UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

META PLATFORMS, INC.,
Petitioner

v.

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

Case IPR2022-00773
U.S. Patent No. 8,677,398 B2
Issue Date: March 18, 2014

Title: SYSTEMS AND METHODS FOR TAKING ACTION WITH RESPECT TO ONE NETWORK-CONNECTED DEVICE BASED ON ACTIVITY ON ANOTHER DEVICE CONNECTED TO THE SAME NETWORK

PETITION FOR *INTER PARTES* REVIEW OF U.S. PATENT NO. 8,677,398 B2

Table of Contents

Page

I. MANDATORY NOTICES UNDER §42.8(A)(1) 1

A. Real Party-In-Interest under §42.8.(b)(1) 1

B. Related Matters under §42.8(b)(2) 1

C. Lead and Back-Up Counsel under §42.8(b)(3) 2

D. Service Information 3

II. FEE PAYMENT 3

III. REQUIREMENTS UNDER §§ 42.104 AND 42.108 AND CONSIDERATIONS UNDER §§ 314(A) AND 325(D) 3

A. Grounds for Standing 3

B. Identification of Challenge and Statement of Precise Relief Requested 3

C. Considerations Under §§ 314(a) and 325(d) 4

IV. OVERVIEW OF THE PATENT 4

A. Level of Ordinary Skill 4

B. Specification Overview 5

V. CLAIM CONSTRUCTION 7

VI. THE CHALLENGED CLAIMS ARE UNPATENTABLE 8

A. Overview of Grounds 8

B. Prior Art Status of Relied-Upon References 9

C. Ground 1: Claims 36 and 37 Are Obvious Over Baig in View of Zwicky, Satapati, and Hahn 11

1. Claim 36 11

(a) "receiving at one or more of the computers an electronic identifier of a first device;" 13

Table of Contents
(continued)

Page

(b) "automatically generating and storing electronic indicia of an association between the first device identifier and an electronic identifier of a second device based on automatically recognizing that each of the first and second devices was connected, independently of the other, to a common local area network, wherein the computer system is connected to the local area network through the Internet but is not in the local area network; and" 24

(c) "based on the electronic indicia of the association between the first and second device identifiers, automatically sending an electronic transmission that causes another programmed hardware computer system to take an action, based on first electronic profile data associated with the first device identifier, with respect to the second device, which is indicated at the time of the action by the second device identifier." 32

2. Claim 37: "The medium of claim 36 wherein the electronic association is recognized based on a common IP address, or portion thereof, wherein network traffic is routed via the common IP address for each of the first and second devices when each is connected to the local area network." 41

D. Ground 2: Claims 36 and 37 Are Obvious Over Baig in View of Zwicky, Satapati, and Hahn, in Further View of Appelman 41

E. Ground 3: Claims 36 and 37 Are Obvious Over Baal-Haness and Appelman 50

1. Claim 36 50

(a) "receiving at one or more of the computers an electronic identifier of a first device;" 51

Table of Contents
(continued)

Page

(b) "automatically generating and storing electronic indicia of an association between the first device identifier and an electronic identifier of a second device based on automatically recognizing that each of the first and second devices was connected, independently of the other, to a common local area network, wherein the computer system is connected to the local area network through the Internet but is not in the local area network; and" 54

(c) "based on the electronic indicia of the association between the first and second device identifiers, automatically sending an electronic transmission that causes another programmed hardware computer system to take an action, based on first electronic profile data associated with the first device identifier, with respect to the second device, which is indicated at the time of the action by the second device identifier." 60

2. Claim 37: "The medium of claim 36 wherein the electronic association is recognized based on a common IP address, or portion thereof, wherein network traffic is routed via the common IP address for each of the first and second devices when each is connected to the local area network." 68

