UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

LINKEDIN CORPORATION,
Petitioner

v.

ALMONDNET, INC. and INTENT IQ, LLC,
Patent Owner

IPR2024-00709
U.S. Patent No. 10,715,878

PETITION FOR *INTER PARTES* REVIEW UNDER 35 U.S.C. § 312 AND 37 C.F.R. § 42.104

TABLE OF CONTENTS

PETITIONER'S EXHIBIT LIST 5

I. MANDATORY NOTICES 7

A. Real Party-in-Interest 7

B. Related Matters..... 7

C. Lead and Back-up Counsel and Service Information 8

II. REQUIREMENTS UNDER §§42.104 AND 42.108 AND CONSIDERATIONS UNDER §§314(A) AND 325(D).....9

A. Standing..... 9

B. Challenge and Relief Requested 9

C. §§314(a) and 325(d) Considerations..... 10

III. PATENT OVERVIEW.....11

A. Level of Ordinary Skill 11

B. Specification Overview 11

IV. CLAIM CONSTRUCTION 13

V. THE CHALLENGED CLAIMS ARE UNPATENTABLE.....13

A. Grounds Overview 13

B. Prior Art Status of Relied-Upon References..... 15

C. Ground 1: Claims 1-2, 8-10, 13-14, 19, and 22 Are Obvious Over Baig in view of Laidlaw, Sitaraman, and Hahn. 17

1. Claim 1 17

2. Claim 2: "The method of claim 1 wherein the first device comprises a mobile device that is connected to the LAN only intermittently." 54

3. Claim 8: "The method of claim 1 wherein the device identifier of at least one of the first device and the second device is a cookie readable by the computer system." 55

4. Claim 9: "The method of claim 8 further comprising, using the computer system, automatically storing, in a memory in the first device, the cookie." 55

5. Claim 10: "The method of claim 1 wherein the device identifiers of the first device and the second device include no personally identifiable information pertaining to a user of the first device or the second device." 56

6. Independent Claim 13 57

7. Claims 14 and 19 58

8. Independent Claim 22 58

D. Ground 2: Claims 3-4, 15-16 Are Obvious Over Ground 1 Prior Art in Further View of Xu. 59

1. Claim 3: "The method of claim 2 wherein the user profile information associated with the device identifier utilized in part (d) comprises behavioral data collected via the first device at a time when the first device is not connected to the LAN." 59

2. Claim 4: "The method of claim 3 wherein the behavioral data collected via the first device is received at the computer system as a result of redirection of the first device from an online site visited by the first device while the first device is not connected to the LAN." 63

3. Claims 15-16 67

E. Ground 3: Claims 6-7, 17-18 Are Obvious Over Ground 1 Prior Art in Further View of Gerace. 67

1. Claim 6: "The method of claim 1 wherein the automatic action comprises selecting an advertisement, from among a plurality of possible advertisements, based at least in part on at least a portion of the user profile information associated with the device identifier of the first device." 68

2. Claim 7: "The method of claim 6 wherein the automatic action comprises causing the selected advertisement to be directed to the second device." 68

3. Claims 17-18 72

F. Ground 4: Claims 11-12, 20-21, 23 Are Obvious Over Ground 1 Prior Art with Xu and Gerace. 72

1. Claim 11 72

2. Claim 12 72

3. Claims 20-21 and 23 73

VI. CONCLUSION 73

CERTIFICATE OF WORD COUNT 74

CERTIFICATE OF SERVICE 75

PETITIONER'S EXHIBIT LIST

Ex.1001	U.S. Patent No. 10,715,878 B2 to Roy Shkedi (filed December 20, 2018, issued July 14, 2020) ("'878" or "'878 patent")
Ex.1002	Declaration of Christopher M. Schmandt ("Schmandt")
Ex.1003	U.S. Patent Application Publication No. 2008/0113674 A1 to Mohammad Faisal Baig (filed October 31, 2007, published May 15, 2008) ("Baig")
Ex.1004	U.S. Provisional Application No. 60/858,204 to Mohammad Baig (filed Nov. 10, 2006) ("Baig Provisional" or "Provisional")
Ex.1005	Redline document showing differences between Baig (EX1003) and Baig Provisional (EX1004)
Ex.1006	U.S. Patent Application Publication No. 2004/0128547 A1 to Robert Laidlaw et al. (filed December 31, 2002, published July 1, 2004) ("Laidlaw")
Ex.1007	U.S. Patent No. 6,427,170 B1 to Aravind Sitaraman et al. (filed December 8, 1998, issued July 30, 2002) ("Sitaraman")
Ex.1008	Excerpts from Harley Hahn, *The Internet Complete Reference* (2d ed. 1996) ("Hahn")
Ex.1009	U.S. Patent No. 7,730,030 B1 to Yongyong Xu (filed August 15, 2004, issued June 1, 2020) ("Xu")
Ex.1010	U.S. Patent Application Publication No. 2006/0282328 A1 to Thomas Gerace et al. (filed June 12, 2006, published December 14, 2006) ("Gerace")
Ex.1011	Excerpts from Robbin Zeff et al., *Advertising on the Internet* (2d ed. 1999) ("Zeff")
Ex.1012	U.S. Patent Application Publication No. 2005/0175181 A1 to Magnus H. Bergs et al. (filed September 7, 2004, published August 11, 2005) ("Bergs")

Ex.1013	Excerpts from *Microsoft Computer Dictionary* (5th ed. 2002)
Ex.1014	Declaration of Sylvia D. Hall-Ellis, Ph.D. ("Hall-Ellis")
Ex.1015	[RESERVED]
Ex.1016	[RESERVED]
Ex.1017	[RESERVED]
Ex.1018	Prosecution history of the '878 patent
Ex.1019	Institution Decision in *Meta Platforms, Inc. v. AlmondNet, Inc. et al.*, No. IPR2022-00773, Paper 6 (PTAB October 22, 2022)
Ex.1020	Complaint filed in *AlmondNet, Inc. v. LinkedIn Corporation*, Case No. 1:23-cv-01373 (D. Del. filed Dec. 1, 2023)
Ex.1021	Proof of Service of Complaint filed in *AlmondNet, Inc. v. LinkedIn Corporation*, Case No. 1:23-cv-01373 (D. Del.)
Ex.1022	Federal Court Statistics, *available at* https://www.uscourts.gov/file/78409/download
Ex.1023	Docket Sheet, *AlmondNet, Inc. v. LinkedIn Corporation*, Case No. 1:23-cv-01373

I. MANDATORY NOTICES

A. Real Party-in-Interest

LinkedIn Corporation is the real party-in-interest to this IPR petition.

B. Related Matters

Patent Owner first asserted the ’878 patent against Petitioner in the following litigation, which remains pending: *AlmondNet, Inc. v. LinkedIn Corporation*, Case No. 1:23-cv-01373 (D. Del. filed December 1, 2023). (**EX1020**.) Petitioner was first served on December 4, 2023. (**EX1021**.)

Meta Platforms, Inc. filed a Petition challenging the ’878 patent, IPR2023-01281 (“the Meta IPR”), which was instituted on February 21, 2024. The instant petition is filed with a motion for joinder to IPR2023-01281 under 35 U.S.C. § 315(c). This petition is substantively identical to the petition in the Meta IPR; it challenges the same claims under the same prior art and grounds.

The ’878 patent is also the subject of other pending litigations involving Patent Owner and various third parties:

- *Roku, Inc. v. AlmondNet, Inc.*, Case IPR2024-00666 (PTAB)
- *Samsung Elecs. Co., Ltd. v. AlmondNet, Inc.*, Case IPR2024-00701 (PTAB)
- *Meta Platforms, Inc. v. AlmondNet, Inc.*, Case IPR2023-01281 (PTAB)
- *AlmondNet, Inc. v. Meta Platforms, Inc.*, Case No. 4:23-cv-00438 (N.D. Cal.)
- *AlmondNet, Inc. v. Samsung Elecs. Co.*, Case No. 4:22-cv-07515 (N.D. Cal.)
- *AlmondNet, Inc. v. Amazon.com, Inc.*, Case No. 6:22-cv-01204 (W.D.

Tex.)

- *AlmondNet, Inc. v. Microsoft Corp.*, Case No. 6:22-cv-01206 (W.D. Tex.)
- *AlmondNet, Inc. v. Roku, Inc.*, Case No. 6-21-cv-00731 (W.D. Tex.)
- *Roku, Inc. v. AlmondNet, Inc.*, Case No. 1:21-cv-01035 (D. Del.)

The '878 patent was also the subject of two earlier IPR petitions filed by third parties Roku (IPR2022-01315) and Samsung (IPR2022-01505) both of which were denied. (*See* IPR2022-01505, Paper 10 (Mar. 22, 2023); IPR2022-01315, Paper 9 (Mar. 13, 2023).) Petitioner had no involvement in either petition.

Petitioner also notes that U.S. Patent No. 8,677,398 B2, an earlier patent in the same family, sharing the same specification, and claiming priority to the same patent application as the '878 patent, was the subject of a prior instituted IPR proceeding involving a third-party and Patent Owner. *See Meta Platforms, Inc. v. AlmondNet, Inc. et al.*, IPR2022-00773, Paper 34 (PTAB Oct. 21, 2022). The Board's institution decision in IPR2022-00773 addressed many of the same issues presented here, including an analysis how the same primary prior art reference (**EX1003**) applies to similar claim limitations. (**EX1019**.) That proceeding was later terminated by the Board pursuant to an agreement between the parties.

C. Lead and Back-up Counsel and Service Information

Lead Counsel
Scott T. Jarratt
HAYNES AND BOONE, LLP
2801 N. Harwood St Suite 2300
Dallas, TX 75201

Phone: (972) 739-8663
Fax: (214) 200-0853
scott.jarratt.ipr@haynesboone.com
USPTO Reg. No. 70,297

Back-up Counsel

Raghav Bajaj
HAYNES AND BOONE, LLP
2801 N. Harwood St Suite 2300
Dallas, TX 75201

Phone: (512) 867-8520
Fax: (214) 200-0853
raghav.bajaj.ipr@haynesboone.com
USPTO Reg. No. 66,630

Angela M. Oliver
HAYNES AND BOONE, LLP
2801 N. Harwood St Suite 2300
Dallas, TX 75201

Phone: (202) 654-4552
Fax: (214) 200-0853
angela.oliver.ipr@haynesboone.com
USPTO Reg. No. 73,271

Laura N. Vu
HAYNES AND BOONE, LLP
2801 N. Harwood St Suite 2300
Dallas, TX 75201

Phone: (415) 293-8930
Fax: (214) 200-0853
laura.vu.ipr@haynesboone.com
USPTO Reg. No. 79,752

Please address all correspondence in this proceeding to lead and back-up counsel. Petitioner consents to service in this proceeding by email at the addresses above.

II. REQUIREMENTS UNDER §§42.104 AND 42.108 AND CONSIDERATIONS UNDER §§314(A) AND 325(D)

A. Standing

Petitioner certifies that the ’878 patent is eligible for IPR and Petitioner is not barred or otherwise estopped.

B. Challenge and Relief Requested

Petitioner requests institution based on:

Ground	Claims	Basis for Challenge under §103
1	1-2, 8-10, 13-14, 19, 22	Baig (EX1003/1004), Laidlaw (EX1006), Sitaraman (EX1007), and Hahn (EX1008)

2	3-4, 15-16	**Ground 1** Prior Art + Xu (EX1009)
3	6-7, 17-18	**Ground 1** Prior Art + Gerace (EX1010)
4	11-12, 20-21, 23	**Ground 1** Prior Art in view of Xu and Gerace

Submitted with this Petition is the Declaration of Christopher Schmandt (**EX1002**) ("Schmandt"), a qualified technical expert. (Schmandt, ¶¶1-7, Ex. A.)

C. §§314(a) and 325(d) Considerations

The *General Plastic* factors are not relevant as this is the first and only IPR petition filed by Petitioner against the '878 patent. The '878 patent was subject to two previous denied IPR petitions (*see* §I.A) and two pending petitions (IPR2024-00701 and IPR2024-00666) filed by parties unrelated to Petitioner. Petitioner was not involved in the preparation or filing of any previous petition. Additionally, as detailed in the accompanying motion for joinder, Petitioner seeks joinder to the Meta IPR, IPR2023-01281.

The *Fintiv* factors weigh in favor of institution. **Factor 1** is neutral —no motion to stay has been filed. *See* EX1023. **Factor 2** favors institution — no trial date has been set, and the median time-to-trial in the District of Delaware is 38.0 months. EX1022. Based on the statistics, trial would occur in February 2026, which is after a final written decision would issue. **Factor 3** favors institution — the litigation is in its early stages, as the complaint was filed only four months ago,

the case is still in early motion practice (*see, e.g.*, EX1023, Dkt. 12, 15, 17), no case schedule has been entered, and no claim construction briefing has occurred. **Factor 4** favors institution — no invalidity contentions have been served and thus there is no present overlap of prior art issues. **Factor 5** is neutral — petitioner is a defendant. **Factor 6** favors institution — the unpatentability grounds are compelling. Indeed, the grounds have already been found to show a reasonable likelihood of prevailing in the Meta IPR.

§325(d): This Petition does not raise §325(d) issues because it relies on new references not considered during the ’878 patent's prosecution or in prior IPR challenges, except for the Meta IPR.

III. PATENT OVERVIEW

A. Level of Ordinary Skill

A person of ordinary skill in the art as of April 17, 2007 would have possessed a bachelor’s degree in electrical engineering or computer science, and two years of work experience in the field of network-based computer systems, such as systems for sending and receiving information over local networks and wide area networks (such as the Internet or World Wide Web). (Schmandt, EX1002, ¶¶10-14.)

