” exists in “locally stored contact information,” which is updated based on “caller ID data” received from “picture server 38”). *E.g.*, Kaplan, 3:53-55, 3:58-4:8, 11:61-12:12, Figs. 1, 4; *see also id.*, 5:36-63, 7:16-8:30, 9:1-8. **Kaplan** teaches the basic concept of checking a local cache for information associated with a received ID before requesting the information from a server to save network and computing resources. *Id.* In applying these teachings, **Mgrdechian’s** device A’s processor compares device C’s ID to the “saved profiles” to determine whether device A already has device C’s profile, and therefore need not request it from the server. *See* Mgrdechian, 20:56-21:6; §IX.A.2.[1.g]; Williams ¶¶179-183.

In light of the above, a POSITA would have found it routine, straightforward and advantageous to apply **Kaplan’s** known teachings of checking a local cache for information associated with a received device identifier before querying a server in implementing **Mgrdechian’s** teachings of receiving device identifiers and storing “saved profiles,” and would have known that such a combination (yielding the

claimed limitations) would predictably work and provide the expected functionality.

Williams ¶184.

C. Grounds 4 And 5: Claims 3 And 4 Are Rendered Obvious By Mgrdechian In View Of Kulakowski (Ground 4), And In Further View Of Kaplan (Ground 5)

To the extent it is argued that further disclosure beyond Mgrdechian’s teaching of dynamic and pseudo-random identifiers is required for claims 3 and 4 (*see* §§IX.A.2.[3]-[4]), claims 3 and 4 are rendered obvious in further view of **Kulakowski**. *See* §§IX.A.2.[3]-[4], IV.B.2 (listing grounds); Williams ¶¶192-199.

Kulakowski describes a network security system and method used in “network communications between a server and client device” for “detecting cloned client devices.” Kulakowski ¶¶2, 6; Williams ¶185.

While **Mgrdechian** discloses that device “ID’s are...dynamic,” **Kulakowski** expressly discloses the implementation detail of a “covert identifier generated for the client device” “which changes over time and which can be stored...by the client device and server.” *E.g.*, Kulakowski ¶8. The identifier is “unique to that particular client device” and “may be updated periodically.” Kulakowski ¶8, 78 (“the covert data values may be ‘counter values’...requiring that the client device operate for a period of time before a value changes, thus providing data values that remain fixed at a single value for days, weeks, or months of operation”). **Kulakowski** expressly

teaches covert identifiers that change after a certain period of time to cause potential hackers “logistical problems.” Kulakowski, ¶¶8, 78, 83; Williams ¶186.

As shown in Fig. 4, **Kulakowski** also discloses the capability to differentiate between an authentic device and a “cloned” device “attempting to steal services” through the use of a “covert identifier,” sent from the client to the server, which compares it to the “stored covert identifier.” Kulakowski ¶¶2, 8, 48. If there is not a match, “the server generates a report...indicating that a potential clone has been detected” and the “service may be discontinued to” the cloned device. Kulakowski ¶¶34, 48-49; Williams ¶187.