F. Ground 4: Claim 37 Is Obvious Over Baal-Haness and Appelman, in Further View of Zwicky and Satapati 70

VII. CONCLUSION 74

List of Exhibits

Exhibit No.	Description of Document
1001	U.S. Patent No. 8,677,398 B2 to Roy Shkedi (filed June 23, 2011, issued March 18, 2014) ("'398" or "'398 patent")
1002	Declaration of Christopher M. Schmandt ("Schmandt")
1003	U.S. Patent Appl. Pub. No. 2008/0113674 A1 to Mohammad Faisal Baig (filed October 31, 2007, published May 15, 2008) ("Baig")
1004	U.S. Provisional Appl. No. 60/858,204 to Mohammad Baig (filed Nov. 10, 2006) ("Baig Provisional" or "Provisional")
1005	Redline document showing differences between Baig (Ex. 1003) and Baig Provisional (Ex. 1004)
1006	Excerpts from Elizabeth D. Zwicky et al., *Building Internet Firewalls* (2d ed. 2000) ("Zwicky")
1007	U.S. Patent No. 7,356,045 B2 to Suresh K. Satapati et al. (filed Oct. 22, 2002, issued April 8, 2008) ("Satapati")
1008	Excerpts from Harley Hahn, *The Internet Complete Reference* (2d ed. 1996) ("Hahn")
1009	U.S. Patent No. 7,899,862 B2 to Barry Appelman et al. (filed November 18, 2003, issued March 1, 2011) ("Appelman")
1010	U.S. Patent Appl. Pub. No. 2007/0067459 A1 to Gal Baal-Haness (filed September 11, 2006, published March 22, 2007) ("Baal-Haness")
1011	U.S. Provisional Appl. No. 60/718,190 to Gal Baal-Haness (filed Sept. 16, 2005) ("Baal-Haness Provisional")
1012	Redline document showing differences between Baal-Haness (Ex. 1010) and Baal-Haness Provisional (Ex. 1011)

List of Exhibits

Exhibit No.	Description of Document
1013	P. Srisuresh et al., Request for Comments (RFC) 2663, *IP Network Translator (NAT) Terminology and Considerations*, August 1999 ("RFC 2663")
1014	Request for Comments (RFC) 793, *Transmission Control Protocol, DARPA Internet Program Protocol Specification*, September 1981 ("RFC 793")
1015	Declaration of Sylvia D. Hall-Ellis, Ph.D. ("Hall-Ellis")
1016	Proof of Service of Complaint

I. MANDATORY NOTICES UNDER §42.8(A)(1)

A. Real Party-In-Interest under §42.8.(b)(1)

Meta Platforms, Inc. is the real party-in-interest to this IPR petition.

B. Related Matters under §42.8(b)(2)

The '398 patent is the subject of pending litigation involving Petitioner: *AlmondNet, Inc. and Intent IQ, LLC v. Meta Platforms, Inc.*, Case No. 6:21-cv-00896-ADA (W.D. Tex.). Petitioner was first served on September 2, 2021. (EX1016.) The '398 patent is also the subject of other pending litigations:

- *AlmondNet, Inc. v. Microsoft Corporation*, 6-21-cv-00897 (W.D. Tex.)
- *AlmondNet, Inc. v. Amazon.com, Inc.*, 6-21-cv-00898 (W.D. Tex.)
- *AlmondNet, Inc. v. Samsung Electronics Co.*, 6-21-cv-00891 (W.D. Tex.)
- *Roku, Inc. v. AlmondNet, Inc.*, 1-21-cv-01035 (D. Del.)
- *AlmondNet, Inc. v. Roku, Inc.*, 6-21-cv-00731 (W.D. Tex.)

The '398 patent was also subject to previous litigation in *AlmondNet, Inc. v. Oath Holdings Inc*., 1-19-cv-00247 (D. Del.), which was terminated in March 2019.

The '398 patent was also the subject of an IPR proceeding filed by third party Yahoo! several years ago, *Yahoo! Inc. v. Intent IQ, LLC*, Case No. IPR2017-01299, in which institution was denied. (*See* IPR2017-01299, Paper 9 (Oct. 31, 2017).) Petitioner had no involvement in the Yahoo! petition.

C. Lead and Back-Up Counsel under §42.8(b)(3)

Petitioner provides the following designation of counsel.