B. Specification Overview

The ’878 patent relates “to online access and targeted delivery of

advertisements." ('878, 1:23-24.) It discloses techniques for recognizing related devices so that activities performed with a first device can be used to take an action with respect to a second device. ('878, *e.g.*, 8:13-25.) In one embodiment, targeted advertisements are provided to a user's television based on online activities taking place on their computer. ('878, 8:52-9:8.) Figure 1 depicts a basic layout of a system for targeting advertisements in this context:

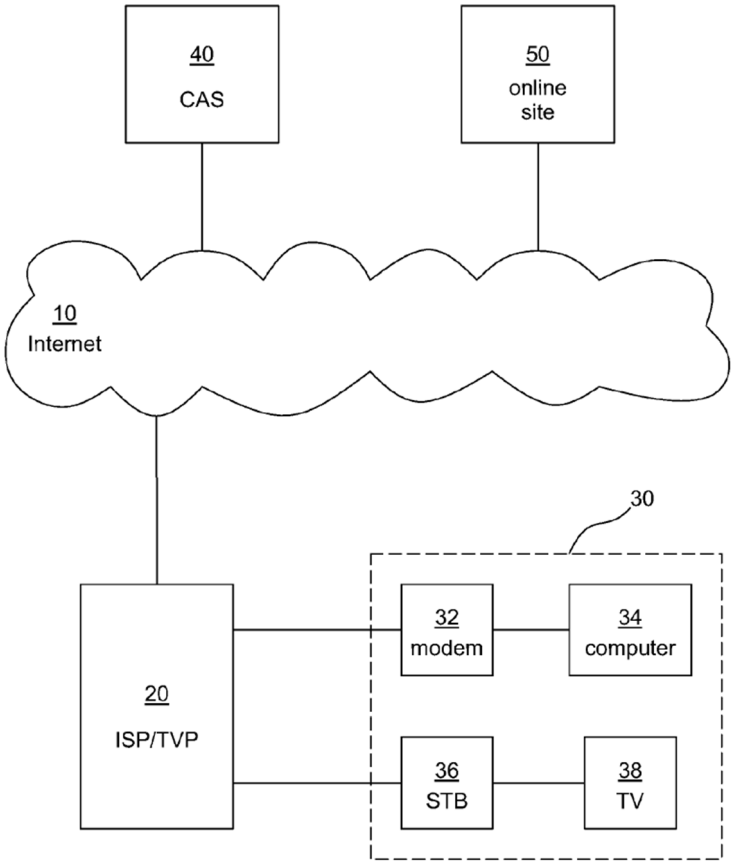


FIG. 1

('878, Fig. 1.) Figure 1 includes online access device **32** (such as a modem), online user interface device **34** (such as a networked computer or mobile device), set-top

box ("STB") **36** and television **38** associated with user **30**. ('878, 9:36-40, 2:49-67.) Common service provider **20** can offer both Internet access via the online access device **32** as well as television service through STB **36**. ('878, 9:45-46.) It also provides to Central Ad Server ("CAS") **40** the IP addresses of the user's devices, such as computer **34** and STB **36**. And online site **50** reports to CAS **40** computer **34**'s online activities at the site. ('878, 11:8-15.) Thus, by determining the computer **34** and STB **36** are related to each other, CAS **40** can provide targeted advertisements to STB/TV based on online activities taking place on the computer. ('878, 9:57-10:18, 10:40-11:62.)

IV. CLAIM CONSTRUCTION

Petitioner does not believe claim construction is necessary at this time, but reserves the right to respond to any claim construction arguments later presented.

V. THE CHALLENGED CLAIMS ARE UNPATENTABLE

A. Grounds Overview

The challenged claims attempt to lay claim to techniques for determining that two devices are connected to the same local area network, and taking action based on that determination. But these techniques were known and the challenged claims rendered obvious by the prior art. In fact, the claims and prior art here are similar to the instituted IPR in *Meta Platforms, Inc. v. AlmondNet, Inc.*, IPR2022-00773, Paper 34 (PTAB Oct. 21, 2022) (**EX1019**), which involved a patent in the same family

with the same specification.

All grounds rely on **Baig** (**EX1003**), which discloses a technique for placing mobile devices connected to the same WiFi access point or hotspot (for example at a coffee shop) into a group, and then providing services (such as chat) to the devices in that group. (Schmandt, ¶¶39-41, 74, 78-79.) Baig is a strong reference that discloses the majority of the limitations. Petitioner cites other references primarily for well-known features that would have fallen within the general knowledge of a skilled artisan.

For example, **Laidlaw** (**EX1006**) discloses known techniques for session management that allow a web server to keep track of users who are currently logged into a website. (Schmandt, ¶¶48-49.) Petitioner relies on Laidlaw for basic web techniques including "cookies" and storage of session management information in a session table. (Schmandt, ¶¶50-52, 88-90.) The proposed grounds also cite **Sitaraman** (**EX1007**), for its disclosure of assigning dynamic IP addresses to devices using the industry-standard Dynamic Host Control Protocol (DHCP) – which was known and admitted prior art in the '878 patent. (Schmandt, ¶¶57-58, 112-113; *see also* '878, 4:7-12.) And finally, all grounds cite **Hahn** (**EX1008**) for techniques, well-known since at least the 1990s, for automatically updating and delivering webpages to visitors. (Schmandt, ¶¶61-62, 141-142, 148.) The remaining references, **Xu** (**EX1009**) and **Gerace** (**EX1010**), are cited in

Grounds 2-4 solely for certain challenged dependent claims. (Schmandt, ¶¶64-66, 69-70.)

B. Prior Art Status of Relied-Upon References

Each reference cited in the grounds listed in **Part II.B** qualifies as prior art. Laidlaw and Sitaraman qualify under at least §102(b) (pre-AIA) because they are patent references published more than one year before April 17, 2007. Hahn qualifies as a prior art printed publication, as evidenced by its availability in public libraries more than one year before the priority date. (Hall-Ellis, EX1014, ¶¶42-48.) Gerace and Xu qualify as prior art under at least §102(e) because they are patent references based on applications filed before the priority date.

Baig qualifies as prior art under at least §102(e). Petitioner acknowledges that the utility application for Baig was filed on October 31, 2007 – after the '878 patent priority date of April 17, 2007 – but Baig claims priority to and incorporates-by-reference an earlier provisional filed on November 10, 2006. (Baig, ¶0001.) Petitioner will refer below to the published Baig patent application (**EX1003**) as "**Baig**," and the provisional application (**EX1004**) as "**Provisional**."

Baig qualifies as prior art as of the filing date of its Provisional.

Baig is usable as §102(e) prior art as of the filing date of the Provisional if: (1) the invalidating disclosures from Baig are supported by the Provisional, and (2) the Provisional provides §112 support for at least one claim appearing in Baig. *See*

MPEP §§2136 (Part I), 2136.02 (Part II). Both are met. Petitioner also notes that in the institution decision on the related '398 patent (IPR2022-00773), the Board preliminarily agreed with Petitioner's priority date showing with respect to Baig. (EX1019, 0010-0011.)

With respect to prong (1), no material differences exist between Baig and the Provisional, as evidenced by a redline comparison submitted herewith. (*See* Schmandt, ¶43 (citing EX1005 (redline comparison)).) All of the relied-upon disclosures in Baig, therefore, appear in the Provisional. Each citation to **Baig** (**EX1003**) will be accompanied by a parallel citation to the **Provisional** (**EX1004**).

With respect to prong (2), the Provisional provides ample §112 support for at least one claim in Baig. The law is clear that claims originally filed with an application can be relied upon for §112 purposes. *See, e.g.*, *In re Gardner*, 480 F.2d 879, 880 (C.C.P.A. 1973). The Provisional here includes originally-filed 17 claims (*i.e.* 1-3, 8-16 and 18-22) that are identical to claims in Baig. (Schmandt, ¶44 (citing EX1005 (redline), 0026-0027).) These originally-filed Provisional claims thus provide written description support for at least their corresponding claims in Baig, and the Provisional would have enabled a skilled artisan to practice their subject matter. (Schmandt, ¶¶44-45.) This alone is sufficient under prong (2).

Beyond that, the disclosures in the Provisional support every limitation of at least published claim 1 and would have enabled a skilled artisan to make and

use its subject matter. (Schmandt, ¶44 (citing for support for each limitation of Baig claim 1: Provisional, 007, 0010-0011 (preamble), Provisional, 007, 0013 ("receiving" step), Provisional, 007, 0010, 0012-114 ("grouping" step), Provisional, 007, 0014, 0024, 0027 ("providing" step).) Baig therefore qualifies as §102(e) prior art as of November 10, 2006.

C. Ground 1: Claims 1-2, 8-10, 13-14, 19, and 22 Are Obvious Over Baig in view of Laidlaw, Sitaraman, and Hahn.

1. Claim 1

The preamble recites: "[**a**] **method for identifying an association among multiple electronic devices of a group of devices connected through a common local area network (LAN) and using the association for cross-device action, the method comprising**…." Assuming the preamble of claim 1 is limiting, it is disclosed and rendered obvious by the prior art.

Baig discloses a technique for identifying when multiple mobile devices are connected to a common local area network (LAN). Baig takes advantage of WiFi networking and WiFi "hotspots" that were common fixtures in the mid 2000s in airports, coffee shops, and other public places. (Schmandt, ¶¶39, 74.) Baig discloses a technique for creating "vicinity-based" communities of devices connected to the same WiFi hotspot. (Baig, ¶0038; Provisional, 0010.) Figure 1 shows the primary

components of the system:

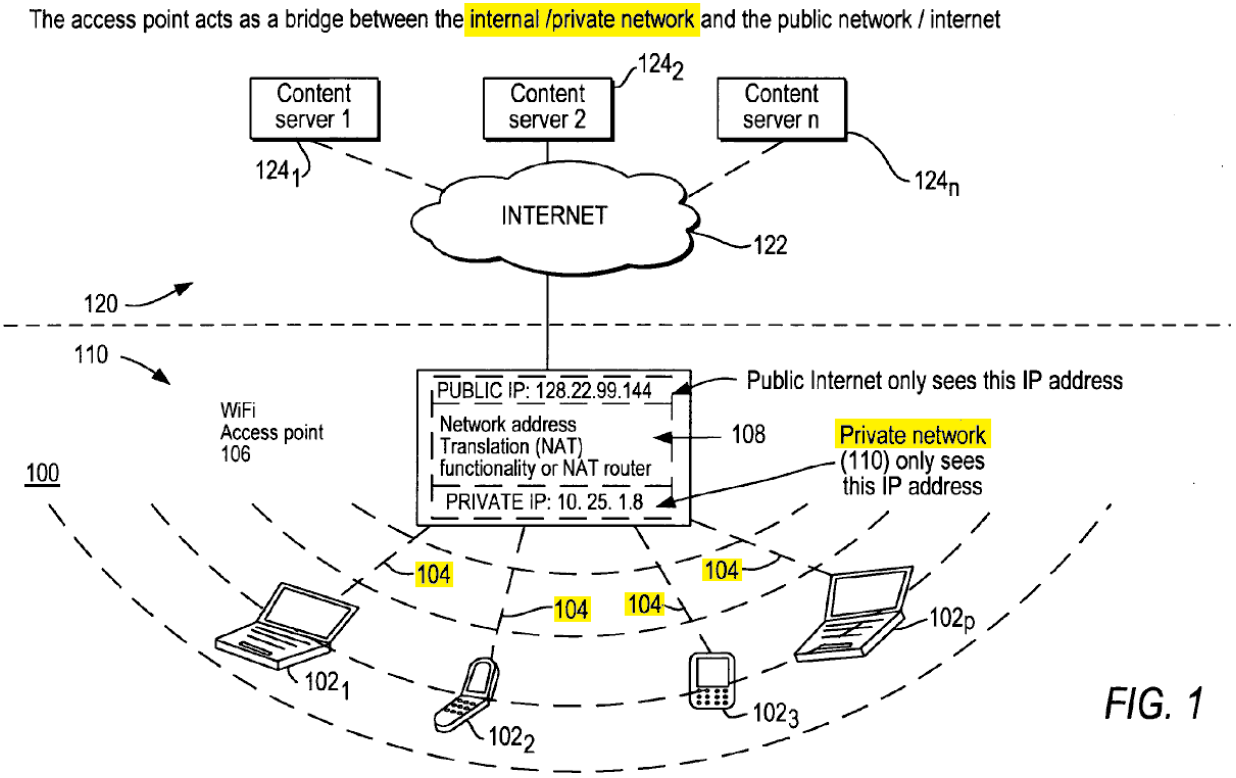


FIG. 1

(Baig, Fig. 1 (highlighting added).) Figure 1 above "illustrat[es] how one or more mobile devices **102** at a public WiFi hotspot **110** interact with the public network **120**." (Baig, ¶0042; Provisional, 0010.) The portion of Figure 1 below the dashed line shows WiFi hotspot **110** that includes access point **106** wirelessly connected to several mobile devices (**102_1** through **102_p**). (Baig, ¶0043; Provisional, 0011.) Access point **106** acts as a router to facilitate communications over the Internet **122** between mobile devices **102** and one or more content servers (**124_1** through **124_n**), which are shown above the dashed line in Figure 1. (Baig, ¶¶0046-0047,

Provisional, 0012.) The content server in Baig is also shown in Figure 2 and also referenced throughout Baig as "content server **224**."

Baig discloses a method for "**identifying an association among multiple electronic devices of a group of devices connected through a common local area network (LAN)**." The claimed "**common local area network (LAN)**" corresponds to local private network **104** in Figure 1, to which each mobile device **102** is connected. (Baig, ¶0043 ("The mobile devices **102** form a 'local network' **104** with the access point **106**…");[1] Provisional, 0011; Schmandt, ¶75.) Local network **104** is also a "**common**" LAN because each mobile device **102** is connected through it.

The "**multiple electronic devices of a group of devices**" correspond to any two or more mobile devices **102** within the plurality of mobile devices $\mathbf{102_1}$ through $\mathbf{102_p}$ and connected to the LAN. As one illustration, the claimed "**multiple electronic devices**" could correspond to laptop computer $\mathbf{102_1}$ and mobile phone $\mathbf{102_2}$ shown in Figure 1 within the plurality of mobile devices.

Baig also discloses the step of "**identifying an association among**" the two or more mobile devices **102**. This step is performed by one or more content servers as shown above the dashed line in Figure 1 above, which communicate with access

[1] Except as otherwise noted, all emphasis (such as underlining, highlighting, bolding) in quotations from the prior art was added by Petitioner.

point **106** via the Internet **122**. (Baig, ¶¶0042-0043, Provisional, 0010-0011.) As Baig explains and shown in Figure 1, access point **106** assigns a "local" IP address to each mobile device **102** to which it is connected, but for communications over the Internet between a mobile device and the content server, access point **106** replaces the local IP address with the common "public" IP address associated with access point **106**. (Baig, ¶¶0044-0046; Provisional, 0011.) This is shown as the "PUBLIC IP" address in Figure 1 above.

