

UNITED STATES PATENT AND TRADEMARK OFFICE

---

BEFORE THE PATENT TRIAL AND APPEAL BOARD

---

**TARGET CORPORATION,**

Petitioner,

v.

**PROXICOM WIRELESS, LLC,**

Patent Owner.

---

Case IPR2020-00978

U.S. Patent No. 8,116,749

---

**PETITION FOR *INTER PARTES* REVIEW**

**TABLE OF CONTENTS**

**LIST OF EXHIBITS..... iii**

**I. INTRODUCTION .....1**

**II. MANDATORY NOTICES (§42.8).....5**

A. Real Party-In-Interest .....5

B. Related Matters.....5

C. Lead and Back-Up Counsel and Service Information .....6

**III. PAYMENT OF FEES .....7**

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

A. Grounds for Standing .....7

B. Identification of Challenge.....7

1. The Specific Art on Which the Challenge is Based .....8

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

3. How the Claims Are Unpatentable .....12

**V. THE '749 PATENT .....12**

**VI. PROSECUTION HISTORY .....15**

**VII. LEVEL OF ORDINARY SKILL.....16**

**VIII. CLAIM CONSTRUCTION.....17**

**IX. GROUNDS OF UNPATENTABILITY.....18**

A. Grounds 1-2: Claims 1-3, 13-14, 17-20 Are Anticipated  
(Ground 1) And Rendered Obvious (Ground 2) By Mgrdechian .....19

1. Overview of Mgrdechian .....19

2. Claim Chart—Mgrdechian.....25

B. Ground 3: Claims 1-3, 13-14, and 17-20 Are Rendered Obvious  
By Mgrdechian In View Of Kulakowski .....53

**X. SECONDARY CONSIDERATIONS .....69**

**XI. CONCLUSION .....70**

**LIST OF EXHIBITS**

Ex. 1001	U.S. Patent No. 8,116,749 (“749”)
Ex. 1002	File History of U.S. Patent No. 8,116,749
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- Ex. 1015	Reserved
Ex. 1016	<i>Lighting Science Group Corp. v. Nicor, Inc. et al.</i> , No. 6:16-cv-413-Orl-37GJK, Dkt. 98 (M.D. Fl. May 9, 2017)
Ex. 1017	<i>Lighting Science Group Corp. v. 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	Reserved

Ex. 1023	U.S. Patent Application Publication No. 2005/0174975 (“Mgrdechian ’975”)
Ex. 1024- Ex. 1025	Reserved
Ex. 1026	Declaration of Crena Pacheco
Ex. 1027	Reserved
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- Ex. 1031	Reserved
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,<sup>1</sup> Target Corporation (“Petitioner”) petitions for *inter partes* review (“IPR”) of claims 1-3, 13-14, and 17-20 (“Claims”) of U.S. Patent 8,116,749 (“’749”) (Ex. 1001), assigned to Proxicom Wireless, LLC (“PO”) according to USPTO records. There is a reasonable likelihood that at least one challenged claim is unpatentable as explained herein. Petitioner requests review of the Claims, and judgment finding them unpatentable under §102 and/or §103.

## I. INTRODUCTION

The ’749’s purported invention is the use of a “central server” to “facilitat[e] the exchange of information...between two entities associated with two wireless devices.” ’749, Abstract, Title. “Rather than directly exchanging application data flow between the two devices using [a] short range wireless capability, a second wireless capability then allows for one or more of the devices to communicate with a central server via the internet” to perform the exchange. *Id.*, 2:66-3:4. The system coordinates the modification of the device identifiers from time to time to facilitate the exchange of information. *Id.*, 4:22-27; Williams ¶¶1-2, 39.

---

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

'749 admits that, prior to the alleged invention, wireless devices already were configured to use both the short-range and wide-area connections claimed in '749. *Id.*, 2:8-20 (admitting “[m]ost mobile phones on the market today support at least two wireless standards; one for the cellular wireless wide area network connection (WWAN) and one for a wireless personal or local area network” such as “Bluetooth”). And '749 admits that prior art systems already were using wireless devices for e-commerce and social networking applications, including in systems with servers. *Id.*, 1:52-64 (e.g., accessing [www.ebay.com](http://www.ebay.com) via mobile phone), 2:21-34. '749 also admits that prior art systems already implemented changing identifiers. *E.g.*, '749, 10:7-19 (BSSID of Wi-Fi’s “Ad-Hoc mode”), Fig. 11 (“Dynamic MAC Address”). Williams ¶¶5, 7, 40-41, 60.

The only purportedly novel elements of '749’s claims are the specific steps of a first wireless device providing initial identification information received from a second wireless device to a central server, then the second wireless device providing modified identification information to the first device. Ex. 1002, 183, 267. For example, independent claim 1 requires a first wireless device receiving identification information from a second wireless device and providing that “initial identification information to a central server.” The second wireless device then sends “modified identification information” to the first wireless device. But, as discussed herein, it

was already well-known to authenticate wireless devices using device identifiers that change in a dynamic or pseudo-random manner. Williams ¶¶42-58.

For example, **Mgrdechian** (Ex. 1005) discloses a known system for using a server to facilitate communications between portable communication devices. *E.g.*, *Mgrdechian*, 1:31-34, 5:4-7. As further discussed in §IX below, a first wireless device uses Bluetooth to receive identifying information from a second wireless device and transmits that identifying information to a server using a long-range communication network. *Id.* 3:14-42, 10:10-15. The server associates device IDs with other information associated with the device’s user. *Id.*, 5:1-3, 11:1-10, 13:16-21. Each wireless device changes its ID in a “dynamic” or “pseudo-random” manner, which is generated using the device’s “local software application[.]” *Id.*, 5:1-3, 9:37-40. These ID changes are coordinated with the server such that the updated IDs are associated with the user’s information. *Id.*, 5:1-3, 11:1-10, 13:16-21. Williams ¶¶49, 52.

Thus, and as further explained below, **Mgrdechian** anticipates claims 1-3, 13-14, and 17-20 and at minimum renders obvious all the Claims. Williams ¶¶95-151.

To the extent it is argued further disclosure beyond **Mgrdechian** is required for the Claims, **Kulakowski** (Ex. 1013) makes express what a POSITA would have also understood from *Mgrdechian*’s teachings. **Kulakowski** teaches implementation details such as changing the identifiers of devices based on operational

characteristics or events of the device to guard against cloning, which render the Claims obvious when these teachings are applied to **Mgrdechian**'s device identifiers, as discussed in §IX.B. *E.g.*, Kulakowski ¶8. Thus, as further explained below, **Mgrdechian** in view of **Kulakowski** renders obvious the Claims. Williams ¶¶152-184.

As demonstrated herein, the prior art anticipates and/or renders obvious the Claims. At best, the Claims of '749 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** and/or rendered obvious by **Mgrdechian** in view of **Kulakowski**. 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** or **Kulakowski** or any other references providing analogous disclosures during prosecution of '749. Had such references been considered previously, the Claims would have been found unpatentable.

As explained in greater detail herein, all the features of the Claims were known well before the earliest possible priority date of '749, and the purported invention is anticipated by the prior art and at most no more than an obvious combination of prior art elements combined according to known methods to yield

predictable results. Petitioner requests that the Board institute trial and find the 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 '749 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 Corporation*, No. 6:19-cv-1886-Orl-37LRH (M.D. Fla.) (pending).

The following table lists matters regarding related patents:

Patent No.	IPR
9,038,129	IPR2020-00903
7,936,736	IPR2020-00904
8,090,359	IPR2020-00931
	IPR2020-00932
8,374,592	IPR2020-00933

8,385,896	IPR2020-00934
8,369,842	IPR2020-00977
8,385,913	IPR2020-00980
9,161,164	IPR2020-00979

**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](mailto:james.l.davis@ropesgray.com)

[Target-Proxicom-IPR-Service@ropesgray.com](mailto: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](mailto: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. 001008-0037-652.

### **IV. REQUIREMENTS FOR INTER PARTES REVIEW**

#### **A. Grounds for Standing**

Pursuant to §42.104(a), Petitioner certifies that '749 is available for IPR. Petitioner is not barred or estopped from requesting IPR challenging the claims of '749 on the grounds identified herein.

#### **B. Identification of Challenge**

Pursuant to §§42.104(b), (b)(1), Petitioner requests IPR of claims 1-3, 13-14, and 17-20 of '749, and that the Board cancel the same as unpatentable. '749 matured from U.S. Application 12/364,938 (filed 02/03/2009), and claims priority to U.S. Provisional Application 61/095,359 (filed 9/9/2008), and U.S. Provisional Application 61/095,001 (filed 9/8/2008).<sup>2</sup> Williams ¶¶4, 72-73.

---

<sup>2</sup> 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 '749.

**1. The Specific Art on Which the Challenge is Based**

Petitioner relies upon the following prior art:

<b>Name</b>	<b>Exhibit</b>	<b>Patent / Publication</b>	<b>Filed</b>	<b>Issued / Published</b>	<b>Prior art under at least</b>
<b>Mgrdechian</b>	1005	U.S. 7,545,784	2/10/2005	6/9/2009	§102(e)
<b>Kulakowski</b>	1013	WO 2007/084973	1/19/2007	7/26/2007	§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 (“IDS”) (Ex. 1002, 255, 270), it was not applied to reject the claims during prosecution of ’749 (*id.*, 91-98, 145-57, 210-19). 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 of discretion under § 325(d) as ’955 and ’129 are not parents of ’749, 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. To overcome the second anticipation rejection, the applicant added a new claim (prosecution claim 35) reciting features not found in ’749’s Claims:

wherein said further information comprises content identifying one or more merchants associated with the second unique identifier or information derived from the second unique identifier;

receiving a message from the first wireless device indicating a user selection of one of said one or more merchants;

receiving a message from the first wireless device indicating selection of input on the first wireless device to engage in a transaction with said selected merchant; and

sending an image of an entity associated with the first unique identifier or with an identifier or other data derived from the first unique identifier to a device associated with the selected merchant,

receiving a message from said device associated with the selected merchant indicating a confirmation that the image matches the entity associated with first unique identifier, and to precede with further steps of said multistep electronic commerce transaction.

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 that those claims were unpatentable over Mgrdechian '975. Ex. 1028, 327, 333. Because '955's issued claims recite features not present in '749's Claims, the '955 prosecution is relevant to '749 only in that the applicant never succeeded in overcoming Mgrdechian '975 as to the canceled claims.

Additionally, '129 was filed January 18, 2013, almost a year after '749 issued. Ex. 1001, 1; Ex. 1029, 1. Accordingly, the '129 office actions applying Mgrdechian '975 were not and could not have been before '749's 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 '749's prosecution, these citations did not identify any particular portions of the disclosures relevant to '749's claims, and '749's examiner did not rely on **Mgrdechian** or Mgrdechian '975 during '749's prosecution. Ex. 1002, 257, 272. 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 '749. The Examiner never considered the grounds presented herein or the testimony of Petitioner's expert David H. Williams ("Williams," Ex. 1003) regarding the scope and content of the prior art. *See* Ex. 1002. Because the presented grounds are not cumulative of any prior art previously considered, and are not the same or substantially the same as prior art or arguments previously considered, the Board

should not exercise its discretion under §325(d).<sup>3</sup> 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 ’749, PO served its infringement contentions on 2/10/2020, identifying over 120 claims at issue in the litigation, PO has refused to reduce the number of asserted claims, which would have also narrowed the number of claims challenged before the Board, and PO has not yet responded to Petitioner’s invalidity contentions in the litigation; (4) in addition to the claims asserted in the litigation, the petition challenges some claims not asserted in the litigation; (5) the litigation and PTAB parties are the same; and (6) as demonstrated herein, the merits of the grounds raised and public policy favor

---

<sup>3</sup> 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).

institution—the Claims are anticipated, and at minimum rendered obvious, by art 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	1-3, 13-14, 17-20
2		§103	
3	Mgrdechian in view of Kulakowski		