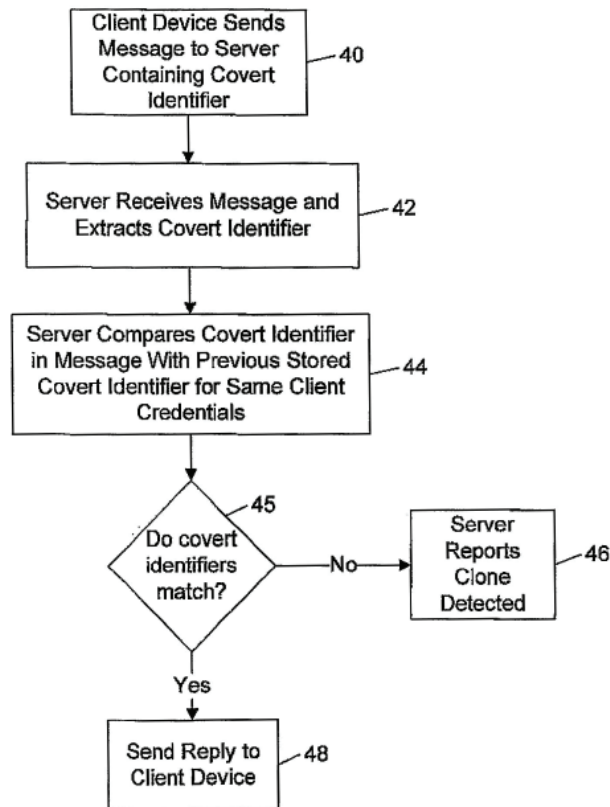


FIG. 4

A POSITA would have been motivated, and would have found it advantageous, to apply **Kulakowski's** teachings described above in implementing **Mgrdechian's** “dynamic” device identifier. Williams ¶188. Like Mgrdechian, **Kulakowski** is in the same field of art and is analogous art to the '164—all are in the same field related to wireless communication systems. *E.g.*, Kulakowski, ¶¶8, 85; Williams ¶188. **Kulakowski** is also reasonably pertinent to the alleged problem identified in the '164 of preventing fraud and spoofing in client-server

communications. *E.g.*, '164, 2:43-56; Kulakowski, ¶2; Williams ¶188. A POSITA would have been motivated to apply **Kulakowski's** known teachings of covert, changing identifiers, in implementing **Mgrdechian's** "dynamic" device identifiers. Williams ¶189. Such application would advantageously improve security and detect spoofed or "cloned" client wireless devices. *E.g.*, Kulakowski, ¶¶8, 15, 48; Mgrdechian, 4:65-5:3, 5:21-30. Moreover, a POSITA would have been motivated to apply **Kulakowski's** known teachings of changing a covert identifier periodically because **Kulakowski** teaches such that changes enable the server to advantageously detect spoofed client devices, as a superseded covert identifier of a spoofed client device would not match the updated covert identifier of the genuine device. *E.g.*, Kulakowski, ¶¶46-48; Williams ¶190. Indeed, such an application would be nothing more than applying **Kulakowski's** known technique of updating a device identifier over time to improve **Mgrdechian's** similar wireless device that uses a dynamic "ID" in the same way. Williams ¶190.

Thus, with respect to claim 3, a POSITA would have been motivated to apply **Kulakowski's teachings of a disclosure policy associated with the second unique identifier or associated with the account associated with the second entity** (*e.g.*, "receiving a message from a client device at a server, the message containing a covert identifier derived from one or more operational events at the client device, determining whether the covert identifier matches a covert identifier for the client

device stored at the server, and reporting detection of a cloned client device if the covert identifiers do not match,” “service may be discontinued to” cloned devices) **allows for secure and fraud resistant application of policies for the disclosure of information and content** (*e.g.*, “detecting clones of true or properly registered client devices attempting to steal services without payment or otherwise mimic a real client device”). *E.g.*, Kulakowski ¶¶2, 6, 8, 49; *see also id.* ¶¶11, 17, 34, 47-48. In applying these teachings, **Mgrdechian’s** disclosure policy allows for the secure and fraud resistant application of policies for the disclosure of information and content by preventing hackers “attempting to steal services” from accessing profile information of the target devices (*e.g.*, “[d]evice C”) when the device identifiers for devices A and B received from device A do not match those stored in the server. *See id.*; Mgrdechian 5:1-3, 13:50-14:8, 16:60-17:10; §IX.A.2.[3]; Williams ¶¶192-196.

With respect to claim 4, a POSITA would have been motivated to apply **Kulakowski’s teachings that the system or a component of the system causes the change of at least one unique identifier from time to time such that disclosure of the at least one unique identifier by one device to another does not compromise the identity of that device once the unique identifier has changed** (*e.g.*, “[T]he covert data values may be ‘counter values’...requiring that the client device operate for a period of time before a value changes, thus providing data values that remain fixed at a single value for days, weeks, or months of operation”). *E.g.*,

Kulakowski ¶¶8, 78, 83, 93, 95. In applying these teachings, **Mgrdechian's** dynamic identifiers are updated periodically in coordination with the server such that disclosure of device C's identifier to device A does not compromise the identity of device C after the identifier is changed because device C's old identifier can no longer be used to retrieve its profile information from the server after the identifier has been changed and any device using the old identifier after the change will be identified as a potential clone. *See id.*; Mgrdechian, 5:1-3, 3:34-35; §IX.A.2.[4]; Williams ¶¶197-199.