In order to determine whether the two or more mobile devices **102** are connected to a common LAN, the content server checks to see if they are connected through an access point **106** having a common IP address as shown in Figure 3:

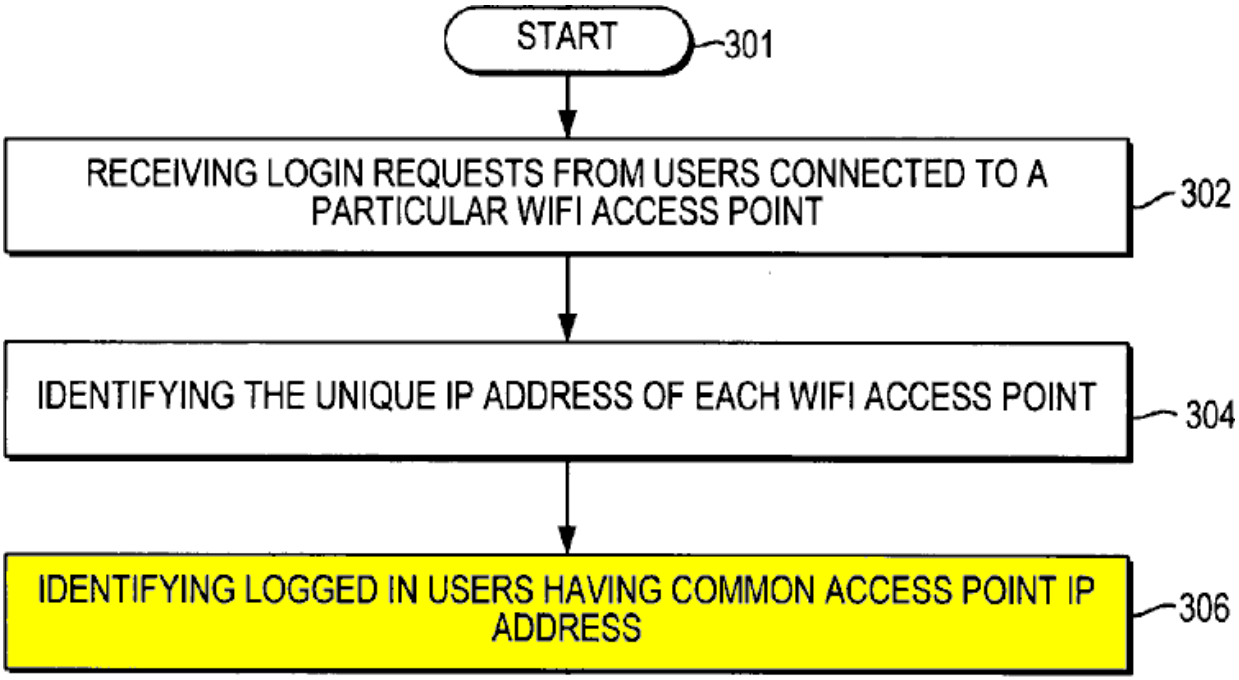


FIG. 3

(Baig & Provisional, Fig. 3 (partial figure; highlighting added).) "At step **306**, the server identifies all the users who have logged in from a common hotspot as having ¶0038; Provisional, 0010.) Baig therefore discloses "**identifying an association among multiple electronic devices**," *i.e.*, multiple mobile devices **102** being connected to the content server through the same access point IP address.

Baig next discloses "**using the association for cross-device action**," as recited in the preamble. After a mobile device in Baig has logged-in, the content server presents a webpage that shows, among other things, a list **660** of other users whose devices are connected to the same hotspot **110**:

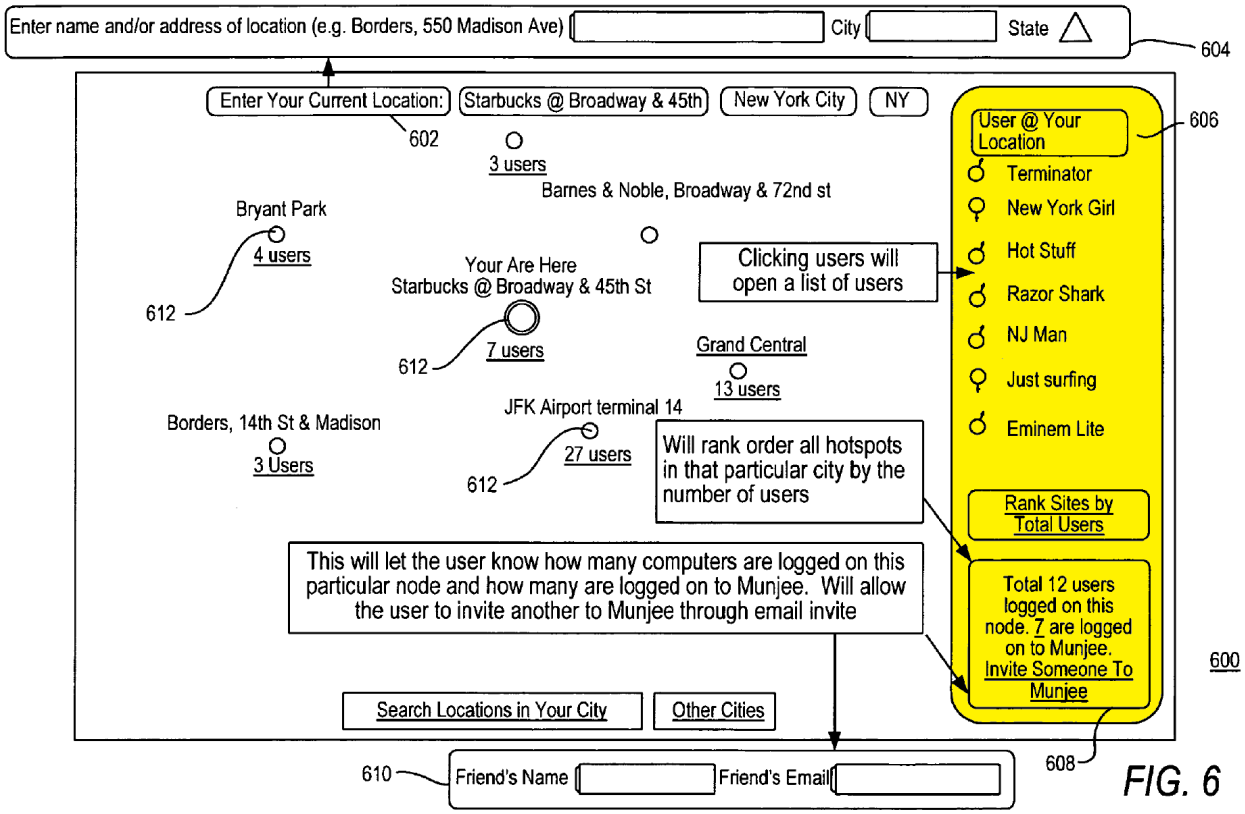


FIG. 6

(Baig, Fig. 6 (highlighting added); Baig, ¶0074; Provisional, 0017.) Figure 6 shows

webpage **600** including list **606**, which "displays a list **606** of other users at the present hotspot **110**." (Baig, ¶0076, Provisional, 0018.) The list **606** in this example shows seven other users (*e.g.* "Terminator," "New York Girl").

The transmission and display of list **606** on mobile devices **102** itself qualifies as "**cross-device action**" because the list would have been transmitted to and displayed on multiple mobile devices that are connected using the same hotspot. And for further examples of "**cross-device action**," the mobile devices connected to the same hotspot can utilize a number cross-device services including "bartering services for goods and services among wireless users in a vicinity," "enabling WiFi users in the vicinity to play video games with one-another, providing chat rooms, among other activities and services." (Baig, ¶0054; Provisional, 0013.) In each case, the cross-device action is provided "**using the association**," because the system uses the fact that the mobile devices are connected to the same access point/hotspot (through the same access point IP address) to identify devices in the same vicinity-based community and thereby provide the features above.

a) "with a computer system, determining an association between device identifiers of two or more Internet- accessing electronic devices based on electronically stored association-detection information about a plurality of Internet-accessing electronic devices, wherein the stored association-detection information for each of the plurality of Internet-accessing electronic devices includes: (i) a device identifier; (ii) at least one dynamically assigned IP address assigned to a modem that connects a router of the LAN to the Internet; and at least one timestamp specifying a time when the Internet-accessing electronic device accessed the Internet via the router of the LAN;"

For convenience of the Board, the following table summarizes how Petitioner has mapped the disclosures of the prior art to the limitations of claim 1(a):

Limitation from Claim 1(a)	Summary of Prior Art Disclosures
"a computer system"	At least one content server in Baig
"two or more Internet-accessing electronic devices"	Two or more mobile devices **102** in Baig, which are connected to and accessing at least one content server over the Internet
"determining an association between device identifiers"	Determining whether the two or more mobile devices **102** are logged in and connected to the content sever using an access point/hotspot having the same IP address
"electronically stored association detection information"	Information stored by the content server for each mobile device **102**, such as a session table under the combination with Laidlaw, that includes at least the information specified in claims 1(a)(i)-(iii) (*see* below)
"a device identifier" (1(a)(i))	A cookie containing a session token used to identify a mobile device **102** that is logged into the content server, under the combination with Laidlaw
"at least one dynamically assigned IP address assigned to a modem that connects a router of the LAN to the Internet" (1(a)(ii))	The IP address of access point **106** (which includes router **108**) used by the mobile device **102** to log into the content server over the Internet. The IP address would have been dynamically assigned via DHCP based on the combination with Sitaraman
"at least one timestamp specifying a time when the Internet-accessing electronic device accessed the Internet via the router of the LAN" (1(a)(iii))	Information specifying the last time that the mobile device **102** accessed the content server via access point **106** over the Internet, based on the combination with Laidlaw

(Schmandt, ¶81.) Petitioner will discuss these disclosures in more detail below.

As explained above, a content server ("**a computer system**") determines whether two mobile devices **102** ("**two or more Internet-accessing electronic devices**") are connected to the same hotspot **110**, and thus, to a common LAN. The content server thus performs the step of "**determining an association between device identifiers of two or more Internet-accessing electronic devices**," when it detects that the two mobile devices are both logged-in and connected to the content server via the same access point IP address. (Baig, ¶0056 & Fig. 3 (Step **306**); Provisional, 0013; Schmandt, ¶¶76-77, 84.) As explained in detail for claim 1(a)(i) below, each mobile device under the proposed combination would have had a "**device identifier**" in the form of a cookie, which is electronically stored by the content server and used to identify the mobile device as currently logged-in. (Schmandt, ¶¶83, 87-92; Laidlaw, ¶¶0006, 0016.)

Under the proposed combination, therefore, identifying two mobile devices **102** that are logged on and connected using the same access point/hotspot discloses "**determining an association between**" their respective device identifiers, under at least two separate theories. First, the claimed association is determined because each device identifier corresponds to a mobile device that is part of the same vicinity-based community and connected via the same access point IP address. (Baig, ¶¶0056

("At step **306**, the server **224** identifies all the users who have logged in from a common hot spot as having the same access point IP address."), 0040 ("Once the end-users at a particular access point log into the website of the VCSP, they are able to view other members of the VCSP who have also logged in from the same access point associated with a particular wireless hotspot."); Provisional, 0013, 0010, 0017.) Second and relatedly, the content server under the proposed combination "**determin**[es] **an association**" between the "**device identifiers**" because it uses the cookie assigned to each device to identify the device as being logged into the server, in order to place it into a vicinity-based community. (Baig, ¶0056 ("At step **306**, the server **224** identifies all the users who have logged in…."), 0059 ("In particular, when a user at a hotspot logs into the website of the VCSP **202**, the user automatically becomes part of the vicinity-based user group."), 0076 ("The web page **600** also displays a list **606** of other users at the present hotspot **110**. In one embodiment, the list includes the user names associated with users that have logged into the VCSP website."), Baig Provisional, 0013-0014, 0018.) The content server under the proposed combination thus determines "**an association**" between device identifiers based on both the IP addresses of the devices (which are used to determine if they are connected via the same access point IP address) and their cookies (which are used to determine if they are currently logged-in), in order to place them into a group of devices in a vicinity-based community. (Schmandt, ¶84.)

Baig further discloses and renders obvious that the determining step is "**based on electronically stored association-detection information about a plurality of Internet-accessing electronic devices**," which includes the information recited in subparts (i) through (iii) of claim 1(a). Petitioner will address this next.

(i) "a device identifier;"

Based on the combination of Baig and **Laidlaw**, each mobile device **102** under would have had a "**device identifier**" corresponding to a cookie stored by the content server (as part of the "**electronically stored association-detection information**"), which would have been used by the content server to identify the mobile device as having logged in. Laidlaw discloses a system for managing "sessions" in a network-based computer system. (Schmandt, ¶88; Laidlaw, ¶0003-0005.) One of the key concepts disclosed in Laidlaw is a session "token," which is included in each request from a client device to a server, and which identifies the requesting device. (Laidlaw, ¶0004.) In the context of the Internet and Web, Laidlaw explains that the session token takes the form of a cookie:

> A cookie is a sequence of binary information that a web server may send to a client system, and which the client system sends back to the web server with each subsequent request… A web application may inspect the value of cookies, and search for cookies that it previously issued in order to determine that a given web request is from a user who had previously been sent a cookie.

(Laidlaw, ¶0006.) The term "cookie" refers to a well-known and industry standard technology developed in the 1990s. (Schmandt, ¶90.) A cookie is stored as a file on the user's device by the web browser, and can be subsequently used by a web site to identify the user's device when it visits the web site. (*Id.*, *see also* **EX1011**, p.0026.) Cookies were (and remain today) in widespread use. (Schmandt, ¶90.) Under the proposed Baig-Laidlaw combination, the "**stored association- detection information**" would have included information stored by the content server in Baig to keep track of users who are currently logged in. (Schmandt, ¶91; Laidlaw, ¶0016 ("When the user authenticates at a login screen, the session token is placed into a cookie.").) Laidlaw describes a structure called a "session table," known to skilled artisans, that stores a variety of information for each session for a device. (Schmandt, ¶91 (citing Laidlaw, ¶¶0016-0031).) One of the key pieces of information in the session table is the session token, which stores the cookie information described above. As explained in Laidlaw:

> When the user authenticates at a login screen, <u>the session token is placed into a cookie</u>. When a subsequent request is received from the same client system, the session token is extracted from the cookie, <u>and the token is obtained from a session table that is keyed by session token</u>.

(Laidlaw, ¶0016.) In plain English, the process above attempts to determine, in response to receiving a cookie from the requesting device, after the user has logged

in using its device, whether the session token in the cookie is stored in the session table. (Schmandt, ¶92.) Laidlaw explains that the session token can include a sequence of encrypted data that uniquely identifies a session and includes, among other things, random data. (Laidlaw, ¶0032.)

It would have been obvious that the session token in the cookie ("**a device identifier**") would have been electronically stored in the session table. Indeed, the session table is "keyed by session token" (*id.*), meaning that the session token provided by the client is used to locate the other information in the table relating to the same client session (which thus further confirms the session token is stored in the table). (Schmandt, ¶92; Laidlaw, ¶¶0016 (session table "is keyed by session token"), 0039 (describing "key fields").)

Petitioner notes that mapping the session token/cookie to the claimed "**device identifier**" is consistent with the '878 patent. Dependent claim 8, addressed below, makes clear that the "**device identifier**" of claim 1(a)(i) may be "**a cookie readable by the computer system**." The cookie under the proposed Baig-Laidlaw combination provides a device identifier because it contains a session token uniquely identifying the session assigned to mobile device **102** that was used to log in and access the content server. (Schmandt, ¶93; Laidlaw, ¶¶0016, 0032.)