## 3. How the Claims Are Unpatentable

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

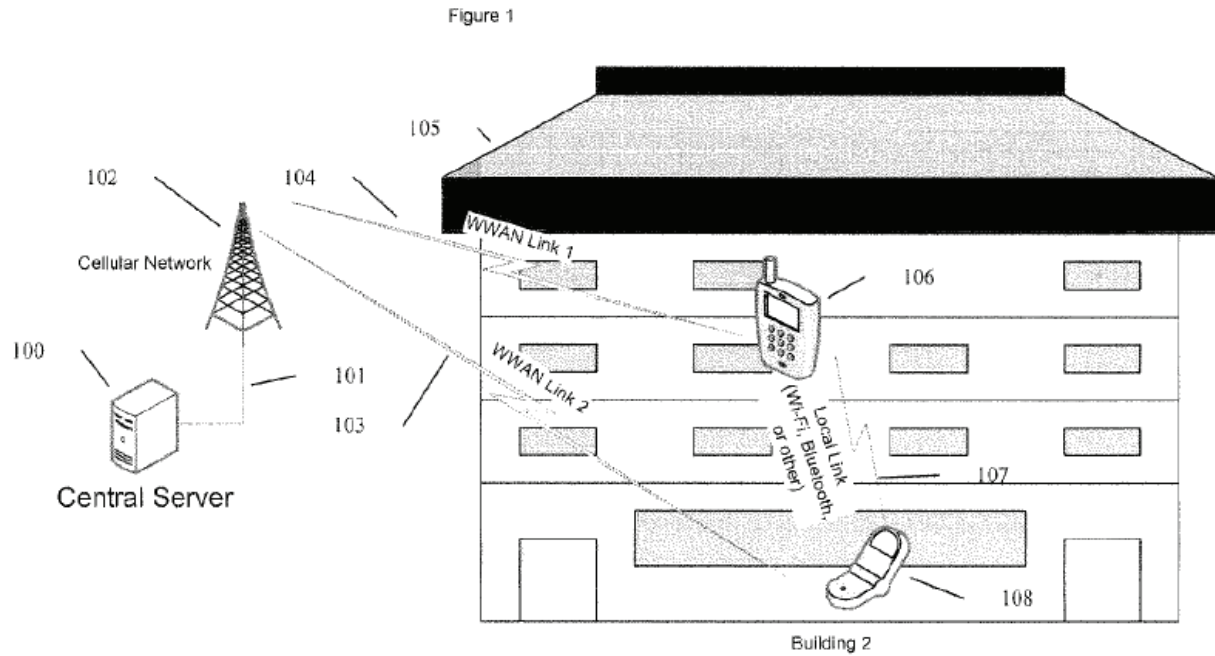
## V. THE '749 PATENT

The '749 describes techniques for using a server to broker the exchange of information between wireless devices. '749, Abstract. Williams ¶¶6, 39. The background section of '749 concedes that wireless devices, such as mobile phones, already had access to both “wide area” cellular connections, and local “Bluetooth” connections permitting “short range” communications. '749, 1:23-34, 2:21-32. '749 also concedes that mobile devices already had access to third party facilitation of electronic transactions, such as purchases on www.ebay.com. '749, 1:52-64. '749 also admits multiple, prior implementations of changing identifiers. *E.g.*, '749, 10:7-

21 (random generation of BSSID of Wi-Fi's "Ad-Hoc mode"), Fig. 11 ("Dynamic MAC Address"). Williams ¶¶35, 40-42, 60.

The '749 combines well-known third party facilitation of transactions and use of changing identifiers with these well-known communication methods. It describes methods for using a server to exchange information using "both a short range and a long range wireless capability" and using changing device identifiers. '749, 2:50-54, 4:22-27. Williams ¶¶6, 39-58, 60-61.

'749's embodiments are directed to some variant of the same general functionality: (1) send an identifier using a short-range connection from a second wireless device to a first wireless device; (2) communicate the received identifier from the first wireless device to a server; and (3) repeat the same process after the second wireless device changes its identifier. For example, Figure 1 of '749 shows that "a central server 100 is connected to devices 106 and 108" through a combination of the Internet, and a "cellular network 102." '749, 5:40-49. The devices are also able to communicate directly with each other via "a short range wireless link 107 such as a Bluetooth." '749, 6:29-37.



'749, Fig. 1; Williams ¶¶62-63. The '749 states that each wireless device searches for nearby devices and exchanges “wireless identifier[s]” using Bluetooth. *E.g.*, '749, 6:45-49. '749 also states that, “[b]y using a central server, the system may coordinate the change of the identifiers from time to time.” '749, 4:22-27. Williams ¶63.

The '749 uses a server to broker the exchange of additional information. '749 states that a first wireless device performs an identifier search and detects a device identifier from a second wireless device. *E.g.*, '749, 6:45-49, 11:26-29, 14:35-47. The first wireless device transmits this received identifying information to a “server” using a cellular or Internet connection. '749, 11:29-34, 14:42-54. The server associates the identifier with the account of an entity such as a person or business.

'749, 8:19-26. '749 states that identifiers are “dynamically assigned” based on “timing” of a “regular interval, or a random generated time period by an algorithm such as a pseudo-random sequence generator, or a combination of both.” '749, 16:58-67. The server coordinates the dynamic identifier updates by communicating with the wireless devices over a data network. '749, 16:67-17:17. Because the server now associates the new identifier with the entity, “ongoing communications and interaction[s]” between the devices are not disrupted. '749, 17:3-17. According to '749, dynamically updating identifiers protects user identities because “disclosure of an identifier by one device to another does not compromise the identity of the device.” *E.g.*, '749, 4:22-27; Williams ¶¶64-65.

## **VI. PROSECUTION HISTORY**

U.S. Patent Application 12/364,938, which matured into '749, was filed 02/03/2009. The examiner rejected the Claims twice over prior art not at issue here. Ex. 1002, 91-98, 145-57. On 12/14/2010, the applicant amended the claims extensively. *Id.*, 183-90. On 7/21/2011, the examiner allowed the Claims and rejected other claims not at issue here. *Id.*, 211-19. As reasons for allowance, the examiner stated the “reviewed prior art” did not contain the following limitations, the second two of which were added in their entireties in the 12/14/2010 amendment:

providing initial identification information to a central server,  
said initial identification information having been collected by the first

wireless device from the second wireless device via a first, direct, short range separate local wireless link

...

wherein the initial identification information is provided to the central server, by the first wireless device, over a second wireless link;

...

providing modified identification information over the first, direct, short range local wireless link in place of the initial identification information, such that the modified identification information is associated at the central server with said identity of a user or entity associated with the second device;

*Id.*, 216-17. The applicant canceled the still-rejected claims, and on 10/14/2011, the examiner issued a Notice of Allowance, repeating the same reasons for allowance.

*Id.*, 239-46, 262-69; Williams ¶66.

## **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 district courts. §42.100(b); Williams ¶¶21, 67. 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 ¶¶22-24.

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 ¶¶67. While the Claims use a term of degree (e.g., “short range local wireless link”), the prior art relied on herein discloses ’749’s examples of those terms as shown in §IX.A below. *See, e.g.*, ’749, 2:59-64 (“short range radio communication standard capabilities such as *Bluetooth*”); Williams ¶¶68-70.

Likewise, regardless of the scope of a central server exchanging information between one application (as recited in “exchange of information between one or more applications executing on at least a first wireless device and a second wireless device”) (claim 1), the prior art relied on herein expressly discloses exchanging information between applications running on a first and second wireless device as shown in §IX. Williams ¶71.

A district court in another proceeding has construed terms of this patent, but these constructions do not impact the outcome of this IPR as the prior art discussed in §IX meets the limitations under either the district court's constructions or the plain and ordinary meaning of the terms. *See* Ex. 1021; Williams ¶67.

## IX. GROUNDS OF UNPATENTABILITY

The '749 is directed to a method and system for facilitating communications between two wireless devices through a server. At their core, the claims recite (1) sending an identifier from a second wireless device to a first wireless device using a short-range connection; (2) communicating the identifier from the first wireless device to a server via a different connection; and (3) repeating this process with a modified identifier from the second wireless device. Claims 1-3, 13-14, and 17-20 are anticipated and, at minimum, these claims are obvious in view of the prior art cited herein, as explained below. Williams ¶¶74-75, 95-97, 152-153.

For example, **Mgrdechian** discloses a system for using a server to facilitate communications between Bluetooth-enabled devices. **Mgrdechian** discloses all the claimed features of the Claims, including devices exchanging dynamic or pseudo-random "identifiers" using a short-range Bluetooth connection, a server receiving the identifiers from the devices, and subsequently exchanging modified identifiers between the devices and sending these identifiers to the server. Williams ¶¶76-85, 95-97.

To the extent it is argued further disclosure is required beyond **Mgrdechian**, **Kulakowski** makes express what a POSITA would have also understood from Mgrdechian's teachings. **Kulakowski's** teachings of changing identifiers for wireless devices in coordination with a server would have been obvious to apply in implementing **Mgrdechian's** wireless devices, which dynamically change identifiers, as discussed in §IX.B. Williams ¶¶86-94, 152-153.

As shown below, the cited prior art renders the Claims of '749 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 '749. Williams ¶¶25-189.

**A. Grounds 1-2: Claims 1-3, 13-14, 17-20 Are Anticipated (Ground 1) And Rendered Obvious (Ground 2) By Mgrdechian**

As further set forth below, Claims 1-3, 13-14, and 17-20 are anticipated by Mgrdechian. However, as further described below for particular limitations, to the extent it is argued that further evidence is required for those limitations, a POSITA would have found the limitations obvious in view of Mgrdechian, rendering the Claims obvious. Williams ¶95.

**1. Overview of Mgrdechian**

**Mgrdechian** discloses a wireless communication system facilitating the “exchange of information between wireless devices” using a “server[.]” *E.g.*,

Mgrdechian, 1:31-34, 5:4-7, 5:16-20, 10:48-56. The wireless communications system includes “[w]ireless devices [A] 310 and [B] 320” that “each include local software applications 311 and 321” and “wireless device identifications 313 and 323,” respectively. Mgrdechian, 9:35-40, 12:7-14. The wireless devices “exchange...information” and “communicate with each other” using “applications 311 and 321” that “control the retrieval of profile information and flow of information between users.” *Id.*, 1:32-35, 9:35-40, 12:7-14.

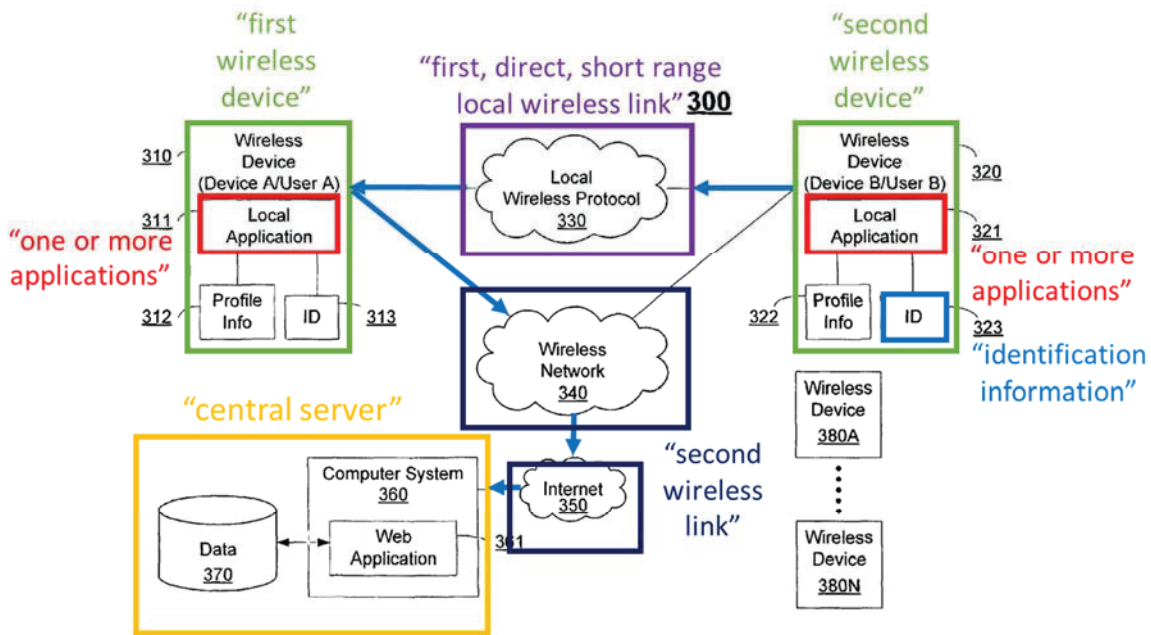


Fig. 3A

Mgrdechian, Fig. 3A (annotated); Williams ¶76.

**Mgrdechian** discloses that “the first wireless device” (e.g., “Device A”) receives an identifier that is associated with a second wireless device (e.g., “Device

B”). Mgrdechian, 3:14-24, 9:35-55. The wireless devices communicate with each other using a “local wireless protocol,” such as “Bluetooth.” *Id.*, 9:35-55, 10:10-15. The first wireless device “transmit[s]” the second wireless device’s ID to the “server” via a “wireless network...and the Internet.” *Id.*, 3:14-24, 10:48-56. The server stores “profile information associated with each wireless device ID,” including device B’s ID. *Id.*, 3:59-67, 4:4-17, 10:48-61, 13:16-21, 21:46-53; Williams ¶77.