In light of the above, a POSITA would have found it routine, straightforward and advantageous to apply **Kulakowski's** known teachings of periodically changing covert identifiers in implementing **Mgrdechian's** teachings of "dynamic" device identifiers and would have known that such a combination (yielding the claimed limitations) would predictably work and provide the expected functionality. Williams ¶191.

D. Grounds 6 And 7: Claim 7 Is Rendered Obvious By Mgrdechian In View Of Eagle (Ground 6), And In Further View Of Kaplan (Ground 7)

To the extent it is argued that further disclosure beyond Mgrdechian's teaching of filtering profile information based on list of friends is required for claim 7 (*see* §§IX.A.2.[7]), claim 7 is rendered obvious in further view of **Eagle**. *See* §§IX.A.2.[7], IV.B.2 (listing grounds); Williams ¶¶200-205.

Eagle teaches a system for using a server to facilitate communications between portable wireless communication devices. *E.g.*, **Eagle**, Abstract, ¶3. The “portable electronic devices” detect other devices and exchange identifying information with them using Bluetooth protocol.” **Eagle** ¶18, claims 2, 3. The identifying information received by an initiating device (a first wireless device) from a target device (a second wireless device) is transmitted to a server using a “long-range cellular phone network.” *E.g.*, **Eagle** ¶¶4, 39. The server provides the initiating device access to the private “friends of friends” content, based on the target device’s list of friends, specifically when an initiating device is listed in a target device’s profile as corresponding to a “device[] owned by [a] ‘friend[].’” **Eagle** ¶¶56, 66; **Williams** ¶¶200-201.

A POSITA would have found it advantageous to apply **Eagle**’s teachings in implementing **Mgrdechian**’s system of facilitating communication between two devices via remote server. **Williams** ¶202. Like **Mgrdechian**, **Eagle** is in the same field and is analogous art to the ’164, namely wireless communication systems. *E.g.*, **Eagle**, Abstract, ¶¶56, 63, 65; **Williams** ¶203. **Eagle** is also pertinent to the alleged problem(s) identified in the ’164 of a “lack of an independent third party to facilitate the services required for a secure proximity based mobile electronic transaction.” *E.g.*, ’164, 2:52-56; **Eagle** ¶9; **Williams** ¶204. For example, **Eagle** discloses the use of a “central server” for “improved privacy protection.” **Eagle** ¶9.

While a POSITA would have understood to use **Mgrdechian's** "list of friends" to filter information being sent from the server to the initiating device (*see* §IX.A.2.[7]), **Eagle** expressly discloses the server using the friends list in each device's "profile data" to define a "trust network," such that the filter parameters prevent disclosure of profile data to devices that are not in the trust network. *E.g.*, Eagle ¶¶56, 60, 66-67. For example, **Eagle** teaches that a device can be set to establish links with others within a "trust network," comprising other users "within one degree from an individual's social circle, i.e.: a friend-of-a-friend." Eagle ¶66; Williams ¶¶201-202. A POSITA would have been motivated to apply Eagle's policy of disclosure only to users within the "trust network" to Mgrdechian's filter parameters as use of a known technique to improve a similar device in the same way. Williams ¶202.

Thus, with respect to claim 7, a POSITA would have been motivated to apply **Eagle's teachings of a disclosure policy that comprises the inclusion of an entity associated with the first wireless device being included in said friends list** (*e.g.*, "The profile data for each user may advantageously include data specifying a set of device IDs for devices owned by 'friends.'") **and resulting in access to the otherwise private social network content of the entity associated with the second wireless device** (*e.g.*, "A given user may then request that alert messages be sent only when such a 'trusted' person having common interests is nearby."). *E.g.*, Eagle

¶¶3-7, 45, 56-66; Williams ¶201. In applying these teachings, **Mgrdechian's** disclosure policy allows sharing device C's profile information including its "list of friends" with device A only if device A's user is included in device C's user's friends list. *See* Mgrdechian, 11:33-34; §IX.A.2.[7]; Williams ¶205.

In light of the above, a POSITA would have found it routine, straightforward and advantageous to apply **Eagle's** known teachings of disclosure only to users within a trust network in implementing **Mgrdechian's** teachings of filter parameters that limit disclosure of non-public information, and would have known that such a combination (yielding the claimed limitations) would predictably work and provide the expected functionality. Williams ¶205.