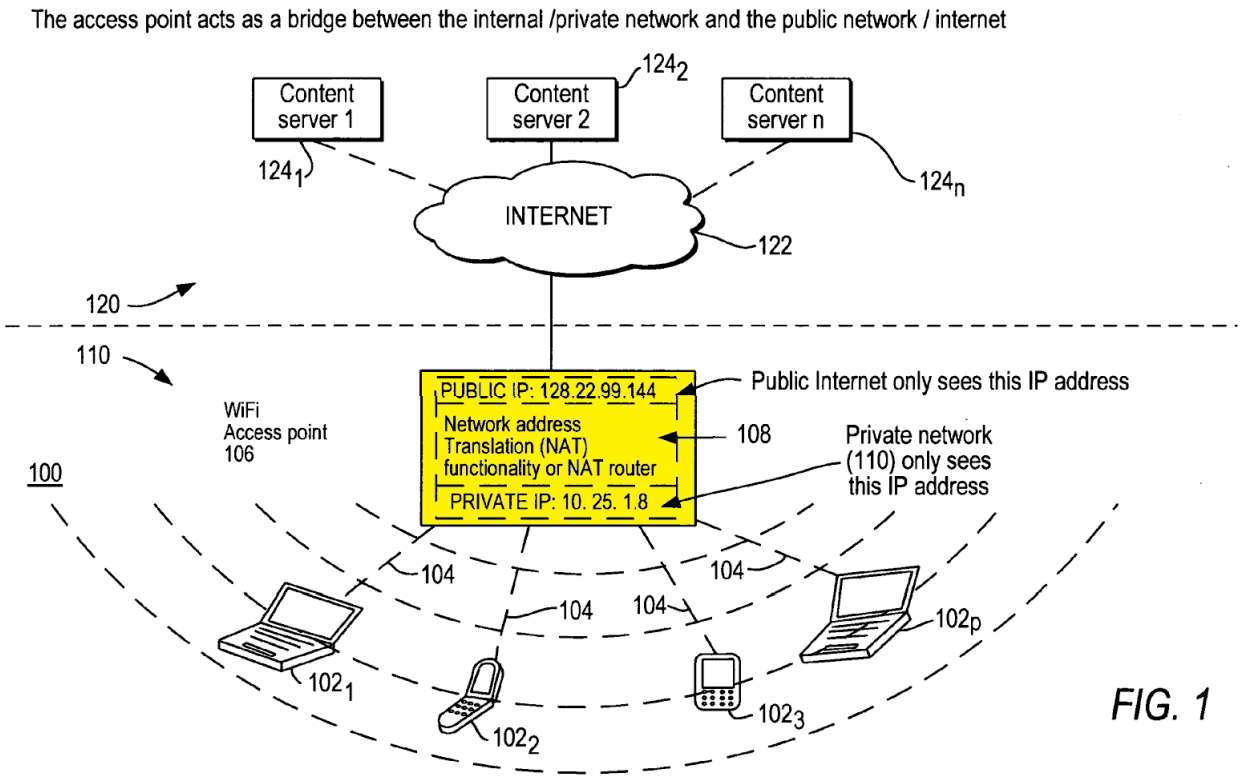
Petitioner will provide a full explanation of the <u>rationale and motivation to combine</u> Baig and Laidlaw after claim 1(a)(iii) below. (Schmandt, ¶¶103-109.)

(ii) "at least one dynamically assigned IP address assigned to a modem that connects a router of the LAN to the Internet; and"

The session table in Laidlaw also stores "information regarding the host that the user logged in from (e.g., the IP address)." (Laidlaw, ¶0022.) Under the proposed Baig-Laidlaw combination, therefore, the claimed electronically stored information would also have included the IP address of the access point **106** used to log into the content server. (Schmandt, ¶94.)

Apart from Laidlaw, it would have been obvious based on Baig alone that the electronically stored information would have included the IP address of the access point **106**. This is because Baig maintains a list of users whose devices are connected to the same hotspot using the same access point IP address. (Baig, *e.g.*, ¶0038; Provisional, 0010.) The content server can thus "identify users that are originating from a particular access point **106** and then group[] those users having a common IP address to the same hotspot **110**." (Baig, ¶0052; Provisional, 0012-0013.) It would have been obvious that, in order for the content server in Baig to perform this function, the server would have stored the mobile device IP addresses in order be able to identify devices belonging to a group. (Schmandt, ¶96.)

The IP address for each mobile device **102** in Baig is also "**assigned to a modem that connects a router of the LAN to the Internet**." The claimed "**modem**" and "**router**" are included in access point **106**:



(Baig, Fig. 1 (highlighting added).) Baig explains that access point **106** includes "NAT router **108**," which "replaces the 'local' IP address with its own 'public' IP address, and forwards the packets to the destination device (e.g., content server) on the Internet or external network **120**." (Baig, ¶0046; Provisional, 0011.) NAT stands for Network Address Translation and is a common technique used by Internet routers. (Schmandt, ¶96.) NAT router **108** routes communications between mobile devices **102** and the Internet. (Baig, ¶¶0046-0047; Provisional, 0011-0012.) Access point **106** therefore includes "**a router of the LAN to the Internet**."

It would also have been obvious that the router is connected to a "**modem**,"

i.e., other device functionality of access point **106** for connecting to the Internet. (Schmandt, ¶97.) The '878 patent describes a modem as "a device that enables online access by a user as an interface between the online access provider's network transmission system and the user's computer or online user interface device." ('878, 3:11-14.) This is precisely what access point **106** in Baig does – it "relays data between the wireless mobile devices **102** connected to the wireless network **104** and the external or public network, such as the Internet **122**." (Baig, ¶0044; *see also id.*, ¶0046; Provisional, 0011.) It would have been obvious that access point **106** would have included a "**modem**," a basic electronic device used as an interface for sending and receiving signals over a communications channel such as the Internet, to perform this function. (Schmandt, ¶97.) It therefore would have been obvious that access point **106** would have included "**a modem that connects a router of the LAN to the Internet**." The IP address of access point **106**, therefore, would also have been assigned to the modem that communicates over the Internet. (Schmandt, ¶97.)

Petitioner notes that claim 1(a)(ii) specifies at least one "**dynamically assigned**" IP address. One embodiment in Baig states that WiFi access points may be static IP addresses. (Baig, *e.g.*, ¶¶0064 ("Since the IP addresses of WiFi hotspots are mostly static IP addresses…."), 0050; Provisional, 0015, 0012.) Petitioner will explain, in a separate discussion below, why it would have been obvious to allow an access point in Baig to be assigned a dynamic IP address.

(iii) "at least one timestamp specifying a time when the Internet-accessing electronic device accessed the Internet via the router of the LAN;"

The '878 patent does not define "**timestamp**," nor does the term appear outside the claims. But "timestamp" was generally understood as referring to a record of when a particular event occurred. (Schmandt, ¶100.) Laidlaw discloses that the session table includes a timestamp, *i.e.*, "information regarding the last time the session was accessed." (Laidlaw, ¶0017.) Under the proposed combination with Baig, therefore, the stored information would have included a "**timestamp**," *i.e.*, information indicating a time, "**when the Internet-accessing electronic device**," *i.e.*, when logged in mobile device **102**, "**accessed the Internet via the router of the LAN**," *i.e.*, accessed the Internet via access point **106** (and via NAT router **108**) to communicate with the content server. (Schmandt, ¶101.)

Although not required by the claim, it would have been obvious to store and use the timestamp for a variety of well-known purposes. For example, Laidlaw explains that a session can be terminated after a period of inactivity. (Laidlaw, ¶¶0005, 0030 (session table includes field for "max inactivity time allowed").) It would have been obvious to use the timestamp, under the proposed combination, to determine whether a mobile device should be timed out (and logged out) if it fails to access the content server within a specified period of time. (Schmandt, ¶102.)

Rationale and motivation to combine (Baig and Laidlaw): It would have

been obvious to combine Baig with Laidlaw, predictably resulting in the system of Baig in which the content server included "**electronically stored association detection information**," such as a session table that stores, for each logged in mobile device **102**, the information specified in claims 1(a)(i)-(iii) discussed above. (Schmandt, ¶103.) It would also have been obvious to use this stored information to "**determine**[e] **an association between device identifiers**" of two or more mobile devices **102**, as described below. Baig and Laidlaw are analogous references in the same field of the '878 patent of facilitating online access through computer networks, and would have been reasonably pertinent to problems facing the inventor such as how to keep track of connected devices. (Schmandt, ¶104.)

A skilled artisan would have been motivated to combine Baig and Laidlaw in the manner discussed above. (Schmandt, ¶¶105-109.) Laidlaw confirms that session management was a common technique for keeping track of devices connected over the Internet. (Laidlaw, ¶¶0002-0006.) A skilled artisan would have been motivated to consult Laidlaw because – to even make the system of Baig function – the system would have needed to store session information about mobile devices to (at a minimum) keep track of currently logged in devices. (Schmandt, ¶105.)

A skilled artisan would also have been motivated to adapt the content server to store and use each of the pieces of session information in Laidlaw mapped to claims 1(a)(i)-(iii) above. With respect to claim 1(a)(i) ("**device identifier**"), it

would have been obvious to store a session token/cookie to enable the content server to determine that the mobile device **102** is currently logged-in. (Laidlaw, ¶0016 ("When the user authenticates at a login screen, the session token is placed into a cookie.").) Baig itself expressly suggests storing a cookie by disclosing the ability of the server to "remember" the user name and password of a user – a textbook use case for cookies well-known to skilled artisans. (Baig, ¶0068 ("A check field **408** is provided for optionally <u>remembering the user name and user password</u>."); Provisional, 0016; *see also* **EX1011**, p.0028 ("When the user returns to that site, the server will automatically check <u>the cookie it gave to that user to determine his or her name and password</u>.").) Cookies also represented an industry-standard and widely-used technique for keeping track of the identity of logged-on devices in web-based systems. (Schmandt, ¶106.) Cookies also represented one of a small number of known techniques for web-based session management, and were regarded as superior in many ways to the two other alternatives (*i.e.*, "hidden form fields" and "URL mangling") identified in Laidlaw. (Schmandt, ¶107 (citing Laidlaw, ¶0006).)

Under the proposed combination, the content server would have stored a session token/cookie for each mobile device after log-in, and then used the session token/cookie to identify the mobile device **102** and place it into a vicinity-based community. It thus would also have been obvious to "**determin**[e] **an association between device identifiers**" of the two mobile devices, under the proposed

combination, based at least in part on the session token/cookie. (Schmandt, ¶106; *see also* Baig, ¶0056 ("At step **306**, the server **224** identifies all the users who have logged in from a common hot spot as having the same access point IP address."), 0059 ("In particular, when a user at a hotspot logs into the website of the VCSP **202**, the user automatically becomes part of the vicinity-based user group."), 0076 ("The web page **600** also displays a list **606** of other users at the present hotspot **110**. In one embodiment, the list includes the user names associated with users that have logged into the VCSP website."), Baig Provisional, 0013-0014, 0018.)

With respect to claim 1(a)(ii) ("**IP address**"), as explained, it would have been obvious to store the IP address of access point **106** used by mobile device **102** to access the content server. As explained above, Baig needs this information to identify and keep track of devices that are connected to the same hotspot via the same access point IP address. (Schmandt, ¶108.) It thus would also have been obvious – and in fact necessary – to "**determin**[e] **an association between device identifiers**" of mobile devices **102**, under the proposed combination, based at least in part on the IP address of access point/hotspot. (*Id.*) As noted, Petitioner will separately explain below why it would also have been obvious for this access point IP address to have been "**dynamically assigned**."

With respect to claim 1(a)(iii) ("**timestamp**"), as explained, a skilled artisan would have been motivated to include and use the claimed timestamp, in this case

the time when mobile device **102** last accessed the content server via the Internet, in order to determine if the device is logged in (also using the cookie), but should nevertheless be "timed out" due to inactivity. (Laidlaw, *e.g.*, ¶¶0005, 0017, 0030; Schmandt, ¶¶102, 109.) A skilled artisan would have been motivated to store and use the timestamp to facilitate this timeout feature, which would have increased both the security and efficiency of the system. (Schmandt, ¶109.) A skilled artisan would have also had a reasonable expectation of success and could have implemented the proposed combination using conventional techniques. (Schmandt, ¶¶102, 203-204.)

"Dynamic" IP Address

The term "IP address" generally refers to a unique address on the Internet where a device or other resource can be located. (Schmandt, ¶110.) IP addresses are commonly categorized as "static" or "dynamic." (Schmandt, ¶¶110-112.)

A static IP address, as its name indicates, is an address that is (as a practical matter) permanently assigned to a particular device or entity. (*Id.*; Sitaraman, EX1007, 4:10-13.) A dynamic IP address, on the other hand, is an address that is selected and assigned upon request to the device by a server. (Schmandt, ¶112.)

As noted, Baig discloses WiFi access points (such as access point **106**) that use static IP addresses. (Baig, *e.g.*, ¶0064 ("mostly static IP addresses"); Provisional, 0015.) Although Baig does not expressly disclose a "**dynamically assigned**" IP address for access point **106**, this would have been obvious in view of

Sitaraman (**EX1007**).

Sitaraman explains, as was well-known, that dynamic IP addresses are assigned by a Dynamic Host Configuration Protocol (DHCP) server, which is also admitted prior art in the '878 patent. (Schmandt, ¶112; Sitaraman, 3:31-51; '878, 4:7-12 (describing DHCP).) DHCP refers to an industry standard technique in which a device on a network (such as a client) can ask a DHCP server "to provide it with an IP address and configuration parameters. A DHCP server on the network that is authorized to configure this client will offer an IP address by sending a reply to the client." (Sitaraman, 3:34-40.)

DHCP servers are used, for example, by Internet Service Providers (ISPs) who typically maintain a "pool" of available IP addresses that can be dynamically assigned to clients upon request. (Sitaraman, 3:64-4:1, 6:63-66.) If the client accepts the offered IP address, "the chosen DHCP server sends an acknowledgement with the offered IP address having an associated 'lease' time," which can be renewed by the client upon request. (Sitaraman, 3:42-47.) "Once the lease expires, the IP address can be 'recycled' and given to another machine." (Sitaraman, 3:49-51.)

Rationale and Motivation to Combine (Baig and Laidlaw with Sitaraman): It would have been obvious to combine Baig and Laidlaw with Sitaraman, predictably resulting in the Baig-Laidlaw system described above with the further ability of access point **106** to have a "**dynamically assigned**" IP address, for

example using known DHCP techniques. Under the proposed combination, therefore, the IP address of access point **106** (which includes the router and modem) would have been dynamically assigned by a DHCP server, and thus, the "**stored association-detection information**" for each mobile device **102** would have also included "**at least one <u>dynamically</u> assigned IP address assigned to a modem that connects a router of the LAN to the Internet**." (Schmandt, ¶114.) Sitaraman is an analogous reference in the field of communication over the Internet, and would have been reasonably pertinent to problems facing the inventor including understanding DHCP and dynamic IP address assignment. (Schmandt, ¶115.)