Each wireless device changes its ID in a “dynamic” or “pseudo-random” manner. Mgrdechian, 4:65-5:3. The changed ID is retrieved using the device’s “local software application.” Mgrdechian, 9:34-40. The “ID” is “associated with” the device’s “profile information” at the “server,” which thus also understands that the ID changes in the “dynamic” or “pseudo-random” manner in order to maintain the “association.” *Id.*, 4:65-5:3, 11:1-22, 13:16-21. At minimum, it would have been obvious to do so to advantageously maintain the association of the user’s profile with the user’s device such that the profile could still be accessed, while achieving Mgrdechian’s goal of allowing users to remain anonymous or “pseudonymous[.]” Mgrdechian, 6:15-19; Williams ¶78. After device B’s “dynamic or pseudo-random” ID changes, device A “receives” the modified ID, which then “transmit[s]” the modified ID to the server. Mgrdechian, 3:14-24, 5:1-3, 13:14-18.

In addition, **Mgrdechian** discloses that device B's "local application" retrieves the "dynamic or pseudo-random" device "ID," thus changing the ID based on a rule-based generation local to the device's application. Mgrdechian, 5:1-3, 16:16-19. At minimum, it would have been obvious to implement dynamic or pseudo-random device IDs using pre-set rules to advantageously enable anonymous or "pseudonymous[]" information exchange, a purpose of Mgrdechian's teachings. Mgrdechian, 4:40-47, 6:15-19, 21:58-61. Williams ¶79.

In addition, in light of **Mgrdechian's** teachings of device B's "dynamic or pseudo-random" "ID," and of enabling anonymous or "pseudonymous[]" information exchange, a POSITA would have understood and at least found it obvious that a benefit of having dynamic or pseudo-random device IDs is to protect privacy of the identity of the user or entity associated with device B. Mgrdechian, 5:1-3, 6:15-19; Williams ¶80. Dynamic IDs reduce the risk of unauthorized users accessing other users' profile information, including their identities, because the intercepted, dynamic IDs are used only until the ID is changed. Williams ¶80. The benefit of protecting the privacy of a user's (e.g., device B's user's) identity is consistent with Mgrdechian's disclosures of providing "public profile information while filtering out any information pertaining to a user's true identity" and "encrypt[ing]" and "decrypting" information. Mgrdechian, 16:60-17:10, 17:17-27; Williams ¶80. For the same reasons, a POSITA would have understood and at least

found it obvious that a benefit of having dynamic device IDs is to validate the legitimacy of the first device and its application, because only nearby devices recently receiving the second device's updated identifier could access the second device's profile information. Mgrdechian, 5:1-3, 5:66-6:5, 10:29-38, 12:53-56, 21:33-41, Fig. 12; Williams ¶80. Devices using superseded identifiers (such as devices who have since moved out of range, or devices using illicitly-obtained identifiers) would not gain access to profile information. Williams ¶80. This would have furthered Mgrdechian's goal of allowing communications only while devices are "in the same area." Mgrdechian, 10:29-38; Williams ¶80.

**Mgrdechian** teaches a server "receiv[ing] device IDs of a target user and an initiating user from an initiating device," generating "a query using the device IDs," and retrieving and comparing "profile information and filter parameters associated with the device IDs" such that "the initiating user may be [allowed or] denied access to the target's profile." Mgrdechian, 5:1-3, 13:50-14:8. Mgrdechian further teaches "den[ying] access" to a user's profile if parameters are not satisfied. Mgrdechian, 5:1-3, 13:50-14:8. Based on these teachings, a POSITA would have understood and at least found it obvious that a server would deny a query with a superseded device ID to advantageously increase security and maintain the confidentiality of the information by minimizing the time during which unauthorized users using improperly obtained IDs could access private information. Williams ¶81.

**Mgrdechian** discloses that the “dynamic or pseudo-random” ID of the second wireless device is received by the server and used to identify the profile information for the second wireless device. Mgrdechian, 5:1-3, 13:50-14:8. If the ID does not match a profile, but is instead a superseded ID, then the legitimacy, identity and authenticity of the first wireless device that sent the ID is not verified and no information is returned to the first wireless device. *Id.*, 13:50-14:8; Williams ¶82. A POSITA would have understood and at least found it obvious that only a legitimate initiating device (and its application) currently in the proximity of the target device would have either the correct identifier, or the correct combination of initial and modified identifiers from the target device. Williams ¶82. Implementing Mgrdechian’s dynamic or pseudo-random identifiers to permit validation of the legitimacy of the requesting device would have furthered Mgrdechian’s goals of maintaining the confidentiality of the second device’s user unless the initiating device user satisfies the second device user’s filter parameters and allowing communications only while devices are “in the same area.” Mgrdechian, 5:1-3, 6:15-19, 10:29-38, 13:50-14:8; Williams ¶82.

**Mgrdechian** is in the same field of art and is analogous art to ’749—both are in the same field related to wireless communication systems. *E.g.*, ’749, 2:50-54; Mgrdechian, 1:32-35; Williams ¶83.

In addition, Mgrdechian is reasonably pertinent to the alleged problem(s) identified in '749 of overcoming the alleged inaccuracies of GPS systems, and avoiding the alleged security and privacy concerns of direct peer-to-peer communications. *E.g.*, '749, 2:34-42, 3:52-59; Mgrdechian 4:40-47, 9:56-60; Williams ¶84.

In light of the above, to the extent it is argued further disclosure is required, a POSITA would have found it routine, straightforward and advantageous to associate dynamically or pseudo-randomly changing device IDs with user profiles on the server, with IDs that change based on a rule-based generation local to the device in order to protect user privacy, in implementing **Mgrdechian's** wireless communication system, and would have known that such an implementation (yielding the claimed limitations) would predictably work and provide the expected functionality. Williams ¶85.

As further discussed below, Mgrdechian anticipates, and at minimum renders obvious, Claims 1-3, 13-14, and 17-20. Williams ¶¶96-97.

## 2. Claim Chart—Mgrdechian

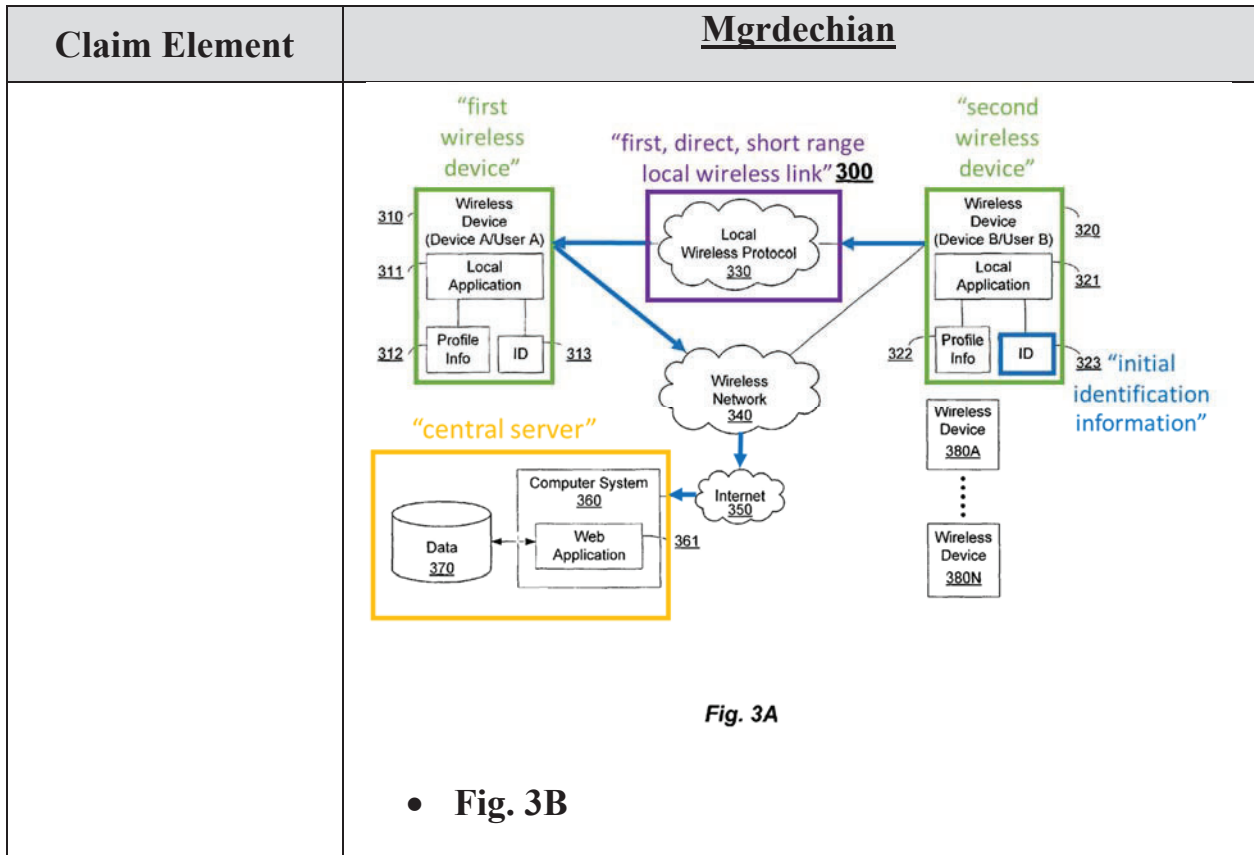
Claim Element	<u>Mgrdechian</u>
[1.pre] A method for exchange of information between one or more applications	<b>Mgrdechian discloses a method for exchange of information between one or more applications executing</b> ( <i>e.g.</i> , “exchange of information between wireless devices,” “[w]ireless devices 310 and 320 each include local software applications 311 and 321”) <b>on at</b>

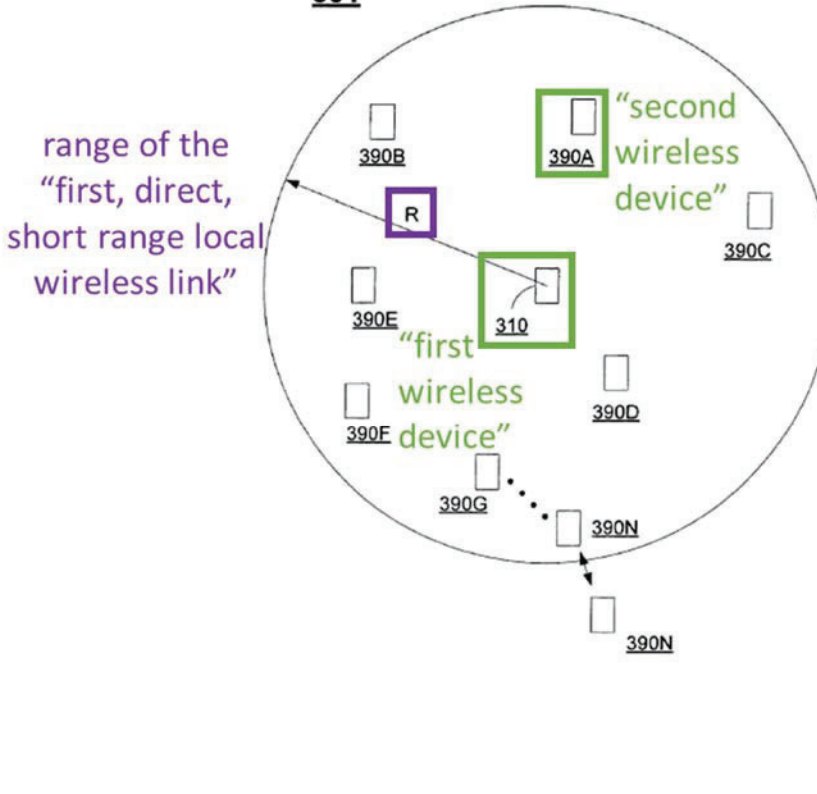
Claim Element	<u>Mgrdechian</u>
<p>executing on at least a first wireless device and a second wireless device, the method comprising the steps of:</p>	<p><b>least a first wireless device</b> (e.g., “first wireless device,” “Device A”) <b>and a second wireless device</b> (e.g., “Device B”).</p> <p><b><u>E.g., Mgrdechian:</u></b></p> <p><b>Mgrdechian</b> discloses “wireless devices [A] 310 and [B] 320” that “each include local software applications 311 and 321” and “wireless device identifications 313 and 323,” respectively. Mgrdechian, 9:35-40, 12:7-14. The wireless devices “exchange...information” and “communicate with each other” using “applications 311 and 321” that “control the retrieval of profile information and flow of information between users.” <i>Id.</i>, 1:32-35, 9:35-40, 12:7-14.</p> <ul style="list-style-type: none"> <li>• <b>1:32-35</b> (“<u>a wireless communication system and method that provides an exchange of information between wireless devices.</u>”)</li> <li>• <b>3:14-24</b> (“receiving in the first wireless device one or more wireless device identifications associated with one or more other wireless devices, and <u>transmitting at least one of the one or more wireless device identifications from the first wireless device to a remote computer system</u>”)</li> <li>• <b>9:35-53</b> (“<u>System 300 may include wireless devices 310 and 320 that communicate with each other using a local wireless protocol 330. Wireless devices 310 and 320 each include local software applications 311 and 321, respectively, and wireless device identifications 313 and 323, respectively.</u> Communication between wireless devices may be initiated by... ‘Device A’)... User A may be referred to herein as the initiator or initiating user..., and <u>Device A may be referred to herein as the initiating device</u>.... The system further includes... ‘Device B’)... User B may be referred to herein as a</li> </ul>