E. Grounds 8 And 9: Claim 8 Is Rendered Obvious By Mgrdechian In View Of Behrens (Ground 8), And In Further View Of Kaplan (Ground 9)

To the extent it is argued that further disclosure beyond Mgrdechian's teaching that each communication device is provided with a unique ID in the manufacturing process is required for claim 8 (*see* §§IX.A.2.[8]), claim 8 is rendered obvious in further view of **Behrens**. *See* §§IX.A.2.[8], IV.B.2 (listing grounds); Williams ¶¶206-214.

Behrens generally relates to a wireless communication system for detecting proximate wireless devices and communicating with a remote server such that "contact is automatically established between users who come into proximity of one

another.” *E.g.*, Behrens, Abstract, ¶¶1, 160, Fig. 2. Wireless devices in Behrens’s communication system transmit “at least one unique identifier (UID)” using a short-range wireless protocol to “uniquely identif[y]” themselves. *Id.*, ¶97. Behrens teaches that a device may have a “combination” of UIDs, “such as the device’s Bluetooth Device Address or WLAN MAC address,” and “[a] user may...exercise control over which or how many UIDs are transmitted by his device.” *Id.*, ¶¶103, 115, 122, *see also* ¶61, Claims 7-9; Williams ¶¶206-208.

A POSITA would have been motivated, and found it advantageous, to apply Behrens’s teachings of a device sending “multiple or changing UIDs” to another device in implementing Mgrdechian’s “wireless device IDs” to advantageously provide for the simultaneous transmission of multiple device identifiers, including a conventional “MAC” address. Behrens, ¶¶97, 115; Mgrdechian, 6:59-61, 16:16-33; Williams ¶¶209-210. Initiating a direct connection via a local wireless protocol requires knowledge of the other device’s address in that protocol. Thus, simultaneous transmission of multiple UIDs beneficially provides multiple options for contacting the second wireless device at a later time, a goal taught by Mgrdechian. *Id.*; Williams ¶211. Mgrdechian discloses saving “[s]ome or all of the profile information” on the wireless device for “contact[ing] such target at a later time.” Mgrdechian 12:25-28. A POSITA would have been motivated to include both Bluetooth and MAC addresses in the saved information to allow later selection of

either protocol. Williams ¶212. For example, different protocols offer different capabilities. A Wi-Fi connection established using a MAC address enables higher-bandwidth connectivity. Williams ¶212. A Bluetooth protocol connection minimizes energy use and prolongs battery life of the wireless device. Williams ¶212. Like Mgrdechian, Behrens is in the same field and is analogous art to the '164, namely wireless communication systems. *E.g.*, Behrens, Abstract, ¶¶136, 141, Fig. 2; Williams ¶213.

In light of the foregoing, a POSITA would have found it obvious and straightforward to apply Behrens's teachings of sending "multiple or changing UIDs," including a "MAC" address, in implementing Mgrdechian's "wireless device IDs," and would have known that such a combination (yielding the claimed limitations) would predictably work and provide the expected functionality. Williams ¶214.

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 any such evidence could overcome the strong showing of obviousness above or that there is a sufficient nexus to any of the Challenged Claims. *See generally*, Ex. 1002; *see also* Williams ¶¶215-216. Indeed, as demonstrated by the prior art referenced herein, any purported problems, solutions or unexpected results in the

'164 were already well known. Williams ¶¶39-58, 80-214. For example, the alleged needs in the specification do not have a nexus to the claims, which do not require, e.g., a “third trusted party,” a “convenient, electronically secure, personally secure and anonymous method,” “cross validat[ing] the identities of the individuals,” or use “indoors.” '164, 2:1-17. Nevertheless, to the extent PO argues that any of the claims satisfy unmet needs, the prior art already met these alleged needs for the reasons discussed in §IX. Williams ¶¶80-214. 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 '164, which are anticipated and/or rendered obvious for the reasons set forth above. Williams ¶¶217-227. There is a reasonable likelihood that Petitioner will prevail as to each of those claims. *Inter Partes* review of claims 1-8 is accordingly requested.

Dated: June 1, 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 13,978 words as counted by the word processing program used to prepare the paper.

Dated: June 1, 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 '164 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 LLP
Denise M. De Mory - ddemory@bdiplaw.com
Chris J. Coulson - ccoulson@bdiplaw.com

Dated: June 1, 2020

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