A skilled artisan would have had many reasons to combine. Petitioner notes, at the outset, that operation of the system of Baig does not depend on access points only having static IP addresses. (Schmandt, ¶116.) Baig merely relies on the IP address to identify devices that accessed the content server from the same hot spot via the same access point IP address. (Baig, *e.g.*, ¶0056 & Fig. 3 (Step **306**), Provisional, 0013.) This functionality would have operated in the same manner regardless of whether the access point had a statically or dynamically assigned IP address. (Schmandt, ¶116.)

Dynamic IP addresses also had many known advantages over static addresses that would have been applicable to the Baig-Laidlaw system. First, dynamic IP address assignment makes more efficient use of available IP addresses because

dynamic addresses can be temporarily used (leased) by devices while they are needed, and then recycled for reuse by other devices. (Schmandt, ¶117.) Sitaraman expressly acknowledges this motivation by explaining that Internet Service Providers (ISPs) "are faced with an increasing shortage of IP addresses," and that DHCP was developed in part "to help solve the shortage of IP addresses." (Sitaraman, 3:25-33.) Second, dynamic IP addresses offer cost savings over static IP addresses, which typically require payment of a fee to maintain the permanent address. (Schmandt, ¶118.) Third, it was also well-known that systems that use static IP addresses could be more susceptible to attacks by malicious parties than systems using dynamic IP addresses. (*Id.*)

A skilled artisan would have also been motivated to use dynamic IP addresses to increase the size and reach of Baig's vicinity-based network system. Because of the cost and other considerations above, many WiFi hotspots may have had dynamic instead of static IP addresses. (Schmandt, ¶119.) The system of Baig would have benefitted by also allowing hotspots with dynamic IP addresses, as this would have increased the number of hotspots the system could support thereby expanding the potential audience (of both hotspots and thus users). (Schmandt, ¶119.) This would have furthered the objective in Baig to use hotspots "to form a mesh network of WiFi hotspots, which are geographically spread, for example, over an entire metropolitan area, a state or the country." (Baig, ¶0065; Baig Provisional, 0016.)

Finally, Petitioner notes that, in one embodiment in Baig, a static IP address of access point **106** may be used to correlate a particular hotspot with a physical address. (Baig, ¶0064; Provisional, 0016.) This allows a user to provide a physical address of the hotspot (such as a street address), which the server can store in a database in association with the static IP address. (*Id.*) But this functionality would have remained available even if access point **106** had a dynamic IP address; the only difference would be that a user may have to occasionally reenter the physical address when a different dynamic IP address is assigned. (Schmandt, ¶120.) This would have amounted, at best, to a minor inconvenience heavily outweighed by the significant advantages of allowing dynamic IP addresses detailed above. This would have been infrequent for various reasons; for example a dynamic IP address could have been assigned to an access point for an extended period, and DHCP servers often reassign the same dynamic IP address to a device to which it was previously assigned. (*Id.*) A skilled artisan would have had a reasonable expectation of success in adapting the system to support dynamic IP addresses, as DHCP was within the general knowledge of skilled artisans. (Schmandt, ¶¶121, 204.)

(b) "wherein determining the association in part (a) is done by using the stored association-detection information to determine that the two or more Internet-accessing electronic devices have separately accessed the Internet through a router of the LAN during a predetermined period of time via a common IP address;"

Claim 1(b) was largely addressed in the above discussion. As explained, the

determining step of claim 1(a) is performed by using "**the stored association-detection information**," *i.e.*, the stored information (for example in a session table) under the proposed Baig-Laidlaw-Sitaraman combination.

Claim 1(b) does not appear to require "**using**" every piece of the stored information recited in claim 1(a)(i)-(iii) for the claimed determining step, but the prior art nevertheless satisfies any such requirement for the reasons stated for claim 1(a) above. It would have been obvious to use each piece of the stored association-detection information is used in carrying out the determining step under the proposed combination. (Schmandt, ¶¶106, 108-109, 122.)

Claim 1(b) further requires that the two or more devices "**have separately accessed the Internet through a router of the LAN… via a common IP address**," which is also satisfied by Baig. For example, as discussed above for Figure 1, each mobile device **102** connected to the local network in Baig has its own local or private IP address. (Baig, ¶0049, Fig. 2 ("1. Devices A, B, C, D & E will be allocated 'local' IP addresses, not visible to the outside world….."); Provisional, 0012, Fig. 2.) NAT router **108** within access point **106** uses these local IP addresses to route outgoing and incoming communications between each mobile device and the Internet, by replacing these local addresses with the public IP address of the access point **106** ("**a common IP address**") when communicating with devices over the Internet. (Baig, ¶¶0045-0047, 0050-0051; Provisional, 0011-0012.)

Each mobile device **102** has also "**separately**" accessed the Internet because, as anyone who had used an IP-based local network would have appreciated, if one device were to log off or disconnect, another connected device could have continued to communicate using its separate local IP address. (Schmandt, ¶123.) This is consistent with Figure 1:

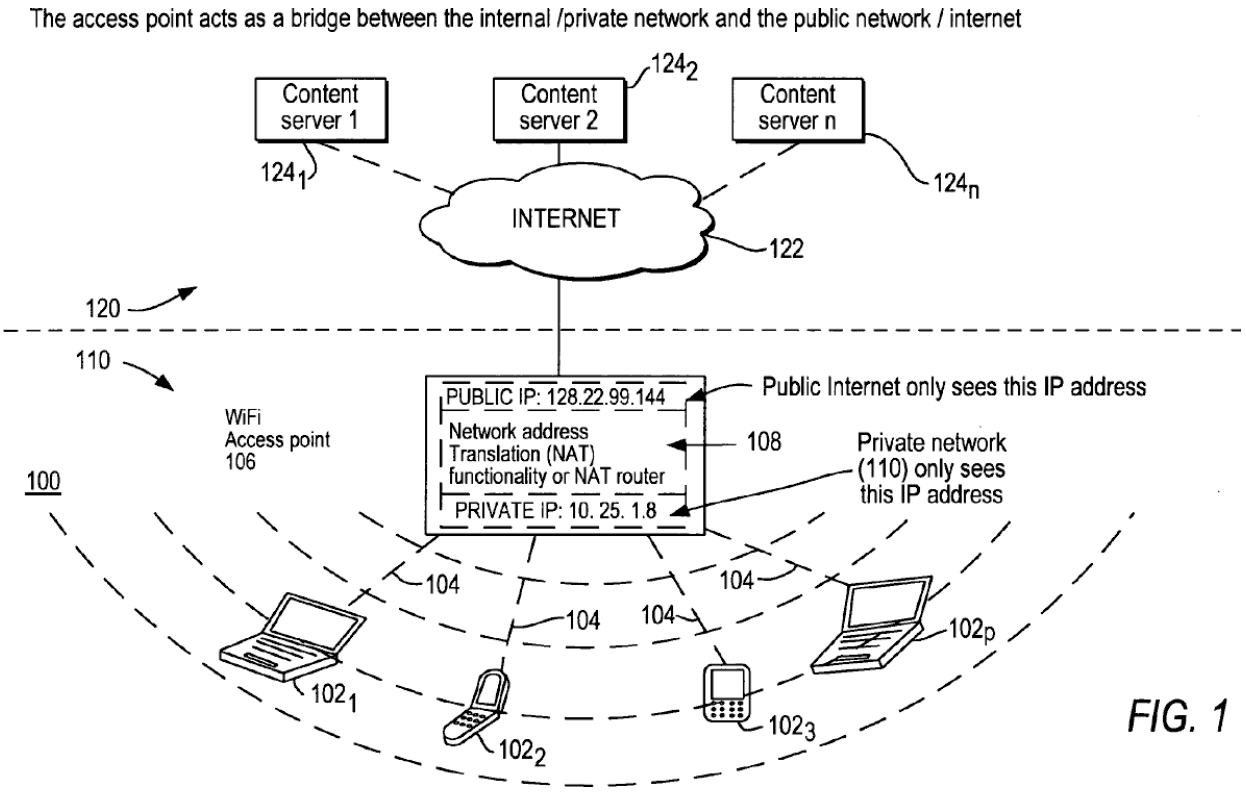


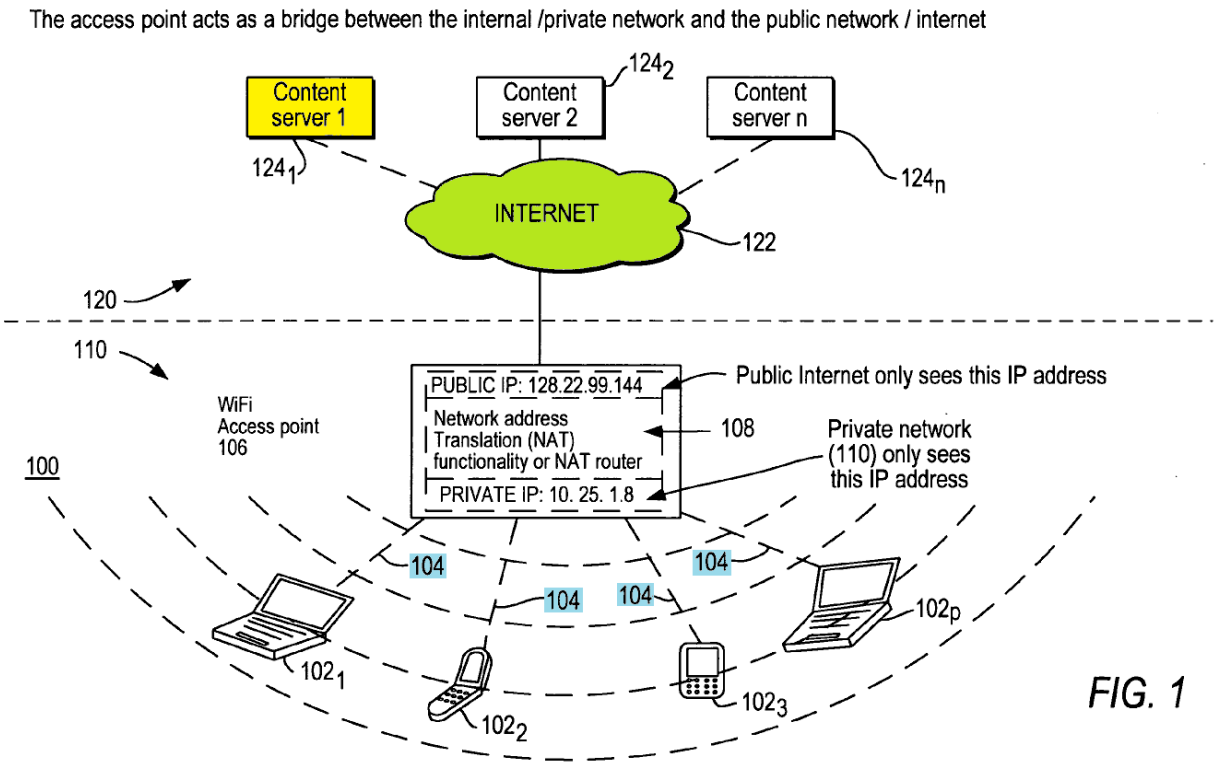
FIG. 1

(Baig, Fig. 1.) Figure 1 does not show any links, connections, or other dependencies between the mobile devices **102** connected to local network **104**. Each mobile device **102** instead depends only on access point **106** – and not on other mobile devices **102**– for its connection to the content server the Internet **122**. (Baig, ¶0043; Provisional, 0011.) This is further confirmed by the fact that, as Baig confirms,

mobile devices need not be connected to the content server at the same time. (Schmandt, ¶¶123-124; Baig, Fig. 3; Baig, ¶¶0055-0056; Provisional, 0013.) Finally, each mobile device has also separately accessed the Internet "**during a predetermined period of time via a common IP address**." This is because, as explained for claim 1(a) above, the IP address of the access point **106** would have been a dynamically assigned IP address with a DHCP "lease" time during which the address remains valid. (Sitaraman, 3:42-51.) "Once the lease expires, the IP address can be 'recycled' and given to another machine." (Sitaraman, 3:49-51.) Mobile devices **102** would thus have accessed the Internet via access point **106** during "**a predetermined period of time via a common IP address**," *i.e.*, during the lease time that the dynamic IP address assigned to access point **106** remains valid. (Schmandt, ¶125.) This period "**predetermined**" because the lease time was provided by the DHCP server when it assigned the dynamic IP address to access point **106**, which would have been before mobile devices logged into the content server using that access point. (Schmandt, ¶126.) This mapping of DHCP lease times to the claimed "**predetermined period of time**" is entirely consistent with the '878 patent, which expressly references DHCP expiry times in describing the claimed predetermined time period. ('878, 4:22-26.)

(c) "wherein the computer system determining the association in part (a) is outside the LAN and is connected to the LAN through the Internet; and"

Baig also satisfies this limitation, as confirmed using Figure 1 of Baig:



(Baig, Fig. 1 (highlighting added).) As discussed, Figure 1 shows that the content server ("**the computer system determining the association in part (a)**"), one of which is shown in yellow above, is connected to local network **104** ("**the LAN**") via the Internet **122** and access point **106**. But Figure 1 and Baig also confirm that the content server sits outside the local network **104**. As Baig explains: "[T]he mobile devices **102** form a 'local network' **104** with the access point **106**, while everything outside of (i.e., external to) the hotspot **110**, i.e., all servers & computers residing on the public Internet, is considered the 'public' network **120**." (Baig, ¶0043;

Provisional, 0011.) Baig therefore discloses that "**the computer system determining the association in part (a) is outside the LAN and is connected to the LAN through the Internet**." (Schmandt, ¶127.)

(d) "with the computer system, using the association determined in part (a) to utilize user profile information associated with the device identifier of a first of the associated Internet-accessing electronic devices, and comprising behavioral or demographic data collected via the first of the associated Internet-accessing electronic devices, to take an automatic action with respect to a second of the associated Internet-accessing electronic devices using the device identifier of the second of the associated Internet-accessing electronic devices."

This final limitation of claim 1 is disclosed by Baig, in combination with **Hahn**. As explained, after a mobile device **102** in Baig logs into the content server ("**a first of the associated Internet-accessing electronic devices**"), the content server ("**the computer system**") places the mobile device **102** in a vicinity-based group with other mobile devices connected to the same hotspot/access point. (Baig, *e.g.*, ¶¶0038, 0052; Provisional, 0010, 0012-0013.) As explained below, this in turn results in a transmission of information to the second mobile device.