Claim Element	<u>Mgrdechian</u>
	<p>targeted user, and <i>Device B may be referred to herein as the target device.</i>")</p> <ul style="list-style-type: none"> <li> <p><b>12:7-14</b> (“[E]mbodiments of the present invention also include <i>executing software algorithms that control the retrieval of profile information and flow of information between users. Such algorithms may be executed in database 370 or using applications 311 and/or 361. For example, local software application may be used to generate the identification requests for communicating with the remote computer as described herein.</i>”)</p> </li> <li> <p><b>Fig. 3A</b></p> <p>The diagram, labeled Fig. 3A, illustrates a network system. At the top, two wireless devices are shown: 'first wireless device' (310) and 'second wireless device' (320). Each device contains a 'Local Application' (311 and 321 respectively) and 'Profile Info' (312 and 322). A double-headed arrow labeled 'exchange of information' (300) connects the Local Applications of the two devices via a 'Local Wireless Protocol' (330). Below these devices is a 'Wireless Network' (340) and an 'Internet' (350). A 'Computer System' (360) containing a 'Web Application' (361) and a 'Data' database (370) is connected to the Internet. A vertical stack of other wireless devices (380A, ..., 380N) is also shown connected to the network.</p> </li> <li> <p><i>See also</i> 4:48-5:30, 10:34-61, 23:54-67, Fig. 15</p> </li> </ul> <p>Williams ¶¶98-101.</p>
<p>[1.a] at the first wireless device, providing initial identification information to a</p>	<p><b>Mgrdechian discloses at the first wireless device, providing initial identification information to a central server (e.g., “transmitting at least one of the one or more wireless device identifications from the first wireless device to a remote computer system,” “computer system</b></p>

Claim Element	<u>Mgrdechian</u>
<p>central server, said initial identification information having been collected by the first wireless device from the second wireless device via a first, direct, short range local wireless link between the second and first wireless devices,</p>	<p>360...may be an Internet server computer”), <b>said initial identification information having been collected by the first wireless device from the second wireless device via a first, direct, short range local wireless link between the second and first wireless devices</b> (e.g., “receiving in the first wireless device one or more wireless device identifications associated with one or more other wireless devices” via a “local wireless protocol”).</p> <p><b><u>E.g., Mgrdechian:</u></b></p> <p><b>Mgrdechian</b> discloses “receiving in the first wireless device” (e.g., “Device A”) an identifier such as a “wireless device identification[...associated with” the second wireless device (e.g., “Device B”). Mgrdechian, 3:14-24, 9:35-55. The second wireless device communicates with “the first wireless device” using a “local wireless protocol,” such as “Bluetooth.” <i>Id.</i>, 3:14-24, 3:38-42, 9:35-55, 10:10-15. The first wireless device “transmit[s]” the second wireless device’s ID to the “server,” which is a “remote computer system.” <i>Id.</i>, 3:14-24, 10:48-56.</p> <ul style="list-style-type: none"> <li>• <b>3:14-24</b> (“<u>receiving in the first wireless device one or more wireless device identifications</u> associated with one or more other wireless devices, <u>and transmitting at least one of the one or more wireless device identifications from the first wireless device to a remote computer system....</u>”)</li> <li>• <b>3:38-42</b> (“[T]he first wireless device and the one or more other wireless devices are coupled together using a first <u>local wireless protocol</u>, and the first wireless device and the remote computer are coupled together over a second wireless network.”)</li> <li>• <b>9:35-55</b> (“System 300 may include <u>wireless devices 310 and 320 that communicate with each other using a local wireless protocol 330</u>...Communication between wireless devices</li> </ul>

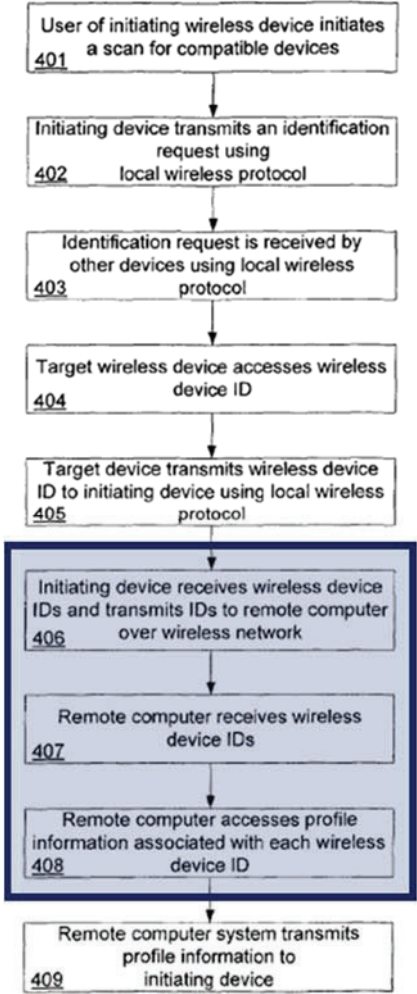
Claim Element	<u>Mgrdechian</u>
	<p>may be initiated by...‘<i>Device A</i>’)...The system further includes...‘<i>Device B</i>’), which may be a device compatible with wireless device 310. User B may be referred to herein as a targeted user, and Device B may be referred to herein as the target device. There can be a plurality of wireless devices 380A-380N that communicate using local wireless protocol 330.”)</p> <ul style="list-style-type: none"> <li>• <b>9:56-58</b> (“[U]sers of wireless devices...interact <u>using a local wireless protocol when the wireless devices are within range</u> of each other.”)</li> <li>• <b>10:10-15</b> (“[W]ireless technologies that may be used as <u>a local wireless protocol include Bluetooth, an 802.11 protocol</u>...for establishing a peer-to-peer or ad hoc network or detecting the presence of other wireless devices and exchanging device IDs.”)</li> <li>• <b>10:48-56</b> (“[R]emote computer system 360...may be an Internet <u>server</u> computer....”)</li> <li>• <b>Fig. 3A</b></li> </ul>



Claim Element	<u>Mgrdechian</u>
	<p style="text-align: center;"><b>301</b></p>  <p style="text-align: center;"><b>Fig. 3B</b></p> <ul style="list-style-type: none"> <li>• <i>See also</i> 3:59-67, 5:4-7, 6:44-47, 13:3-18, 16:6-15, 16:34-42, Fig. 4, Fig. 8</li> </ul> <p>Williams ¶¶102-107.</p>
<p>[1.b] wherein the initial identification information is associated at the central server with an identity of a user or entity associated with the second wireless device, and wherein the initial</p>	<p><b>Mgrdechian discloses that the initial identification information is associated at the central server with an identity of a user or entity associated with the second wireless device (e.g., User B’s “profile information associated with” device B’s ID), and wherein the initial identification information is provided to the central server, by the first wireless device, over a second wireless link (e.g., “the initiating device [device A] may transmit [device B’s ID] to a remote computer system 360</b></p>

Claim Element	<u>Mgrdechian</u>
identification information is provided to the central server, by the first wireless device, over a second wireless link;	<p>through wireless network 340 (e.g., a wireless phone network) and the Internet 350”).</p> <p><b><u>E.g., Mgrdechian:</u></b></p> <p><b>Mgrdechian</b> discloses that the first wireless device (e.g., device A, “initiating device”) “transmit[s] [device B’s ID] to a remote computer system 360 through wireless network 340 (e.g., a wireless phone network) and the Internet 350.” Mgrdechian, 3:38-42, 3:59-67, 4:4-17, 10:48-61, 13:16-21. The remote computer, e.g., a server, stores “profile information associated with each wireless device ID,” including User B’s profile associated with device B’s ID. <i>Id.</i>, 3:59-67, 4:4-17, 10:48-61, 13:16-21, 21:46-53.</p> <ul style="list-style-type: none"> <li>• <b>3:38-42</b> (“[T]he first wireless device and the remote computer are coupled together over <i>a second wireless network.</i>”)</li> <li>• <b>3:59-67</b> (“<i>transmitting at least one of the one or more wireless device identifications from the first wireless device to a remote computer system, and receiving information associated with the one or more wireless device identifications from the remote computer system in the first wireless device.</i>”)</li> <li>• <b>4:4-17</b> (“[A] computer system coupled to a network, ...storing a plurality of wireless device identifications, storing information for a plurality of users, <i>associating the wireless device identifications with the information, receiving one or more wireless device identifications from a wireless device, ...the wireless device identifications and information are stored in a database accessible over the Internet.</i>”)</li> </ul>

Claim Element	<u>Mgrdechian</u>
	<ul style="list-style-type: none"> <li data-bbox="589 317 1424 989">• <b>10:48-61</b> (“<u>[T]he initiating device may transmit the device IDs to a remote computer system 360 through wireless network 340 (e.g., a wireless phone network) and the Internet 350</u>, for example. Computer system 360 may be an Internet server computer and may include multiple computers coupled to the Internet for processing information as described herein, for example, and may further include a web application 361. Computer system 360 may provide access to further information about User B or other users associated with the device IDs received from the initiating device. Furthermore, computer system 360 may act as a central storage location for all user information as well as a clearinghouse and delivery system for messages sent between users.”)</li> <li data-bbox="589 1031 1424 1283">• <b>11:28-33</b> (“Profile information may include a variety of information about a user’s likes and dislikes, background, education, friends and other information such as text, audio, video, images (i.e., electronic pictures of the user), Blogs, links to favorite websites or items or services for sale.”)</li> <li data-bbox="589 1304 1424 1640">• <b>13:16-21</b> (“At 406, <u>the initiating device</u> receives the wireless device IDs from the other wireless devices and <u>transmits the device IDs to a remote computer</u> over a wireless network. At 407, the remote computer (e.g., a server) receives the wireless device IDs. At 408, <u>the remote computer accesses profile information associated with each wireless device ID.</u>”)</li> <li data-bbox="589 1671 1424 1883">• <b>21:46-53</b> (“[A] new user may enter <u>user profile information</u>, configuration parameters (e.g., preferences) and other relevant information (e.g., device ID or other Mobile ID) and may even upload information (e.g., <u>pictures</u>) from a desktop</li> </ul>

Claim Element	<u>Mgrdechian</u>
	<p>computer, wireless device or any other source. The profile information, configuration parameters, associated device IDs and other information may be stored in a database, for example.”)</p> <ul style="list-style-type: none"><li data-bbox="586 516 727 554">• <b>Fig. 4</b></li></ul>  <pre>graph TD; 401[User of initiating wireless device initiates a scan for compatible devices 401] --&gt; 402[Initiating device transmits an identification request using local wireless protocol 402]; 402 --&gt; 403[Identification request is received by other devices using local wireless protocol 403]; 403 --&gt; 404[Target wireless device accesses wireless device ID 404]; 404 --&gt; 405[Target device transmits wireless device ID to initiating device using local wireless protocol 405]; 405 --&gt; 406[Initiating device receives wireless device IDs and transmits IDs to remote computer over wireless network 406]; 406 --&gt; 407[Remote computer receives wireless device IDs 407]; 407 --&gt; 408[Remote computer accesses profile information associated with each wireless device ID 408]; 408 --&gt; 409[Remote computer system transmits profile information to initiating device 409];</pre> <p data-bbox="1159 1587 1243 1621"><b>Fig. 4</b></p> <ul style="list-style-type: none"><li data-bbox="586 1682 727 1719">• <b>Fig. 8</b></li></ul>

Claim Element	<u>Mgrdechian</u>
	<p style="text-align: center;"><b>Fig. 8</b></p> <ul style="list-style-type: none"> <li>• <i>See also</i> 4:48-53, 13:39-49, 16:6-15, 16:34-42, Fig. 3A, Fig. 6</li> </ul> <p>Williams ¶¶108-113.</p>
<p>[1.c] at the second wireless device, upon an occurrence of a predetermined event coordinated with said central server, within a specific application on the second wireless device, providing modified identification information over the first, direct, short range local wireless link in place of the initial identification</p>	<p><b>Mgrdechian discloses at the second wireless device, upon an occurrence of a predetermined event coordinated with said central server, within a specific application on the second wireless device (e.g., see [1.pre]), providing modified identification information (e.g., “the ID’s are...dynamic or pseudo-random”) over the first, direct, short range local wireless link in place of the initial identification information (e.g., see [1.a]), such that the modified identification information is associated at the central server with said identity of a user or entity associated with the second device (e.g., each “ID” is “associated with” the device’s “profile information” at the “server”).</b></p> <p><b><u>E.g., Mgrdechian:</u></b></p> <p><i>See</i> [1.pre]-[1.a].</p> <p>In addition, <b>Mgrdechian</b> discloses that each wireless device, including a second device (e.g., device B) that</p>

Claim Element	<u>Mgrdechian</u>
<p>information, such that the modified identification information is associated at the central server with said identity of a user or entity associated with the second device; and</p>	<p>provides its “ID” to “a first wireless device” using a “local wireless protocol,” changes its ID in a “dynamic” or “pseudo-random” manner, which is provided using the device’s “local software application.” Mgrdechian, 3:38-42, 3:59-67, 4:4-14, 5:1-3, 12:7-14, 16:17-19. The “ID” is “associated with” the device’s “profile information” at the “server,” which thus also understands the ID changes in the “dynamic” or “pseudo-random” manner in order to maintain the “association.” <i>Id.</i>, 5:1-3, 11:7-10, 13:16-21. At minimum, it would have been obvious to do so as discussed in §IX.A.1. Williams ¶119.</p> <ul style="list-style-type: none"> <li>• <b>3:38-42</b> (“[T]he first wireless device and the one or more other wireless devices are coupled together using a first <i>local wireless protocol</i>, and the first wireless device and the remote computer are coupled together over a second wireless network.”)</li> <li>• <b>3:59-67</b> (“[A] communication method comprising <i>receiving in a first wireless device one or more wireless device identifications</i> associated with one or more other wireless devices, transmitting at least one of the one or more wireless device identifications from the first wireless device to a remote computer system....”)</li> <li>• <b>4:4-14</b> (“[A] computer system coupled to a network, ...<i>storing a plurality of wireless device identifications</i>, storing information for a plurality of users, <i>associating the wireless device identifications with the information</i>, receiving one or more wireless device identifications from a wireless device, accessing the information associated with the one or more wireless device identifications, and transmitting the information associated with the one or more wireless device identifications to the wireless device.”)</li> </ul>

Claim Element	<u>Mgrdechian</u>
	<ul style="list-style-type: none"> <li>• <b>5:1-3</b> (“[E]mbodiments of the devices can include cases where <i>the ID’s are static, dynamic or pseudo-random.</i>”)</li> <li>• <b>10:48-56</b> (“[R]emote computer system 360...may be an Internet <i>server</i> computer....”)</li> <li>• <b>11:7-10</b> (“The <i>association</i> may be implemented using a variety of techniques such as associated fields in a relational database or as links or references between objects, for example.”)</li> <li>• <b>12:7-14</b> (“[E]mbodiments of the present invention also include executing software algorithms that control the retrieval of profile information and flow of information between users. Such algorithms may be executed in database 370 or using applications 311 and/or 361. For example, <i>local software application may be used to generate the identification requests</i> for communicating with the remote computer as described herein.”)</li> <li>• <b>13:16-21</b> (“At 406, <i>the initiating device receives the wireless device IDs from the other wireless devices</i> and transmits the device IDs to a remote computer over a wireless network. At 407, the remote computer (e.g., a server) receives the wireless device IDs. At 408, the remote computer accesses <i>profile information associated with each wireless device ID.</i>”)</li> <li>• <b>16:17-19</b> (“If a unique ID is stored in the wireless device, a local application may be included for retrieving the unique ID.”)</li> <li>• <b>Fig. 3A:</b></li> </ul>

Claim Element	<u>Mgrdechian</u>
	<p style="text-align: center;"><b>Fig. 3A</b></p> <ul style="list-style-type: none"> <li>• <i>See also</i> 13:21-23, 13:39-42, 16:6-15, 16:34-42, Fig. 4</li> </ul> <p>Williams ¶¶114-119.</p>
<p>[1.d] at the first wireless device, collecting said modified identification information.</p>	<p><b>Mgrdechian discloses at the first wireless device, collecting said modified identification information</b> (e.g., “receiving in the first wireless device one or more wireless device identifications associated with one or more other wireless devices”; “the ID’s are...dynamic or pseudo-random”).</p> <p><b><u>E.g., Mgrdechian:</u></b></p> <p><i>See</i> [1.a], [1.c].</p> <p>In addition, <b>Mgrdechian</b> discloses that after device B’s “dynamic or pseudo-random” ID changes, device A “receives” the modified ID. Mgrdechian, 3:14-24, 5:1-3, 13:14-18.</p>

Claim Element	<u>Mgrdechian</u>
	<ul style="list-style-type: none"> <li>• <b>3:14-24</b> (“<i>receiving in the first wireless device one or more wireless device identifications associated with one or more other wireless devices</i>”)</li> <li>• <b>5:1-3</b> (“[E]mbodiments of the devices can include cases where <i>the ID’s are static, dynamic or pseudo-random.</i>”)</li> <li>• <b>13:14-18</b> (“At 405, each target wireless device transmits the device ID to the initiating device using the local wireless protocol. At 406, <i>the initiating device receives the wireless device IDs from the other wireless devices</i> and transmits the device IDs to a remote computer over a wireless network.”)</li> <li>• <b>See also</b> 3:59-67, 4:48-5:7, 6:44-47, 9:56-10:1, 16:6-15, Fig. 3A, Fig. 4</li> </ul> <p>Williams ¶¶120-122.</p>
<p>[2] The method of claim 1 wherein the predetermined event is one or more of:</p> <p>an elapsed time;</p> <p>a number of uses of the identifier; and</p> <p>/or</p> <p>a step in a process.</p>	<p>See [1].</p> <p><b>Mgrdechian discloses that the predetermined event is one or more of an elapsed time; a number of uses of the identifier; and/or a step in a process</b> (e.g., “the ID’s are...dynamic or pseudo-random”).</p> <p><b><u>E.g., Mgrdechian:</u></b></p> <p>See [1.c].</p> <p>In addition, <b>Mgrdechian</b> discloses that device B’s “dynamic or pseudo-random” “ID” thus changes based on a step in a process—<i>i.e.</i>, a pseudo-random or dynamic process. Mgrdechian, 5:1-3.</p> <ul style="list-style-type: none"> <li>• <b>5:1-3</b> (“[E]mbodiments of the devices can include cases where <i>the ID’s are static, dynamic or pseudo-random.</i>”)</li> </ul>

Claim Element	<u>Mgrdechian</u>
	<ul style="list-style-type: none"> <li>• <b>16:16-19</b> (“[W]ireless device IDs 813 and 823 are unique identifications. If a unique ID is stored in the wireless device, a local application may be included for retrieving the unique ID.”)</li> </ul> <p>Williams ¶¶123-125.</p>
<p>[3] The method of claim 1 wherein the step of changing the user or entity identification information at said second wireless device is further: effected by a rule-based generation local to the application, downloaded from the server directly, or synchronized such that it is coordinated with predetermined receiving and transmitting times.</p>	<p><i>See</i> [1].</p> <p><b>Mgrdechian discloses that the step of changing the user or entity identification information at said second wireless device is further: effected by a rule-based generation local to the application</b> (<i>e.g.</i>, “the ID’s are...dynamic or pseudo-random”).</p> <p><b><u>E.g., Mgrdechian:</u></b></p> <p><i>See</i> [1.c].</p> <p>In addition, <b>Mgrdechian</b> discloses that the “local application” retrieves the “dynamic or pseudo-random” device “ID,” thus changing the ID based on a rule-based generation local to the device’s application. Mgrdechian, 5:1-3, 12:12-14, 16:16-19. At minimum, it would have been obvious to do so as discussed in §IX.A.1. Williams ¶129.</p> <ul style="list-style-type: none"> <li>• <b>5:1-3</b> (“[E]mbodiments of the devices can include cases where <i>the ID’s are static, dynamic or pseudo-random.</i>”)</li> <li>• <b>12:12-14</b> (“<i>For example, local software application may be used to generate the identification requests for communicating with the remote computer as described herein.</i>”)</li> <li>• <b>16:16-19</b> (“<i>[W]ireless device IDs 813 and 823 are unique identifications. If a unique ID is stored in the</i> </li></ul>

Claim Element	<u><b>Mgrdechian</b></u>
	<p><i>wireless device, a local application may be included for retrieving the unique ID.”)</i></p> <ul style="list-style-type: none"> <li>• <i>See also</i> 10:48-61</li> </ul> <p>Williams ¶¶126-129.</p>
<p>[13] The method of claim 1 wherein the user or entity identification information is changed to protect the privacy of the identity of the a [sic] user or entity associated with the second wireless device.</p>	<p><i>See</i> [1].</p> <p>To the extent the “wherein” clause merely recites an intended result and is not limiting, <b>Mgrdechian</b> anticipates [13] 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, <b>Mgrdechian discloses that the user or entity identification information is changed to protect the privacy of the identity of the user or entity associated with the second wireless device (e.g., “the ID’s are...dynamic or pseudo-random”).</b></p> <p><u><b>E.g., Mgrdechian:</b></u></p> <p><i>See</i> [1.c].</p> <p>In addition, in light of <b>Mgrdechian</b> teachings of device B’s “dynamic or pseudo-random” “ID,” a POSITA would have understood and at least found it obvious that dynamic or pseudo-random device IDs protect the privacy of the identity of the user or entity associated with device B, which is also consistent with Mgrdechian’s disclosures of providing “public profile information while filtering out any information pertaining to a user’s true identity” and “encrypt[ing]” and “decrypting” information, as discussed in §IX.A.1. Mgrdechian, 5:1-3, 12:12-14, 16:16-33, 16:60-17:10, 17:19-27; Williams ¶132.</p>

Claim Element	<u>Mgrdechian</u>
	<ul style="list-style-type: none"> <li data-bbox="589 317 1406 436">• <b>5:1-3</b> (“[E]mbodiments of the devices can include cases where <i>the ID’s are static, dynamic or pseudo-random.</i>”)</li> <li data-bbox="589 478 1406 940">• <b>10:48-61</b> (“[T]he initiating device may transmit the device IDs to a remote computer system 360 through wireless network 340 (e.g., a wireless phone network) and the Internet 350, for example....<i>Computer system 360 may provide access to further information about User B or other users associated with the device IDs received from the initiating device. Furthermore, computer system 360 may act as a central storage location for all user information as well as a clearinghouse and delivery system for messages sent between users.</i>”)</li> <li data-bbox="589 982 1406 1150">• <b>16:16-19</b> (“[W]ireless device IDs 813 and 823 are <i>unique identifications. If a unique ID is stored in the wireless device, a local application may be included for retrieving the unique ID.</i>”)</li> <li data-bbox="589 1192 1406 1816">• <b>16:62-17:10</b> (“<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 in response to a request 805), and may store other information that may be designated public (i.e., information may be disclosed in response to a request 805)....Thus, non-public information may be filtered out when generating reply 806. For example, the true identity of User B may be stored in the database 870 and designated non-public (e.g., when the user signs up for the service). Therefore, a particular request 805 may only return public profile information while filtering</i>”)</li> </ul>