As mentioned, after a user logs in, the server presents webpage **600**:

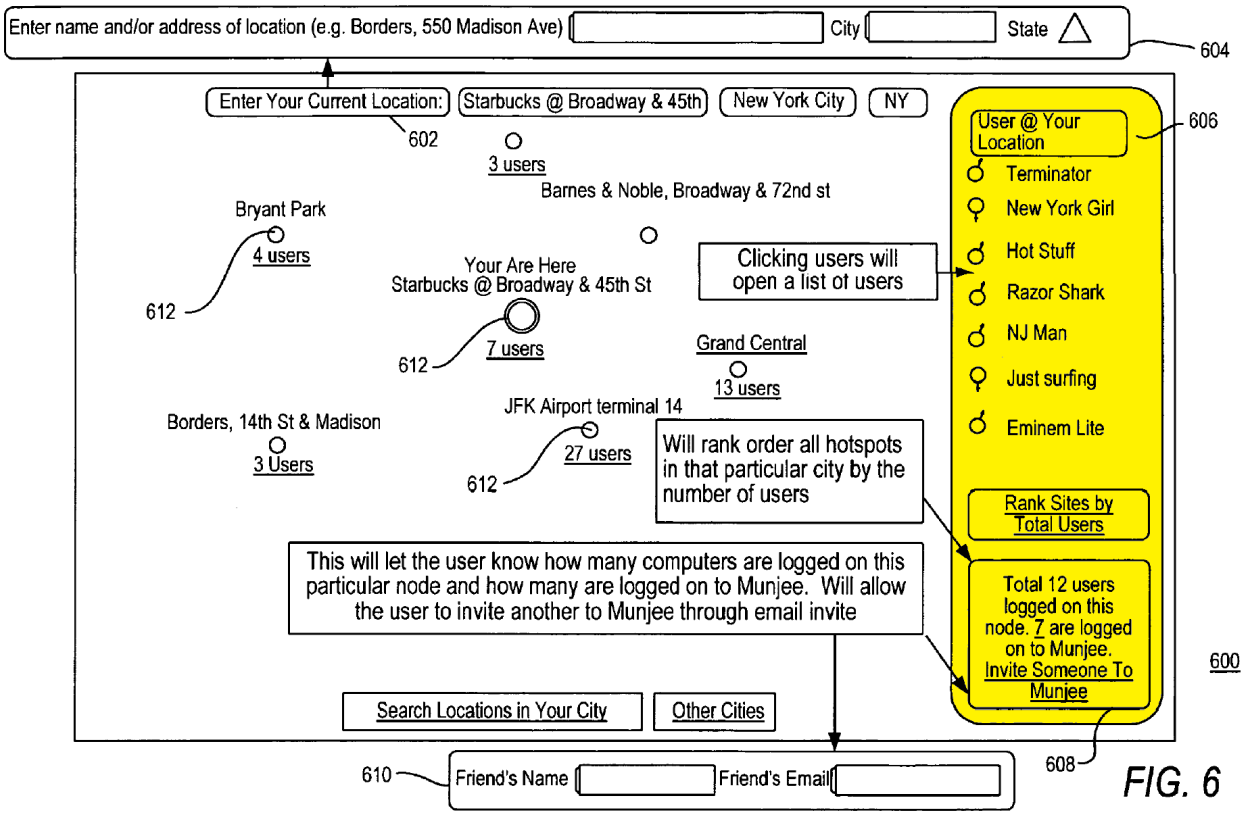
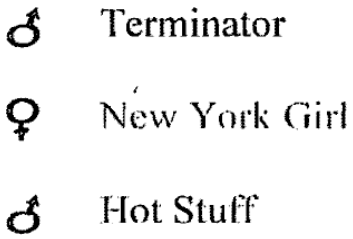


FIG. 6

(Baig, Fig. 6 (highlighting added); Baig, ¶0074; Provisional, 0017.) The key part of webpage **600** is list **606**, which "displays a list **606** of other users at the present hotspot **110**." (Baig, ¶0076, Provisional, 0018.) As shown, the list includes the names of seven other users whose devices are logged-on (*e.g.* "Terminator," "New York Girl"), and further shows, for each name, either a male or female gender symbol. The gender symbols are clear from Figure 6 above, but the version of Figure 6 in the incorporated-by-reference provisional (shown in part at right) shows them more clearly. (Baig Provisional, Fig. 6.) List **606** also appears in Figure 7 of Baig, which shows a webpage that allows users to engage in chat conversations with other



users. (Baig, Fig. 7 & ¶0080; Provisional, 0019.)

The transmission and display of list **606** discloses and renders obvious claim 1(d) because it discloses "**with the computer system**," *i.e.*, with the content server, "**using the association determined in part (a)**," *i.e.*, using the fact that the first and second mobile devices (identified by their respective device identifiers) are logged in and also connected to the same hotspot/access point using the same access point IP address, **"tak**[ing] **an automatic action with respect to a second of the associated Internet-accessing electronic devices**," *i.e.*, sending list **606** as part of a webpage to the second mobile device over the Internet.

Consider a concrete example. Suppose the user "Terminator" in Figure 6 connected and logged-in using his mobile device (**the first device**), and at that time, another user "New York Girl" was already connected and logged-in and currently viewing the webpage of Figure 6 or Figure 7 on her mobile device (**the second device**), with both users connected via the same access point as discussed. In this scenario, after "Terminator" logged in, the content server would have sent the webpage to the second device of "New York Girl" including list **606**, showing that "Terminator" was now part of the vicinity-based group. This would have resulted in an "**action with respect to a second of the associated Internet-accessing electronic devices**," because the second device would have received and displayed "Terminator" on list **606** when displaying the webpage shown in Figure 6 or 7.

(Baig, ¶¶0076 ("The web page **600** also displays list **606** of other users at the present hotspot **110**."), 0080 (same, Fig. 7); Provisional, 0018-0019.)

Petitioner notes that the claim further requires taking "**automatic**" action, and Baig is unclear as to when or how list **606** in Figure 6 gets updated or refreshed on the second device when "Terminator" joins using the same access point/hotspot. For this reason, Petitioner has relied on Baig in further combination with **Hahn** for the "**automatic**" issue, which will be the subject of a separate discussion below.

Turning back to Baig, the action taken with respect to the second device was also the result of "**utiliz**[ing] **user profile information associated with the device identifier of a first of the associated Internet-accessing electronic devices and comprising behavioral or demographic data collected via the first of the associated Internet-accessing electronic devices**." This is because, as explained above, list **606** transmitted to and displayed on the second device identifies the gender of the other logged-in users. For "Terminator" who is logged in using the first device using our example above, list **606** includes a gender symbol ("♂") indicating that he is male. The transmission and display of list **606** to the second device is thus the result of "**utilizing user profile information**," because it includes gender information of "Terminator," who has connected using his first device that is logged into the content server and part of the same vicinity-based network as "New York Girl" ("**associated with the device identifier of a first of the associated**

Internet-accessing electronic devices"). The mapping of gender information to "**profile data**" is consistent with the '878 patent, which broadly describes profile data as including "demographic or behavioral information," such as information "concerning the user's characteristics or activities." ('878, 6:7-12.)

The gender of "Terminator" clearly qualifies as user profile information including at least "**demographic data**" that was "**collected**" via the first device. (Baig, ¶¶0093 ("As users register online on the VCSP website, profile information about our users, such as age, gender, occupation, interests and the like are requested during the registration process and securely stored by the VCSP **202**."), 0096, 0070 & Fig. 5 (explaining that new user registration form includes "Gender" field **508** to collect gender information); Provisional, 0022, 0017.)

Although not required by claim 1(d), the transmission and display of list **606** in Baig was also the result of utilizing "**behavioral**" data collected via the first device. The '878 describes "**behavioral**" information as including any of a wide variety of previous action by the user/subscriber, including "any other form of previous subscriber activity." ('878, 4:49-57.)

Baig discloses behavioral data in the form of action by the user indicating that they wish to be visible to other users. (Baig, *e.g.*, ¶¶0081 ("A link **720** can also be provided to remove [the user's] concealment (i.e. invisibility) to other users."), 0124 ("All users who are logged on can see the other users in the chat-room, unless a user

options out from being visible to other users."); Provisional, 0019, 0027.) The transmission and display of list **606** is thus the result of utilizing profile information including "**behavioral information**," because list **606** transmitted to the second device includes "Terminator" if he took action allowing himself to be visible to other users. (Schmandt, ¶136.) In other words, the fact that "Terminator" appeared in list **606** sent to the second device is the result of behavioral information collected via his first mobile device when he decided to make himself visible to other users.

Finally, Baig discloses taking the claimed action "**using the device identifier of the second of the associated Internet-accessing electronic devices**," under at least two separate theories. First, at the time the webpage including list **606** is transmitted to and displayed on the mobile device of the viewing user (**the second device**), the second device has logged into the content server using its device identifier, *i.e.*, the session token in a cookie as explained in claim 1(a)(i). (Schmandt, ¶¶88-92, 106-107.) As explained for claim 1(a)-(b), this cookie allows the content server to identify the mobile device as being logged in – a prerequisite to display of the webpages in Figures 6 and 7 that include list **606**. (Schmandt, ¶122; Baig, ¶0073; Provisional, 0017.) Because logging into the content server is a necessary prerequisite – and direct cause – of the transmission of list **606** to the second device for display (the "**action**"), the transmission occurred "**using**" at least the cookie assigned to the second device.

Second, as explained for claim 1(a)(i), the "**device identifier**" cookie under the proposed combination is also used as a "key" to locate information in the session table pertaining to the second device. (Laidlaw, ¶0016; Schmandt, ¶92.) That session table, as explained, further includes the IP address of the access point used by the second device to connect to the content server – a piece of information the content server obviously needs in order to send list **606** to the second device over the Internet. (Schmandt, ¶¶95-96, 108.) This provides a further basis for showing that the claimed action is taken "**using the device identifier**" of the second device.

"Take an <u>Automatic</u> Action"

As mentioned, it is unclear if Baig discloses taking "**<u>automatic</u> action**." For example, consider again the scenario of **(a)** the second device belonging to "New York Girl" who is already connected to the access point and viewing list **606** on the webpage, and **(b)** at some point later, another user "Terminator" at the first device connects at the same access point and logs in. It would have been obvious that list **606** shown to "New York Girl" on her second device would have to be updated at some point to display "Terminator" (assuming he chose to make himself visible). (Schmandt, ¶138.) But it is unclear from Baig how updates are triggered.

It would have been obvious to implement Baig such that list **606** gets automatically updated, for example by the server automatically sending an updated or refreshed version of the webpage when users are added to the access point vicinity

group. This is confirmed by **Hahn** (**EX1008**), which describes well-known features for automatically updating webpages:

> **Updating Information Automatically**
>
> Once you tell your web browser to load a web page, you must wait for the information be sent from the web server to your computer… Nevertheless, there are times in which it is desirable to display information which can be updated automatically. There are two ways which this can be done.

(Hahn, p.0048 (bold in original).) Hahn goes on to describe these "two ways." The first technique, "CLIENT PULL," involves the web browser automatically requesting that the page be reloaded at periodic intervals, for example every 30 seconds. (*Id*.) With the second technique, "SERVER PUSH," the server automatically sends new data without the browser making a request. (*Id*.) Both techniques independently qualify as "**automatic**," as they occur without requiring user action. (Schmandt, ¶¶141-142.)

Manner, Rationale, and Motivation to Combine (Baig with Laidlaw and Sitaraman): It would have been obvious to adapt the automatic update techniques of Hahn to the Baig-Laidlaw-Sitaraman combination, predictably resulting in the content server automatically sending an updated or refreshed version of the webpage shown in Figure 6 and Figure 7 –with an updated list **606** – to the second device for

display. (Schmandt, ¶143.) Building on the scenario described above, when "Terminator" connects to the access point and logs into the website using his first device, under the proposed combination, the content server would have automatically sent an updated webpage with an updated list **606** to the second device of "New York Girl" for display. (Schmandt, ¶144.) Hahn is an analogous reference in the same field of providing online access to information such as websites over the Internet, and would have been reasonably pertinent to problems facing the inventors, including how to take automatic action such as transmitting information after determining that two devices are connected to the same network. (Schmandt, ¶145.)

A skilled artisan would also have been motivated to combine. Hahn provides an express motivation by explaining that "there are times when it is desirable to display information which can be updated automatically," and further explains the CLIENT PULL and SERVER PUSH techniques "are useful in situations where you are looking at data that changes." (Hahn, p.0048.) This would have provided a clear benefit to Baig given that membership in a vicinity group (and thus the content of list **606**) would have frequently changed. (Schmandt, ¶146; Baig, *e.g.*, ¶¶0039, 0078; Provisional, 0010, 0018.) A skilled artisan would have been motivated to incorporate the automatic techniques of Hahn so users would have up-to-date information about users in their vicinity group. (Schmandt, ¶¶146-147.)

Hahn provides a further motivation by explaining that automatic update is

suitable for "web-based talk facilities," in which users send messages back and forth with other users – which is similar to the chat feature of Baig. (Hahn, pp.0048-0049, 0070; Schmandt, ¶147.) A skilled artisan would have had more than a reasonable expectation of success and the proposed combination could have been implemented using conventional programming techniques. (Schmandt, ¶¶148, 205.)

2. Claim 2: "The method of claim 1 wherein the first device comprises a mobile device that is connected to the LAN only intermittently."

As explained for claim 1, each device connected to the LAN is a "**mobile device**." (Baig, ¶0042; Provisional, 0010-0011.) It would have been obvious that each mobile **102** device would have been "**connected to the LAN only intermittently**," because the access points/hotspot could have been located in places where users gather for short periods, such as coffee shops or airport terminals. (Baig, *e.g.*, ¶¶0039 (coffee shop), 0078 (airport terminal); Provisional, 0010, 0018; Schmandt, ¶149.) After a mobile device user leaves such a location – for example by moving to a location outside the range of the WiFi hotspot – they would no longer be "**connected to the LAN**." (Baig, ¶0052 (noting that "the range of wireless communications for any given hotspot is limited…"); Provisional, 0013.) That user, of course, could later return to that location and reconnect to the hotspot. It therefore would have been obvious that the first mobile device would have been "**connected to the LAN only intermittently**." (Schmandt, ¶¶149-150.)

3. Claim 8: "The method of claim 1 wherein the device identifier of at least one of the first device and the second device is a cookie readable by the computer system."

As fully explained for claim 1(a) above, the "**device identifier**" for the first and second mobile device **102**, based on the combination of Baig and Laidlaw, would have been a cookie that stores the session token provided to the mobile device **102** by the content server. (Schmandt, ¶¶89-92; Laidlaw, ¶¶0006, 0016.)

It would also have been obvious (and basic knowledge of a skilled artisan) that the cookie would have been "**readable by the computer system**," *i.e.*, by the content server of Baig under the proposed combination. (Schmandt, ¶151.) The whole purpose of a cookie, in fact, is to be subsequently passed back from a client device <u>to the server</u> so the server can read the cookie to identify and recognize the client device. (Laidlaw, *e.g.*, ¶0006; Schmandt, ¶151.)

4. Claim 9: "The method of claim 8 further comprising, using the computer system, automatically storing, in a memory in the first device, the cookie."