Claim Element	<u>Mgrdechian</u>
	<p><i>out any information pertaining to a user’s true identity.”)</i></p> <ul style="list-style-type: none"> <li>• <b>17:19-27</b> (“[T]he senders of these requests and replies may include additional software code that <i>encrypts the transmitted data</i>, and the recipients of these requests and replies come with software code for <i>decrypting the received data</i>.”)</li> <li>• <i>See also</i> 12:12-14.</li> </ul> <p>Williams ¶¶130-132.</p>
<p>[14] The method of claim 1 wherein the user or entity identification information is changed to provide for a confirmation of the identification information provided to the central server, or to provide a validation of the legitimacy of one or both of the first or the second wireless devices and respective applications.</p>	<p><i>See</i> [1].</p> <p>To the extent the “wherein” clause merely recites an intended result and is not limiting, <b>Mgrdechian</b> anticipates [14] for the reasons discussed in [1]. <i>See</i> MPEP §2111.04.I; <i>Minton</i>, 336 F.3d at 1381.</p> <p>To the extent the “wherein” clause is limiting, <b>Mgrdechian discloses that the user or entity identification information is changed...to provide a validation of the legitimacy of one or both of the first or the second wireless devices and respective applications</b> (<i>e.g.</i>, “the ID’s are...dynamic or pseudo-random,” “ID” is “associated with” the device’s “profile information” at the “server”).</p> <p><b><u>E.g., Mgrdechian:</u></b></p> <p><i>See</i> [1.c].</p> <p>In addition, in light of <b>Mgrdechian’s</b> teachings of device B’s “dynamic or pseudo-random” “ID,” a POSITA would have understood and at least found it obvious that dynamic or pseudo-random device IDs validate the legitimacy of the device A and its application, which provide device B’s ID to the server. <b>Mgrdechian</b>, 5:1-3; Williams ¶135. If the provided ID does not match a profile, then the legitimacy of device A is not validated and no information is returned</p>

Claim Element	<u>Mgrdechian</u>
	<p>to device A. Mgrdechian, 13:50-14:8. This would have furthered <b>Mgrdechian’s</b> goal of confirming the identity of the second device’s user by comparing her to a profile image received from the server and verifying the two devices are still “in the same area,” as discussed in §IX.A.1. Mgrdechian, 5:1-3, 5:21-28, 10:34-38; Williams ¶135.</p> <ul style="list-style-type: none"> <li>• <b>5:1-3</b> (“[E]mbodiments of the devices can include cases where <i>the ID’s are static, dynamic or pseudo-random.</i>”)</li> <li>• <b>5:21-28</b> (“<i>Once Device A has received images of the neighboring users from the server or through other means, User A can scroll through them to uniquely select the person with whom they are attempting to communicate or whose profile they wish to view.</i> Upon selection of this person, Device A may upload the request via the cellular network to the server which will then download the associated profile of User B to Device A.”)</li> <li>• <b>10:34-38</b> (“[P]resent invention allow[s] a user...to view information about...another user...if the other user is operating a wireless device in the same area.”)</li> <li>• <b>See also</b> 10:34-38; 11:27-34, 11:59-64, 12:18-26, 13:24-37, 13:50-14:8, Fig. 5</li> </ul> <p>Williams ¶¶133-135.</p>
<p>[17] The method of claim 1 wherein the first wireless device further performs the step of providing modified identification</p>	<p>See [1].</p> <p><b>Mgrdechian discloses that the first wireless device further performs the step of providing modified identification information (e.g., “the ID’s are...dynamic or pseudo-random”) to said central server, as collected</b></p>

Claim Element	<u>Mgrdechian</u>
<p>information to said central server, as collected by the first wireless device from the second wireless device.</p>	<p><b>by the first wireless device from the second wireless device</b> (<i>e.g.</i>, <i>see</i> [1.a]).</p> <p><b><u>E.g., Mgrdechian:</u></b></p> <p><b><i>See</i> [1.a], [1.c]</b></p> <p>In addition, <b>Mgrdechian</b> discloses that after the second device (<i>e.g.</i>, device B) changes its “ID” either in a “dynamic” or “pseudo-random” manner, it is then “broadcast” and received by the “first wireless device,” which “transmit[s]” the modified ID to the server. Mgrdechian, 3:38-42, 5:1-3, 10:49-52, 13:16-21.</p> <ul style="list-style-type: none"> <li>• <b>3:38-42</b> (“[T]he first wireless device and the one or more other wireless devices are coupled together using a first <i>local wireless protocol</i>, and <i>the first wireless device and the remote computer are coupled together over a second wireless network.</i>”)</li> <li>• <b>3:59-67</b> (“[A] communication method comprising...<i>transmitting at least one of the one or more wireless device identifications from the first wireless device to a remote computer system....</i>”)</li> <li>• <b>4:4-14</b> (“[A] computer system coupled to a network,...<i>receiving one or more wireless device identifications from a wireless device....</i>”)</li> <li>• <b>5:1-3</b> (“[E]mbodiments of the devices can include cases where <i>the ID’s are static, dynamic or pseudo-random.</i>”)</li> <li>• <b>10:49-52</b> (“<i>[T]he initiating device may transmit the device IDs to a remote computer system 360 through wireless network 340 (e.g., a wireless phone network) and the Internet 350, for example.</i>”)</li> <li>• <b>13:16-21</b> (“At 406, the initiating device receives the wireless device IDs from the other wireless devices</li> </ul>

Claim Element	<u>Mgrdechian</u>
	<p><i>and transmits the device IDs to a remote computer over a wireless network. At 407, the remote computer (e.g., a server) receives the wireless device IDs. At 408, the remote computer accesses profile information associated with each wireless device ID.”)</i></p> <ul style="list-style-type: none"> <li>• <i>See also</i> 4:48-53</li> </ul> <p>Williams ¶¶136-138.</p>
<p>[18] The method of claim 1 wherein the initial identification information, if re-sent to the central server following said pre-determined event, is processed by said central server in a manner different from which it was processed prior to said pre-determined event.</p>	<p><i>See</i> [1].</p> <p><b>Mgrdechian discloses that the initial identification information, if re-sent to the central server following said pre-determined event, is processed by said central server in a manner different from which it was processed prior to said pre-determined event (e.g., device B’s “profile” not retrieved because prior value for its dynamic or pseudo-random ID no longer “associated” with profile at the server).</b></p> <p><b><u>E.g., Mgrdechian:</u></b></p> <p><b><i>See</i> [1.c].</b></p> <p>In addition, <b>Mgrdechian</b> teaches a server “receiv[ing] device IDs of a target user and an initiating user from an initiating device,” generating “a query using the device IDs,” and retrieving and comparing “profile information and filter parameters associated with the device IDs” such that “the initiating user may be [allowed or] denied access to the target’s profile.” <i>Mgrdechian</i>, 5:1-3, 13:50-14:8. Because the “ID” is “associated with” the device’s “profile information” at the “server,” which thus also understands that the ID changes in the “dynamic” or “pseudo-random” manner in order to maintain the “association.” <i>Id.</i>, 5:1-3, 11:7-10, 13:16-21; Williams ¶141. Based on these teachings, a POSITA would have understood and at least found it obvious that device B’s superseded device ID that</p>

Claim Element	<u>Mgrdechian</u>
	<p>had since been changed could no longer access any stored information consistent with Mgrdechian’s disclosures of “den[ying] access” to a user’s profile if parameters are not satisfied, as discussed in §IX.A.1. <i>Id.</i>; Williams ¶144.</p> <ul style="list-style-type: none"> <li>• <b>3:48-58</b> (“[T]he message is sent from the first wireless device to the remote computer system...<u>[T]he remote computer system filters the message based on the information associated with the at least one wireless device identification.</u> In another embodiment, the method further comprises transmitting a wireless device identification of the first wireless device to the remote computer system, wherein <u>the remote computer system filters the message based on information associated with the wireless device identification of the first wireless device.</u>”)</li> <li>• <b>5:1-3</b> (“[E]mbodiments of the devices can include cases where <u>the ID’s are static, dynamic or pseudo-random.</u>”)</li> <li>• <b>13:50-14:8</b> (“FIGS. 7A-B illustrate filtering based on profile information according to one embodiment of the present invention....Some applications may use the device IDs of both the target and the initiating devices to perform filtering...<u>[A] web application may receive device IDs of a target user and an initiating user from an initiating device. At 702, a query using the device IDs is generated, and at 703 profile information and filter parameters associated with the device IDs are retrieved.</u> At 704, the filter parameters are applied to the profile information. For example, <u>the profile information of a target may be compared to the initiator’s filter parameters,</u> and the target’s profile is filtered out....Alternatively, <u>the profile information of an initiating user may be compared</u></li> </ul>

Claim Element	<u>Mgrdechian</u>
	<p><i>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> At 705, the system branches based on whether or not the filter parameters are satisfied. If the profile information does not pass the filter, the target profiles are rejected at 706. However, if the profile information does pass the filter, the target profiles may be sent to the initiating device at 707.”)</p> <ul style="list-style-type: none"> <li>• <i>See also</i> 5:21-30, 5:51-65, 7:5-9, 11:7-10, 14:9-45, Fig. 7B</li> </ul> <p>Williams ¶¶139-144.</p>
<p>[19] The method of claim 17 wherein the modified identification information is used by the central server to verify the legitimacy, identity or authenticity of the first wireless device.</p>	<p><i>See</i> [17].</p> <p>To the extent the “wherein” clause merely recites an intended result and is not limiting, <b>Mgrdechian</b> anticipates [14] for the reasons discussed in [1]. <i>See</i> MPEP §2111.04.I; <i>Minton</i>, 336 F.3d at 1381.</p> <p>To the extent the “wherein” clause is limiting, <b>Mgrdechian discloses the method of claim 17 wherein the modified identification information (e.g., “the ID’s are...dynamic or pseudo-random”) is used by the central server to verify the legitimacy, identity or authenticity of the first wireless device (e.g., “query using the device IDs” would be unsuccessful).</b></p> <p><b><u>E.g., Mgrdechian:</u></b></p> <p><i>See</i> [14].</p> <p>In addition, <b>Mgrdechian</b> discloses that the “dynamic or pseudo-random” ID of the second wireless device is received by the server and used to identify the profile information for the second wireless device. <i>Mgrdechian</i>, 5:1-3, 13:50-14:8. If the ID does not match a profile, then</p>

Claim Element	<u>Mgrdechian</u>
	<p>the legitimacy, identity and authenticity of the first wireless device that sent the ID is not verified and no information is returned to the first wireless device, and at minimum it would have been obvious to use the modified ID to do so as discussed in §IX.A.1. <i>Id.</i>, 5:1-3, 13:50-14:8.</p> <p>To the extent it is argued that the ID must be checked before and after it has changed, <b>Mgrdechian</b> discloses that the second wireless device’s ID received by the server is used to retrieve the profile information each time the ID is received—both before and after the “dynamic or pseudo-random” change. <i>Id.</i>, 13:50-14:8.</p> <ul style="list-style-type: none"> <li>• <b>3:48-58</b> (“[T]he message is sent from the first wireless device to the remote computer system...<u>[T]he remote computer system filters the message based on the information associated with the at least one wireless device identification.</u> In another embodiment, the method further comprises transmitting a wireless device identification of the first wireless device to the remote computer system, wherein <u>the remote computer system filters the message based on information associated with the wireless device identification of the first wireless device.</u>”)</li> <li>• <b>5:1-3</b> (“[E]mbodiments of the devices can include cases where <u>the ID’s are static, dynamic or pseudo-random.</u>”)</li> <li>• <b>13:50-14:8</b> (“FIGS. 7A-B illustrate filtering based on profile information according to one embodiment of the present invention...Some applications may use the device IDs of both the target and the initiating devices to perform filtering...<u>[A] web application may receive device IDs of a target user and an initiating user from an initiating device.</u> At 702, <u>a query using the device IDs is generated, and at 703 profile information and</u></li> </ul>

Claim Element	<u>Mgrdechian</u>
	<p><i>filter parameters associated with the device IDs are retrieved.</i> At 704, the filter parameters are applied to the profile information. For example, <i>the profile information of a target may be compared to the initiator’s filter parameters</i>, and the target’s profile is filtered out....Alternatively, <i>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.</i> At 705, the system branches based on whether or not the filter parameters are satisfied. If the profile information does not pass the filter, the target profiles are rejected at 706. However, if the profile information does pass the filter, the target profiles may be sent to the initiating device at 707.”)</p> <ul style="list-style-type: none"> <li>• <i>See also</i> 5:21-30, 5:51-65, 7:5-9, 14:9-45, Fig. 7B Williams ¶¶145-148.</li> </ul>
<p>[20] The method of claim 17 wherein the modified identification information is used by the central server to verify the legitimacy, validity, or authenticity of a transaction associated with one of (a) the first wireless device or (b) a user or entity associated with the</p>	<p><i>See</i> [17].</p> <p>To the extent the “wherein” clause merely recites an intended result and is not limiting, <b>Mgrdechian</b> anticipates [14] for the reasons discussed in [1]. <i>See</i> MPEP §2111.04.I; <i>Minton</i>, 336 F.3d at 1381.</p> <p>To the extent the “wherein” clause is limiting, <b>Mgrdechian discloses the method of claim 17 wherein the modified identification information (e.g., “the ID’s are...dynamic or pseudo-random”) is used by the central server to verify the legitimacy, validity, or authenticity of a transaction associated with one of (a) the first wireless device or (b) a user or entity associated with the first wireless device (e.g., “electronic commerce applications”).</b></p>