It would also have been obvious, and basic knowledge of a skilled artisan, that the cookie would have been "**stored, in a memory of the first device**." As Laidlaw explains, "[a] cookie is a sequence of binary information that a web server may <u>send to a client system</u>, and which the client system sends back to the web server with each subsequent request…." (Laidlaw, ¶0006.) It would have been obvious that a client system, such as mobile device **102**, would have stored the cookie in a memory

in order to later send it back to the web server with subsequent requests. (Schmandt, ¶152 (citing **EX1011**, p.0026).) It also would have been obvious that storage of the cookie in the memory of the first device would have occurred "**using the computer system**," *i.e.*, the content server, because the content server sends the cookie to the mobile device **102** for storage so it can be included in subsequent requests. (Schmandt, ¶152; Laidlaw, ¶0006.)

It would also have been obvious that the claimed cookie storage occurs "**automatically**." Nothing in Laidlaw suggests (let alone requires) user intervention in creation of the cookie or the transmission of the cookie to the client device for storage. (Schmandt, ¶153.) This is also consistent with the well-known behavior of cookies; storage of cookies is so automatic that users often had no idea that they even existed. (Schmandt, ¶154.)

Finally, the fact that cookie storage in the proposed combination may be preceded by user actions (such as logging in) does not make the claim storage any less automatic, because such user actions precede and are separate from the claimed cookie storage. (Schmandt, ¶154.) This is consistent with the '878 patent which likewise discloses storage of cookies in response to user actions. ('878, 6:49-54.)

5. Claim 10: "The method of claim 1 wherein the device identifiers of the first device and the second device include no personally identifiable information pertaining to a user of the first

device or the second device."

It would also have been obvious that the session token/cookie for the first and second mobile devices **102** ("**device identifiers**") would have included no personally identifiable information pertaining to either user. Laidlaw describes an exemplary session token that "contains three elements: random data, a UNIX time stamp, and an incremental token ID," which is concatenated together then encrypted. (Laidlaw, ¶0032.) The "token ID" is simply "an integer whose value increments by a predetermined amount every time the system generates a new ID." (*Id.*) None of this data includes any personally identifiable information pertaining to any user – it is in fact entirely independent of the user's characteristics. (Schmandt, ¶155.)

6. Independent Claim 13

Claim 13 is substantially similar to claim 1 except written as a computer system claim. (Schmandt, ¶156.) The computer system of claim 13 "**compris**[es] **at least one hardware server computer, wherein the computer system is programmed and connected to perform**" the same steps of claim 1.

The "**computer system**" in the proposed combination, as with claim 1, corresponds to a content server in Baig that includes "**at least one hardware server computer**," which is "**programmed and connected to perform**" the method steps of claim 13. The content server includes a processor, memory and support circuitry that stores and executes computer programs for connecting to access points and

carrying out the techniques disclosed in Baig. (Baig, *e.g.*, ¶¶0052-0053; Provisional, 0013.) The "**at least one hardware server**" under the proposed combination, would have been programmed to perform each step of claim 13. (Schmandt, ¶157.)

7. Claims 14 and 19

Dependent claims 14 and 19 are substantially similar to claims 2 and 10, respectively, except that they depend from claim 13. (Schmandt, ¶158.) They are obvious for the reasons previously stated.

8. Independent Claim 22

Claim 22 is substantially similar to claim 1 and claim 13 except that it is written as an "**article**" claim. (Schmandt, ¶160.) The article of claim 22 "**compri**[ses] **a tangible data storage medium… encoding computer-readable instructions that, when applied to a computer system comprising at least one hardware server computer, instruct the computer system to perform**" the same steps recited in claim 1.

As explained for claim 13, Baig discloses "**a computer system**" comprising "**at least one hardware server computer**," *i.e.*, a content server. (Schmandt, ¶¶157, 161.) The claimed "**article**" in Baig takes the form of memory included with the content server for storing computer programs for carrying out the techniques in Baig. (Baig, *e.g.*, ¶¶0052-0053; Provisional, 0012-0013; Schmandt, ¶161.) It would have been obvious that the programs in Baig would have included "**computer-readable**

instructions" that, under the proposed combination, would have been used to carry out each of the steps of claim 22. (Schmandt, ¶161.)

D. Ground 2: Claims 3-4, 15-16 Are Obvious Over Ground 1 Prior Art in Further View of Xu.

1. Claim 3: "The method of claim 2 wherein the user profile information associated with the device identifier utilized in part (d) comprises behavioral data collected via the first device at a time when the first device is not connected to the LAN."

The majority of the limitations in claim 3 were already addressed the analysis of claim 1(d) for **Ground 1**. As explained, under the proposed combination, "**the user profile information associated with the device identifier utilized in part (d) comprises behavioral data collected via the first device**," with the behavioral information corresponding to the first device user's decision to be visible to other users in a community. (Baig, ¶0081 ("A link **720** can also be provided to <u>remove their concealment (i.e., invisibility) to other users</u>."); Provisional, 0019.)

The key aspect of claim 3 that was not covered by the analysis of claim 1(d) was the last clause, in which the behavioral data would have been collected "**when the first device is not connected to the LAN**." But it would have been obvious to anyone who had used a public WiFi hotspot as of April 2007, or was familiar with WiFi generally, that mobile devices **102** in Baig could have been moved out of the range of a particular hotspot/access point, and into the range of another hotspot/access point. (Schmandt, ¶164; Baig, ¶0052 (noting that "the range

of wireless communications for any given hotspot is limited…"); Provisional, 0013).) Baig also confirms that use of hotspots had skyrocketed in bookstores, airports, and other places where people temporarily gather. (Baig, ¶0037; Provisional, 0009.) The following scenario would thus have been obvious and predictable:

(1) The first device user could have previously logged into the content server using a first access point/hotspot at a first location (*e.g.*, an airport). While connected at this first access point/hotspot, the user clicked link **720** to "remove their concealment (i.e., invisibility) to other users." (Baig, ¶0081; Provisional, 0019.) The content server would thus have "**collected**" the behavioral data while connected to the LAN created by this first access point/hotspot.

(2) Later, the first user moves to the current location and logs into the content server using the current access point/hotspot (*e.g.*, at a coffee shop). Because the first user has now connected using an access point/hotspot having a different IP address, it was thus connected to a different LAN ("**the LAN**"), from the one at step **(1)**. (Schmandt, ¶164.) When the content server then transmits list **606** to the **second** device, that list will include the first user because of the first user's action (clicking link **720**) at step **(1)** when the first device was connected to the previous LAN.

This scenario, which is a predictable and typical use of WiFi hotpots in the context of Baig, confirms that it would have been obvious for the "**behavioral data**" to have been "**collected via the first device at a time when the first device is <u>not</u> connected to <u>the</u> LAN**," *i.e.*, because the visibility selection was collected by the content server while the first device connected to the first earlier/different LAN created by the airport access point/hotspot. (Schmandt, ¶¶164-166.)

One final issue warrants further discussion. The scenario above assumes that the content server in Baig would have stored the first device user's visibility selection at point **(1)** so the selection would later be applicable when first device later logs in from the second access point/hotspot at point **(2)**. Baig explains that when users register, profile information is stored by the server. (Baig, ¶0094; Provisional, 0022.) But Baig does not indicate whether the user's visibility selection is stored. Nevertheless, storing the user's visibility selection between hotspot logins would have been obvious in view of **<u>Xu</u>**.

Xu discloses a system similar to Baig for creating virtual communities that allow users to share resources such as websites, software, chat channels, discussion threads, or any other type of resource. (Xu, 10:24-31, 11:41-46.) Xu discloses a similar feature of allowing users to be made aware of the presence of other users in a virtual community. (Xu, 19:32-36.) Like Baig, users in Xu choose whether or not they wish to be visible to other members of the community, and this information can

be persistently stored in a global user database. (Xu, 27:32-35, 26:5-7.) "User preferences such as privacy, security settings can also be stored there. For example, the system uses them to determine if the user should be anonymous or invisible to the rest of the community." (Xu, 26:13-15.)

Rationale and Motivation to Combine (Ground 1 Prior Art with Xu): It would have been obvious to adapt the content server in Baig to store the first device user's visibility setting, predictably resulting in the user's visibility preference being applicable when the first user logs out and later logs in to the content server from another hotspot. (Schmandt, ¶169.) Xu is an analogous reference in the same field of providing online access to information (such as websites) between multiple devices over the Internet, and would have been reasonably pertinent to problems facing the inventor. (Schmandt, ¶170.)

A skilled artisan would have been motivated to combine in order to give users greater control over their own privacy when interacting with other users via the content server. Storing the user's visibility preference would have obviated the need for the user to set the visibility setting each time they log in. As a further advantage as noted, a mobile device user in Baig could have logged into the VCSP multiple times through different hotspots/access points at different locations. It thus would have been beneficial for the content server to store (and thus be able to apply) the user's visibility preference from one login to the next, as Baig does for other stored

registration information. (Schmandt, ¶170.) A skilled artisan would have had a reasonable expectation of success and would have found the further combination with Xu trivially simple to implement. (Schmandt, ¶171.)

2. Claim 4: "The method of claim 3 wherein the behavioral data collected via the first device is received at the computer system as a result of redirection of the first device from an online site visited by the first device while the first device is not connected to the LAN."

Claim 4 would also have been obvious based on Baig, based on multiple different theories. Baig explains that, in order to access the content server, the user must first log on by entering a username and password into the VCSP website. (Baig, ¶0068; Provisional, 0016.) This is shown in Figure 4:

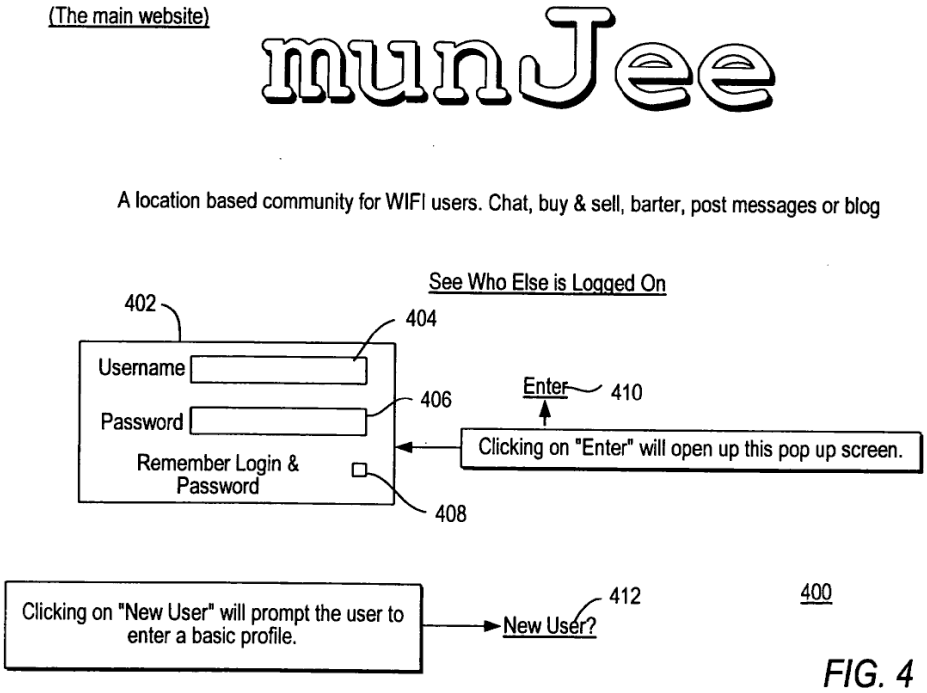


FIG. 4

(Baig, Fig. 4.) Home page 400 above allows the user to "log in for accessing the VCSP website and services." (Baig, ¶0068; Provisional, 0016.) Once the user

registers and then logs in, the content server presents the web page of FIG. 6, shown below. (Baig, ¶0074; Provisional, 0017.)

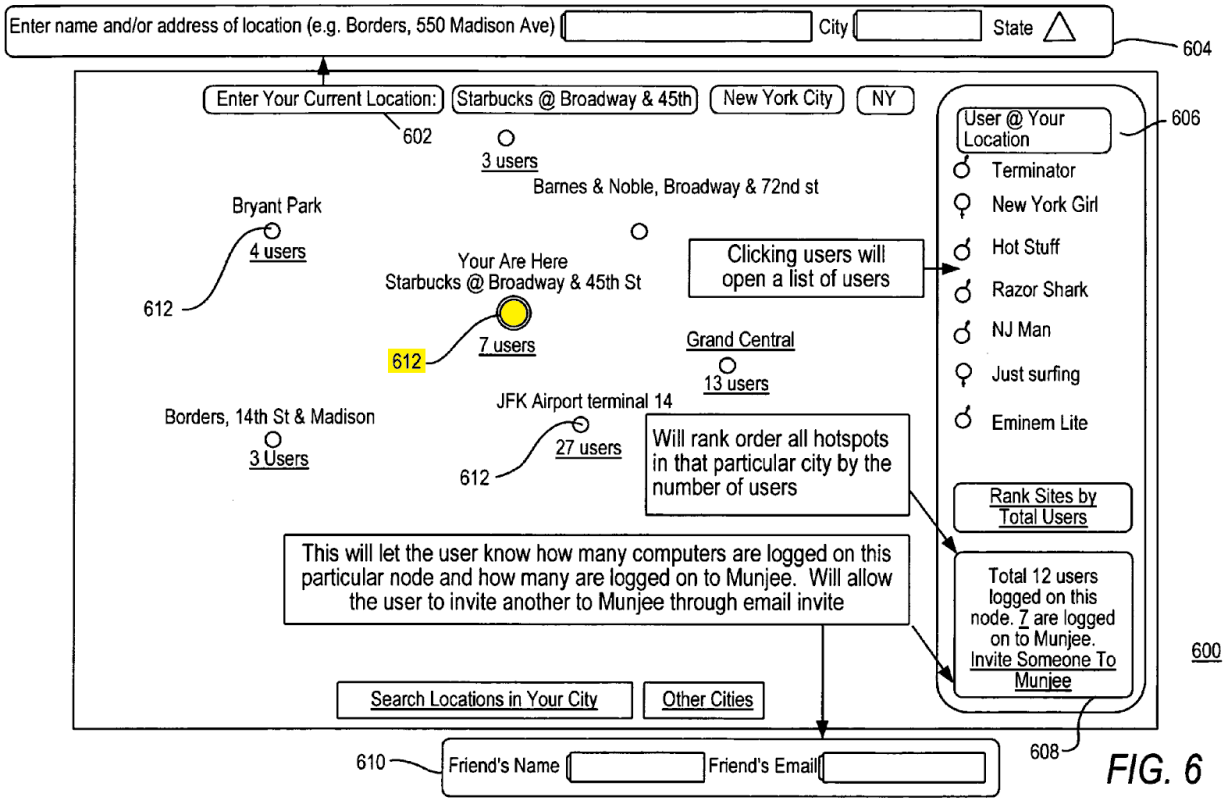


FIG. 6

(Baig, Fig. 6 (highlighting added).)