Claim Element	<u>Mgrdechian</u>
first wireless device.	<p><u><b>E.g., Mgrdechian:</b></u></p> <p><i>See</i> [14], [19].</p> <p>In addition, <b>Mgrdechian</b> discloses that its system is used in “electronic commerce applications” (<i>e.g.</i>, “micro-payment” transactions for “low dollar amount purchases” from device A to device B). <i>Mgrdechian</i>, 5:1-3, 7:42-44, 15:11-15. Thus, in addition to verifying the legitimacy, identity and authenticity of the first wireless device that sent the “dynamic or pseudo-random” ID to the server as discussed in [19], <b>Mgrdechian</b> also discloses verifying the legitimacy, identity and the authenticity of the transaction sent with the second wireless device’s ID for the same reasons, and at minimum it would have been obvious to use the modified ID to do so as discussed in §IX.A.1. If the ID received from the first wireless device does not match the ID associated with any second wireless device’s profile, then the profile will not be retrieved and the transaction will not go through. <i>Id.</i>, 13:50-14:8.</p> <ul style="list-style-type: none"> <li>• <b>3:48-58</b> (“[T]he message is sent from the first wireless device to the remote computer system...<u>[T]he remote computer system filters the message based on the information associated with the at least one wireless device identification.</u> In another embodiment, the method further comprises transmitting a wireless device identification of the first wireless device to the remote computer system, wherein <u>the remote computer system filters the message based on information associated with the wireless device identification of the first wireless device.</u>”)</li> <li>• <b>5:1-3</b> (“[E]mbodiments of the devices can include cases where <u>the ID’s are static, dynamic or pseudo-random.</u>”)</li> </ul>

Claim Element	<u>Mgrdechian</u>
	<ul style="list-style-type: none"> <li data-bbox="589 317 1406 478">• <b>7:42-44</b> (“An additional embodiment of the present invention includes the use of the service and/or hardware for the <u>electronic commerce applications</u> including micro-payments.”)</li> <li data-bbox="589 506 1424 1604">• <b>13:50-14:8</b> (“FIGS. 7A-B illustrate filtering based on profile information according to one embodiment of the present invention....Some applications may use the device IDs of both the target and the initiating devices to perform filtering....<u>[A] web application may receive device IDs of a target user and an initiating user from an initiating device. At 702, a query using the device IDs is generated, and at 703 profile information and filter parameters associated with the device IDs are retrieved. At 704, the filter parameters are applied to the profile information. For example, the profile information of a target may be compared to the initiator’s filter parameters, and the target’s profile is filtered out....Alternatively, 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. At 705, the system branches based on whether or not the filter parameters are satisfied. If the profile information does not pass the filter, the target profiles are rejected at 706. However, if the profile information does pass the filter, the target profiles may be sent to the initiating device at 707.</u>”)</li> <li data-bbox="589 1631 1370 1877">• <b>15:11-15</b> (“An additional embodiment of the present invention includes the use of the service and/or hardware for the <u>electronic commerce applications</u> including micropayments. Micropayments are prepaid accounts that may be used for <u>low dollar amount purchases</u>....”)</li> </ul>

Claim Element	<u>Mgrdechian</u>
	<ul style="list-style-type: none"><li>• <i>See also</i> 5:21-30, 5:51-65, 7:5-9, 14:9-45, Fig. 7B Williams ¶¶149-151.</li></ul>

**B. Ground 3: Claims 1-3, 13-14, and 17-20 Are Rendered Obvious By Mgrdechian In View Of Kulakowski**

To the extent it is argued that further disclosure of the procedure, timing, effect, or purpose of changing an identifier of a device is required for Elements [1.c], [2], [3], [13], [14], [18], [19], or [20], **Kulakowski** provides these teachings and **Mgrdechian** in view of **Kulakowski** renders obvious the Claims. Williams ¶¶152-184. *See* §IX.A.2.

**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. **Kulakowski** discloses that a “covert identifier” is generated for a “client device” and “may comprise one or more covert data values collected and stored by a client device.” Kulakowski ¶8. The “covert data values...may be based on any operational characteristic or event of a client device which changes over time and which can be stored...by the client device and server,” including “the time of occurrence of an event or the number of times a particular event has occurred at the client device.” Kulakowski ¶¶7, 8; Williams ¶86.

**Kulakowski** discloses that the covert identifiers enhance security of communications between client devices. Kulakowski ¶¶63, 73; Williams ¶87. For example, **Kulakowski** discloses that its covert data techniques “enhance...communications...between two computer devices” and can be applied “to any type of client device linked to servers of the service provider, such as personal computers, cellular phones, personal digital assistants (PDAs), video equipment (TIVO, DVD, CD, etc.), and any other type of client device.” Kulakowski ¶¶63, 73; Williams ¶87. **Kulakowski’s** teachings are widely applicable to “all types of software and firmware running in a system including application software, system middleware, billing software, any type of e-commerce transaction, any type of client/server communications, and any type of messaging between a client and a server or where a client needs to be identified.” Kulakowski ¶73. In addition, **Kulakowski’s** covert data techniques “can be applied to any type of network service provider and to any type of client device..., and for any type of service such as...e-commerce,...message communications systems, etc.” Kulakowski ¶63. Williams ¶87.

**Kulakowski** provides further examples of operational events that cause the identifier to change, including “a time at which a predetermined operational event occurs, for example sending or receiving a predetermined message at the client device or server, a firmware update, a delay time between sending a message to the

network and receiving a response from the network.” Kulakowski ¶8. The identifier is “unique to that particular client device” and “may be updated periodically” “to further reduce the risk of successful hacking” by a cloned client device. *Id.*; Williams ¶88.

As shown in Fig. 4 below, **Kulakowski** discloses a method for detecting the presence of a cloned client device such that “a client device sends a message to the server containing a covert identifier,” and the server “receives the message and extracts the covert identifier.” Kulakowski ¶48, Fig. 4. The server “compares the covert identifier with the stored covert identifier” and determines whether there is “a match between” the identifiers. Kulakowski ¶48. If there is a match, “the server sends a message reply when appropriate to the client device...stores the new covert identifier, and the desired service or transaction takes place.” *E.g.*, Kulakowski ¶48. If there is not a match, “the server generates a report...indicating that a potential clone has been detected.” *E.g.*, Kulakowski ¶48; Williams ¶89.

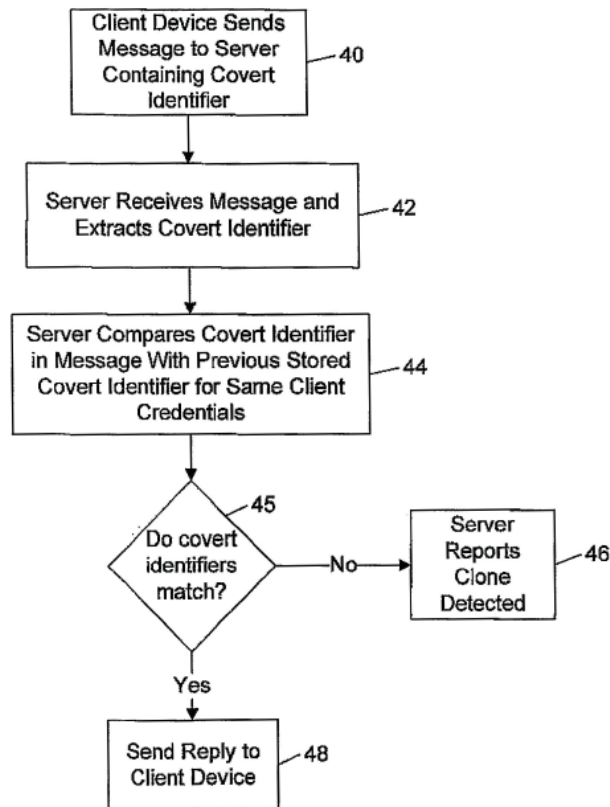


FIG. 4

For example, an “initial covert identifier” is sent to the server, and the server registers the client device and stores the “initial covert identifier.” Kulakowski ¶¶74, Fig. 7. This “initial covert identifier” is used by the client device and server to validate the client device in a manner similar to that described in reference to Figure 4. *Id.* ¶¶48, 74, Fig. 4. To prevent “hackers” from “hack[ing] into the system and obtain[ing] the initial set of covert data values,” “new covert data is created based on operational characteristics as the client device continues to run.” *E.g., Id.* ¶¶75,

Fig. 7. The “new covert data” is added to the “initial set of covert data values in subsequent communications between the server and client device,” wherein new covert data values are “added to the previously stored covert data values for that client device (step 160) at both the server and client device.” *Id.* ¶75. The “new covert data” may be created by timed or counted events, and “[n]ew covert data continues to be added as the client device continues to run.” *Id.* ¶¶10, 75. If the covert data received by the server from the client device does not match the server’s “current set of covert data stored for that client device at the server, a clone detection report is generated.” *Id.* ¶75. As a result, once an operational event has occurred (*e.g.*, a timer has expired) causing a device’s identifier to change, **Kulakowski** teaches that the server refuses access to devices that do not use the updated identifier. *Id.* ¶95 (“The covert identifier may be used...in a periodic renewal process which may eliminate service to cloned client devices.”); Williams ¶90.

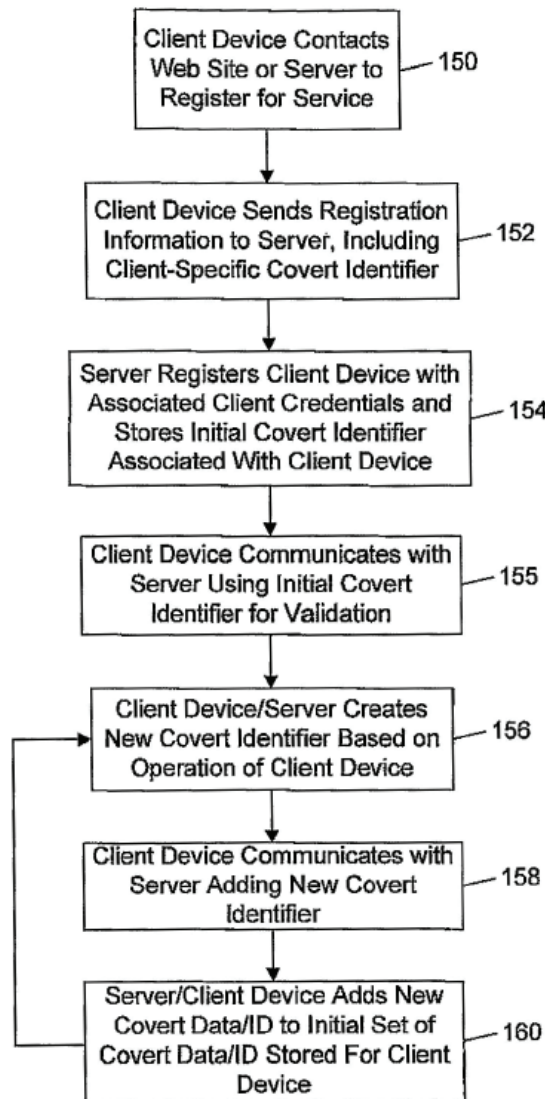


FIG. 7

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 ¶¶91-92. Like Mgrdechian, **Kulakowski** is in the same field of art and is analogous art to '749—all are in the

same field related to wireless communication systems. *E.g.*, Kulakowski ¶¶8, 85; Williams ¶93. **Kulakowski** is also reasonably pertinent to the alleged problem identified in '749 of preventing fraud and spoofing in client-server communications. *E.g.*, '749; 2:34-46; Kulakowski ¶¶2, 73; Williams ¶93. A POSITA would have been motivated to apply **Kulakowski's** known teachings of covert, changing identifiers in implementing **Mgrdechian's** "dynamic" device identifiers. Kulakowski ¶95; Williams ¶92. Such application would advantageously improve security and detect spoofed or "clone" client wireless devices. *E.g.*, Kulakowski ¶¶8, 15, 48; Mgrdechian, 4:65-5:3, 5:21-30; Williams ¶92. **Kulakowski** explains that the "covert identifier" of a client device "changes over time" based on coordination with the server, such as by "sending or receiving a predetermined message at the client device or server." *E.g.*, Kulakowski ¶8. Subsequently, the server compares covert identifiers received in client messages "with the stored covert identifier," and if "there is no match between any part of the covert identifiers, the server...indicat[es] that a potential clone has been detected." *E.g.*, Kulakowski ¶48. Moreover, a POSITA would have been motivated to apply **Kulakowski's** known teachings of changing a covert identifier periodically in implementing **Mgrdechian's** "dynamic" device identifiers. Kulakowski ¶95; Williams ¶92. **Kulakowski** teaches that such changes enable the server to advantageously protect user privacy by validating the legitimacy of the client devices. *E.g.*, Kulakowski ¶¶46-48; Williams ¶92. For

example, 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 ¶92. Further, changing the device identifier periodically as taught in **Kulakowski** renders improperly obtained identifiers worthless after the identifiers are changed, advantageously preventing unauthorized users from accessing private user information. *E.g.*, Kulakowski ¶¶46-48, 88, 95; Williams ¶92. Indeed, such an application would have been nothing more than applying **Kulakowski**'s known technique of authenticating devices by updating device identifiers over time to improve **Mgrdechian**'s wireless devices that use dynamic or pseudo-random "IDs" in the same way. Williams ¶92.

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 ¶94.

Thus, with respect to [1.c], a POSITA would have been motivated to apply **Kulakowski**'s teachings of the second wireless device (*e.g.*, "the client device"), upon an occurrence of a predetermined event coordinated with said central server, providing modified identification information (*e.g.*, "[t]he covert

identifier generated for the client device may comprise one or more covert data values...may be based on any operational characteristic or event of a client device which changes over time and which can be stored...by the client device and server,” “sending or receiving a predetermined message at the client device or server”). *E.g.*, Kulakowski ¶¶6-9, 75, Fig. 7; *see also id.* ¶¶10, 34, 65. For example, **Kulakowski** discloses that the identifier changes upon occurrence of a “predetermined operational event,” which is coordinated with the server via “sending a message to the network and receiving a response from the network.” Kulakowski ¶8. In addition, **Kulakowski** discloses that the covert identifiers enhance security of communications between client devices. Kulakowski ¶¶63, 73. When these **Kulakowski** teachings are applied, **Mgrdechian’s** “dynamic” or “pseudo-random” identifier for device B is changed based on a predetermined event stored in (and thus coordinated between) device B and the server, and then broadcast again by device B to device A. *See id.*; §IX.A.2.[1.c]. Williams ¶¶154-159.

With respect to [2], a POSITA would have been motivated to apply **Kulakowski’s teachings that the predetermined event is one or more of** (*e.g.*, “[t]he covert identifier...may be based on”) **an elapsed time** (*e.g.*, “any operational characteristic or event of a client device which changes over time...such as...a delay time between sending a message to the network and receiving a response from the network”); **a number of uses of the identifier** (*e.g.*, “a value generated by or based

upon one or more operational events, for example...the number of times a particular event has occurred at the client device”); **and/or a step in a process** (e.g., “data received in a message from the server and used in a subsequent message to the server. This value may be updated by the server at each subsequent communication”). E.g., Kulakowski ¶¶7-10, 50; *see also id.* ¶¶34, 51, 69, 84. For example, **Kulakowski** discloses that the covert identifier is updated when predetermined operational events occur, such as a delay time between sending and receiving a reply from a server, the number of times an event has occurred at the client device, and data contained in messages being exchanged with the server. Kulakowski ¶¶7-8. **Kulakowski** also discloses, “[a] covert data value may comprise data received in a message from the server and used in a subsequent message to the server. This value may be updated by the server at each subsequent communication.” Kulakowski ¶9. When these **Kulakowski** teachings are applied, **Mgrdechian’s** “dynamic” or “pseudo-random” identifier for device B changes when one or more of the following occurs: an operational characteristic or event of device B, a number of times a particular event has occurred at device B, and/or data received at device B in a message from the server. *See id.*; §IX.A.2.[2]. Williams ¶¶160-162.

With respect to [3], a POSITA would have been motivated to apply **Kulakowski’s teachings that changing the user or entity identification information at said second wireless device is further effected by a rule-based**

**generation local to the application** (*e.g.*, the “covert identifier may be a value generated by or based upon one or more operational events, for example...the number of times a particular event has occurred at the client device”), **downloaded from the server directly** (*e.g.*, “[a] covert data value such as a token or key received from the server that the client device retains and uses as part of a covert identifier...in subsequent messages with the server”), **or synchronized such that it is coordinated with predetermined receiving and transmitting times** (*e.g.*, “[a] covert data value may comprise data received in a message from the server and used in a subsequent message to the server. This value may be updated by the server at each subsequent communication”; “[t]he time of the last firmware update”). *E.g.*, Kulakowski ¶¶7-10, 50. For example, **Kulakowski** discloses that operational events causing an update to the covert identifier include an event occurring local to the client device, receipt of a token or key downloaded from the server, and data being exchanged in messages with the server. Kulakowski ¶¶7-8, 50. When these **Kulakowski** teachings are applied, the step of changing **Mgrdechian’s** “dynamic” or “pseudo-random” identifier for device B is further effected by a value generated by or based upon one or more operational events at device B, is updated using a token or key received from the server, or is a covert data value that device B receives from (or optionally transmits back to) the server. *See id.*; §IX.A.2.[3]. Williams ¶¶163-165.

With respect to [13], a POSITA would have been motivated to apply **Kulakowski's teachings of changing a device identification to protect the privacy of the identity of the user or entity associated with the second wireless device** (e.g., providing “a network security system...for detecting clones of true or properly registered client devices attempting to steal services without payment or otherwise mimic a real client device,” “a periodic renewal process which may eliminate service to cloned client devices”). E.g., Kulakowski ¶¶2, 5, 8, 95; *see also id.* ¶¶3, 6, 11, 19. For example, **Kulakowski** discloses that using covert identifiers allows the server to detect cloned or spoofed client devices. Kulakowski ¶2. **Kulakowski** discloses that when a covert identifier is updated, “hackers have to re-start their hacking to find the covert identifier of the real client device immediately after receiving the update code.... Such hacking attempts are unlikely to be successful in time.” Kulakowski ¶88. **Kulakowski** also discloses that the server “eliminate[s] service” to devices that do not use the updated covert identifier and thus are detected cloned devices. Kulakowski ¶95. When these **Kulakowski** teachings are applied, **Mgrdechian's** “dynamic” or “pseudo-random” identifier for device B is changed to prevent unauthorized users from using cloned client devices to access services such as personal profiles that include private identifying information. *See id.*; §IX.A.2.[13]. Williams ¶¶166-168.

With respect to [14], a POSITA would have been motivated to apply **Kulakowski's teachings of changing a device identification to provide for a confirmation of the identification information provided to the central server, or to provide a validation of the legitimacy of one or both of the first or the second wireless devices and respective applications** (*e.g.*, “detecting clones of true or properly registered client devices attempting to steal services without payment or otherwise mimic a real client device”; “using the covert identifier...to validate the client device,” “a system including application software”). *E.g.*, Kulakowski ¶¶2, 5, 8, 48, 73-75, Figs. 4, 7; *see also id.* ¶¶3, 14. For example, **Kulakowski** teaches a “client device” and “application software” generating an “identifier” that “changes over time,” providing a secure system that detects “clones of true or properly registered client devices attempting to steal services without payment or otherwise mimic a real client device” by “using the covert identifier...to validate the client device.” Kulakowski ¶2, 5, 8, 48, 73-74. Kulakowski discloses that updating the covert identifier frequently provides only a narrow window in time during which “hackers” can “attempt to duplicate that covert identifier,” which renders the hacking attempt “unlikely to be successful.” Kulakowski ¶88. When these **Kulakowski** teachings are applied, **Mgrdechian's** “dynamic” or “pseudo-random” identifier for device B is changed to validate both device B and its application as a legitimate client device and application that have not been cloned and device A and its

application as a legitimate nearby client device and application which have recently received device B's updated identifier. *See id.*; §IX.A.2.[14]. Williams ¶¶169-171.

With respect to [18], a POSITA would have been motivated to apply **Kulakowski's teachings that the initial identification information, if re-sent to the central server following said pre-determined event, is processed by said central server in a manner different from which it was processed prior to said pre-determined event** (*e.g.*, “using the covert identifier...to validate the client device”; “[i]f the server receives a communication which purports to be from the registered client device but does not have covert data values matching the initial covert data values stored at the server for that client device, a cloned device detection report is generated by the server,” “a periodic renewal process which may eliminate service to cloned client devices.”). *E.g.*, Kulakowski ¶¶2, 5, 8, 14, 48, 74-75, 95, Figs. 4, 7; *see also id.* ¶¶3, 8, 11. **Kulakowski** discloses that, after a covert identifier is updated or renewed, service is eliminated to devices using superseded or incorrect identifiers. Kulakowski ¶¶75, 95. When these **Kulakowski** teachings are applied, after **Mgrdechian's** “dynamic” or “pseudo-random” identifier for device B is changed, the server will determine that any device using device B's superseded identifier is a clone and will prevent such devices from accessing device B's profile information. *See id.*; §IX.A.2.[18]. Williams ¶¶172-174.

With respect to [19], a POSITA would have been motivated to apply **Kulakowski's teachings that the modified identification information is used by the central server to verify the legitimacy, identity or authenticity of the first wireless device** (e.g., “using the covert identifier...to validate the client device”; “[i]f the server receives a communication which purports to be from the registered client device but does not have covert data values matching the initial covert data values stored at the server for that client device, a cloned device detection report is generated by the server”). E.g., Kulakowski ¶¶5, 8, 48, 74-75, Figs. 4, 7; *see also id.* ¶¶3, 8, 11. For example, **Kulakowski** teaches a “client device” and “application software” generating an “identifier” that “changes over time” providing a secure system that detects “clones of true or properly registered client devices attempting to steal services without payment or otherwise mimic a real client device” by “using the covert identifier...to validate the client device.” Kulakowski ¶¶2, 5, 8, 48, 73-74. **Kulakowski** also discloses that its covert data techniques are applied to communications between wireless client devices such as cellular phones and PDAs. Kulakowski ¶¶63 (“any type of client device linked to servers..., such as...cellular phones, personal digital assistants (PDAs)”), 73 (“between two computer devices”). When these **Kulakowski** teachings are applied, **Mgrdechian's** “dynamic” or “pseudo-random” identifier for device B is changed to validate device A as a legitimate nearby client device that has recently received device B's updated

identifier and no cloned device detection report is generated. *See id.*; §IX.A.2.[19].  
Williams ¶¶175-179.

With respect to [20], a POSITA would have been motivated to apply **Kulakowski’s teachings that the modified identification information is used by the central server to verify the legitimacy, validity, or authenticity of a transaction** (*e.g.*, “performing an e-commerce transaction,” “If a match is found,...the desired service or transaction takes place.”) **associated with one of (a) the first wireless device or (b) a user or entity associated with the first wireless device** (*e.g.*, “using the covert identifier...to validate the client device”; “[i]f the server receives a communication which purports to be from the registered client device but does not have covert data values matching the initial covert data values stored at the server for that client device, a cloned device detection report is generated by the server”). *E.g.*, Kulakowski ¶¶5, 8, 18, 48, 74-75, Figs. 4, 7; *see also id.* ¶¶3, 8, 11. For example, **Kulakowski** discloses that the server compares the most recently received covert identifier with a stored identifier, and allows a transaction only if the identifiers match. Kulakowski ¶48. When these **Kulakowski** teachings are applied, **Mgrdechian’s** “dynamic” or “pseudo-random” identifier for device B is used to validate both that a transaction has come from a legitimate client device (device A) that has not been cloned, and that device A is currently nearby device B

because it has the most up-to-date identifier for device B. *See* Kulakowski ¶¶5, 8, 18, 48, 74-75, Figs. 4, 7; *see also id.* ¶¶3, 8, 11; §IX.A.2.[20]. Williams ¶¶180-184.

For the reasons discussed above, the Claims are rendered obvious by **Kulakowski's** teachings of changing the identifiers of devices based on operational characteristics or events of the device, applied to **Mgrdechian's** dynamic device identifiers. *See* §IX.A; Williams ¶¶152-184.

## **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 Claims. *See generally*, Ex. 1002; *see also* Williams ¶¶34, 185-186. Indeed, as demonstrated by the prior art referenced herein, any purported problems, solutions or unexpected results in '749 were already well known. Williams ¶186. 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.” '749, 1:64-2:7. 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 ¶¶74-184. 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 Claims of '749, which are anticipated and, at minimum, rendered obvious for the reasons set forth above. Williams ¶¶187-189. There is a reasonable likelihood Petitioner will prevail as to each of those claims. *Inter Partes* review of claims 1-3, 13-14, and 17-20 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 13,922 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 '749 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 - dmemory@bdiplaw.com  
Chris J. Coulson - ccoulson@bdiplaw.com

Dated: June 1, 2020

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