Figure 6 shows web page **600** that "displays the present hotspot, as well as other hotspots that are proximately located to the user's present hotspot." (Baig, ¶0077; Provisional, 0018.) Baig further explains that "if the user selects the link **612** associated with the present hotspot or another hotspot, the user is presented with the illustrative web page **700** shown in FIG. 7." (Baig, ¶0078; Provisional, 0018.) Figure 7 is shown below:

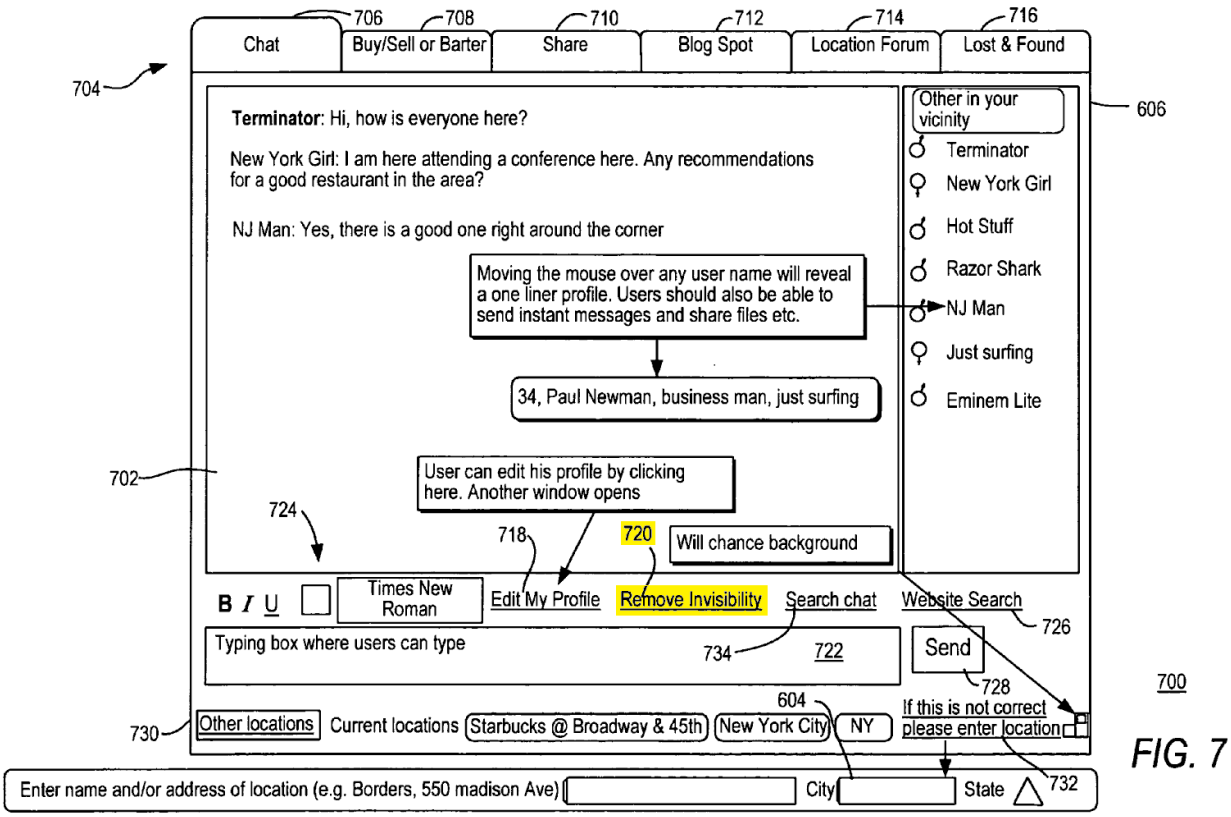


FIG. 7

(Baig, Fig. 7 (highlighting added).)

Figure 7 shows a web page **700** with a number of options for the selected hotspot. The web page also includes link **720** that allows the user to become visible to other users and which, as discussed above, provides a mechanism for collecting behavioral data from the first device user. (Schmandt, ¶¶136, 162.)

The behavioral data under the proposed combination was therefore collected "**as a result of redirection of the first device from an online site visited by the first device**," under at least two independent theories. First, as the sequence above makes clear, the first device was only able to reach web page **700** of Figure 7 – which allowed the user to specify their visibility preference using link **720** – as a result of

being redirected from the VCSP website ("**an online site visited by the first device**"), first from the login page **400** (Fig. 4) to web page **600** (Fig. 6), and then from web page **600** (Fig. 6) to web page **700** (Fig. 7). These redirections, either individually or collectively, qualify as "**redirection of the first device from an online site visited by the first device**," because in each case the web browser was redirected from a page on the VCSP website. The behavioral information was collected "**as a result of**" these redirections because, individually and collectively, they were an essential step in the causal chain that allowed the user to access web page **700** and activate link **720**. (Schmandt, ¶177.) But for the redirection, the behavioral information could not have been collected via the first device.

As a second and alternative way to find the claimed "**redirection**," as was well-known, a "link" such as link **720** refers to a well-known user interface option that, when activated by the user, causes the web browser to access a particular URL. (Schmandt, ¶178 (citing Hahn, 0035 ("A nice way to think about links is to imagine that underneath each link lies a URL.").) Accordingly, when the first mobile device user in Baig clicks link **720** on web page **700**, this causes "**a redirection**" of the browser to a URL associated with the link, which informs the server that the user has changed their visibility setting. The behavioral information was thus collected "**as a result of**" the redirection because the redirection via the URL notified the server of the user action. (Schmandt, ¶178.)

Under either theory, the behavioral data was also collected "**while the first device is not connected to the LAN**," because as explained for claim 3, it would have been collected when the first device user was logged in from a different LAN. And as also explained, under the combination with Xu, the user's visibility setting would have been saved and thus applicable when the first device later connected to "**the LAN**" through the current access point **106**. (Schmandt, ¶¶170-171.)

Finally, it appears that each webpage above (*i.e.* **400** (Fig. 4), **600** (Fig. 6), **700** (Fig. 7)) is part of the VSCP website provided by the content server. But nothing in claim 4 requires redirection to a different website; the claim only specifies redirection "**from an online site**," and places no limits on the destination of the redirection. Nothing in the term "**redirection**" requires different sites; in fact redirection was a basic feature of web programming for causing a browser to redirect to any arbitrary URL, which could have pointed to a webpage on the same or a different website. (Schmandt, ¶179.)

3. Claims 15-16

Dependent claims 15 and 16 are substantially similar to claims 3 and 4, respectively, but depend from claim 14. (Schmandt, ¶¶180-181.) They are obvious for the reasons previously stated.

E. Ground 3: Claims 6-7, 17-18 Are Obvious Over Ground 1 Prior Art

in Further View of Gerace.

1. Claim 6: "The method of claim 1 wherein the automatic action comprises selecting an advertisement, from among a plurality of possible advertisements, based at least in part on at least a portion of the user profile information associated with the device identifier of the first device."

2. Claim 7: "The method of claim 6 wherein the automatic action comprises causing the selected advertisement to be directed to the second device."

Claims 6 and 7 are closely related and thus will be discussed together.

Baig discloses a vicinity-based community service that includes, in addition to the features described for **Ground 1**, an advertising service in which advertisers can target advertisements to users at a particular hotspot based on (among other things) demographic information such as age and gender. (Baig, ¶¶0095, 0093; Provisional, 0022; Schmandt, ¶182.) Advertisements are selected based on a competitive bidding system. (Baig, ¶0062; Provisional, 0015.) As Baig explains in discussing one example, "[t]he winner of the bidding contest receives exclusive rights to advertise on the VCSP website for the selected hotspot at a particular time of day, for example between 6-8 pm to female end-users who are 18-25 years old at a particular location." (Baig, ¶0104; Provisional, 0024.)

Baig therefore discloses actions, in addition to the automatic actions described for claim 1, comprising "**selecting an advertisement, from among a plurality of possible advertisements**" (claim 6), and "**causing the selected advertisement to**

be directed to the second device" (claim 7), with the "**advertisement**" corresponding to an advertisement selected for delivery to the second device based on a winning bid. The advertisement is selected from "**among a plurality of possible advertisements**," *i.e.*, the available advertisements including those from other competing advertisers. The selection is, as noted, based on demographic user profile information of the second device user, such as age and/or gender.

And as explained for claim 1(d), it would have been obvious that such action would have been "**automatic**" because the advertisement would have been selected and delivered to the second device using the automatic website update techniques in Hahn discussed above. (Schmandt, ¶¶141-147, 183.) Alternatively, the advertisement could have been selected and delivered automatically as part of the creation and transmission of the webpage sent to the second device, after the second device logs into the content server. (Baig, Fig. 6, ¶0074; Provisional, 0017.)

But Baig does not disclose that the selection and display of the advertisement was "**based at least in part on at least a portion of the user profile information associated with the device identifier of the <u>first device</u>**," *i.e.*, associated with the <u>first</u> user whose first device is also connected to access point/hotspot, but this feature would have been obvious in view of **<u>Gerace</u>**.

Gerace discloses a system for targeted advertising based on a "user profile" that can include user demographic information. (Gerace, ¶¶0008-0009, 0083, 0062.)

A key feature of Gerace, for purposes of claims 6-7, is its ability to "assume" or "deduce" demographic information such as age and gender even if the user has not provided such information. (Gerace, ¶0010.) As Gerace explains:

> This profile information is used to better target the known user with advertisement[s]. The system **100** deduces demographic information (city, state, etc.) from a user's IP address, the type of article the user reads, search query he enters, shared behavior with other users (behavior or activities in common with) or shared relationships to other users. In one embodiment, the system **100** (a) assumes a Zip code for a given user based on Zip codes detected in the user's activities, (b) assumes age of the given user based on ages of others detected in the user's activities, and (c) assumes gender of the given user based on gender of others detected in the user's activities.

(Gerace, ¶0083.) The user profile, which includes the assumed demographic information, can then be used to target and display ads to the user. (Gerace, ¶0055 ("The present invention forms and maintains user profiles **17** (**FIG**. **2***h*) based on information received from end-users and information deduced by end-user activity as users of system **100**.").) Gerace therefore discloses selecting an advertisement to display to a user based, at least in part, on a portion of a user profile of at least one other user, such as age or gender of other users detected in the user's activities.

Manner, Rationale, and Motivation to Combine (Ground 1 Prior Art with

Gerace): It would have been obvious to combine the prior art for **Ground 1** with Gerace, predictably resulting in the combined system with the further ability to select and deliver advertisements to the second device user, "**based at least in part on at least a portion of the user profile information associated with the device identifier of the first device**," *i.e.*, based at least in part on demographic profile information of the first device user, *e.g.*, age and/or gender. (Schmandt, ¶187.)

For example, if the second device user did not provide demographic profile information such as age and/or gender, the system under the proposed combination would have deduced this information based on profile information of other users, which could have included the first device user based on (among other things) its relationship with the second device user, common activities, or simply the fact that the two are connected to the same access point/hotspot. These deduced characteristics, in turn, would have then been used in selecting advertisements for delivery to the second device. (Schmandt, ¶188.) Gerace is an analogous reference in the same field of Internet-based advertising and would have been reasonably pertinent to problems facing the inventor. (Schmandt, ¶190.)

A skilled artisan would have had many reasons to combine in this manner. Many users may have felt reluctant to provide their age and/or gender, and thus may have declined to do so. Baig acknowledges as much by making clear that, in one embodiment, entry of such information is optional. (Baig, ¶¶0070 & Fig. 4, 0071

("Preferably, some or most of the entry fields [for registration] are optional, such that only the user name field **502** and password related fields **504** and **506** are mandatory for registration."), Provisional, 0017.) The techniques in Gerace would thus have allowed the system of Baig – where the second device user elected to not provide age and/or gender – to deduce those characteristics and use them in selecting an advertisement. (Schmandt, ¶191.) These deduced characteristics are clearly preferable to having no information relating to the second device user, and would have improved the likelihood of selecting a relevant advertisement for delivery to the second device user. (*Id.*) A skilled artisan would have had more than a reasonable expectation of success and could have implemented the proposed combination using conventional techniques. (Schmandt, ¶¶192, 206.)

3. Claims 17-18

Dependent claims 17 and 18 are substantially similar to claims 6 and 7, respectively, except that they depend from claim 14. (Schmandt, ¶¶193-194.) They are obvious for the reasons previously stated.

F. Ground 4: Claims 11-12, 20-21, 23 Are Obvious Over Ground 1 Prior Art with Xu and Gerace.

1. Claim 11

2. Claim 12

Dependent claim 11 recites four subparts (i)-(iv) that consist of limitations

directly copied from claim 2 (subpart (i)), claim 3 (subpart (ii)), claim 4 (subpart (iii), and claims 6-7 (subpart (iv))and is thus obvious based on **Ground 1** in view of Xu and Gerace, based on the analysis for claims 2-4 and 6-7 provided above. (Schmandt, ¶¶195-199.) Claim 12 recites the same feature as claim 10 and is obvious for the same reasons. (Schmandt, ¶200.)

3. Claims 20-21 and 23

Dependent claims 20-21 and 23 are substantially similar to claims 11-12. (Schmandt, ¶¶201-202) and obvious for the previously-stated reasons.

VI. CONCLUSION

Petitioner respectfully requests institution.

Respectfully submitted,

/Scott T. Jarratt/

Scott T. Jarratt
Lead Counsel for Petitioner
Registration No. 70,297

Dated: March 20, 2024

HAYNES AND BOONE, LLP
2801 N. Harwood Ave Suite 2300
Dallas, Texas 75201
Customer No. 27683

CERTIFICATE OF WORD COUNT

Pursuant to 37 C.F.R. § 42.24(d), Petitioner hereby certifies, in accordance with and reliance on the word count provided by the word-processing system used to prepare this Petition, that the number of words in this paper is 14,000. Pursuant to 37 C.F.R. § 42.24(d), this word count excludes the table of contents, table of authorities, mandatory notices under § 42.8, certificate of service, certificate of word count, appendix of exhibits, and any claim listing.

Dated: March 20, 2024

/Scott T. Jarratt/
Scott T. Jarratt
Lead Counsel for Petitioner
Registration No. 70,297

CERTIFICATE OF SERVICE

The undersigned certifies that, in accordance with 37 C.F.R. § 42.6(e) and 37 C.F.R. § 42.105, service was made on Patent Owner as detailed below.

Date of service	March 20, 2024
Manner of service	FEDERAL EXPRESS
Documents served	Petition for *Inter Partes* Review Under 35 U.S.C. § 312 and 37 C.F.R. § 42.104 of U.S. 10,715,878; Petitioner's Exhibit List; Exhibits 1001-1014 and 1018-1023 and Petitioner's Power of Attorney.
Persons served	LOUIS J. HOFFMAN, P.C. 7689 East Paradise Lane Suite 2 Scottsdale, AZ 85260 UNITED STATES

/Scott T. Jarratt/
Scott T. Jarratt
Lead Counsel for Petitioner
Registration No. 70,297