LEAD COUNSEL	BACK-UP COUNSEL
Heidi L. Keefe (Reg. No. 40,673) hkeefe@cooley.com COOLEY LLP ATTN: Patent Group 1299 Pennsylvania Ave. NW, Suite 700 Washington, DC 20004 Tel: (650) 843-5001 Fax: (650) 849-7400	Phillip E. Morton (Reg. No. 57,835) pmorton@cooley.com COOLEY LLP ATTN: Patent Group 1299 Pennsylvania Ave. NW, Suite 700 Washington D.C. 20004 Tel: (202) 728-7055 Fax: (202) 842-7899
	Andrew C. Mace (Reg. No. 63,342) amace@cooley.com COOLEY LLP ATTN: Patent Group 1299 Pennsylvania Ave. NW, Suite 700 Washington D.C. 20004 Tel: (650) 843-5808 Fax: (650) 849-7400
	Mark R. Weinstein (Admission *pro hac vice* to be requested) mweinstein@cooley.com COOLEY LLP ATTN: Patent Group 1299 Pennsylvania Avenue NW Suite 700 Washington D.C. 20004 Tel: (650) 843-5007 Fax: (650) 849-7400

D. Service Information

This Petition is being served by Federal Express to the attorney of record for the ’398 patent, Intent IQ, LLC, 37-18 Northern Boulevard, Suite 404, Long Island City, NY 11101. Petitioner consents to electronic service at the addresses provided above for lead and back-up counsel.

II. FEE PAYMENT

Petitioner requests review of 2 claims, with a $41,500 payment.

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

A. Grounds for Standing

Petitioner certifies that the ’398 patent is available for IPR and that Petitioner is not barred or otherwise estopped.

B. Identification of Challenge and Statement of Precise Relief Requested

Petitioner requests IPR institution based on:

Ground	Claims	Basis for Challenge under §103
1	36, 37	Baig (EX1003/1004), Zwicky (EX1006), Satapati (EX1007), and Hahn (EX1008)
2	36, 37	Ground 1 Prior Art (Baig, Zwicky, Satapati, and Hahn), in further view of Appelman (EX1009)
3	36, 37	Baal-Haness (EX1010/1011) and Appelman
4	37	Ground 3 Prior Art (Baal-Haness and Appelman), in further view of Zwicky and Satapati

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

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

§314(a): The *General Plastic* factors are not relevant as this is the first and only IPR petition filed by Petitioner with respect to the '398 patent. As noted in **Part I.B** above, the '398 patent was subject to a previous IPR petition filed by Yahoo! (IPR2017-01299), with which Petitioner had no involvement.

Nor do the *Fintiv* factors support discretionary denial under §314(a). The pending litigation against Petitioner is in early stages, and the present Petition was filed several months before the one-year deadline. No claim construction rulings and no significant discovery have occurred. A trial date has been set for August 21, 2023, but Petitioner intends to move to stay pending any instituted IPR.

§325(d): This Petition does not raise §325(d) issues because it relies on new prior art references that were not considered during the prosecution of the '398 patent, or in the prior IPR challenge (IPR2017-01299).

IV. OVERVIEW OF THE PATENT

A. Level of Ordinary Skill

A person of ordinary skill in the art as of April 17, 2007 (the earliest priority date for the '398 patent) would have possessed at least 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). A person could also have qualified with more formal education and less technical experience, or vice versa. (Schmandt, ¶¶10-14.)

B. Specification Overview

The '398 patent states that it relates "to online access and targeted delivery of advertisements." ('398, 1:17-18.) The patent discloses a number of techniques involving, generally speaking, recognizing related devices so that activities performed with a first device can be used to take an action with respect to a second device. (*E.g.*, '398, 7:66-8:11.) In one embodiment, targeted advertisements are provided to a user's television based on online activities taking place on the user's computer. (*E.g.*, '398, 8:38-60.) Figure 1 depicts a basic layout of a system for targeting advertisements in this context:

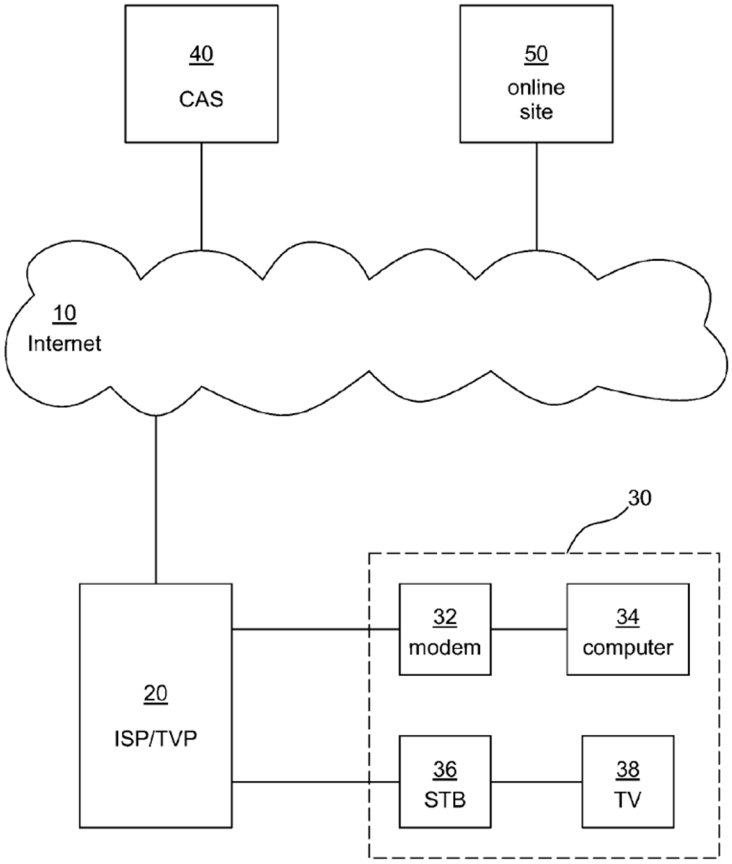


FIG. 1

('398, Fig. 1.) The system of Figure 1 includes online access device **32** (such as a modem or wireless access point), 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**. ('398, 9:21-24, 2:42-60.) Common service provider **20** can offer both Internet access via the online access device **32** as well as television service through STB **36**. ('398, 9:30-41.) 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. ('398, 10:57-

64.) 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. ('398, 10:53-11:41.)

In order to determine that, for example, computer **34** and STB **36** are related to each other, IP address information associated with those devices can be used. ('398, 9:42-10:2, 10:23-52.) For example, if both the computer and STB access the internet via modem **32** (*e.g.*, they are part of a local area network ("LAN")), the remote network will only see the same IP address—i.e., modem **32**'s IP address—for both devices. ('398, 9:52-57, 10:23-27, 12:60-13:21 ("An online site or server access by any one of the multiple devices only 'sees' the common IP address (the modem IP address).").) Thus, "[t]he common IP address enables delivery of television ads to STB **36** based on access of an online site via the common IP address (or based on other user profile information derived from online activity observed as originating from the online access IP address of modem **32**, i.e., from the common IP address)." ('398, 13:42-47.)

V. CLAIM CONSTRUCTION

Petitioner does not believe an express claim construction is necessary at this time for this IPR.

VI. THE CHALLENGED CLAIMS ARE UNPATENTABLE

A. Overview of Grounds

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 are rendered obvious by the prior art.

Grounds 1 and 2 rely primarily on **Baig** (EX1003), which discloses a technique for placing multiple users connected to the same WiFi access point or hotspot into a group, and then providing services (such as chat and instant messaging) to the users in that group. (Schmandt, ¶¶39-41.) Grounds 3 and 4 rely primarily on **Baal-Haness** (EX1010), which discloses a system similar to Baig for identifying and providing services to users whose computers are connected to the same local area network. (*Id.*, ¶¶63-64.)

Baig and Baal-Haness are strong references that disclose the majority of the limitations of the challenged claims. Petitioner cites other references in combination primarily for well-known or ancillary features. For example, Grounds 1, 2, and 4 cite **Zwicky** (EX1006) and **Satapati** (EX1007) for industry-standard Network Address Translation (NAT) techniques that would have been within the general knowledge of an ordinarily skilled artisan. (*Id.*, ¶80.) Grounds 1-2 cite **Hahn** (EX1008) for well-known techniques for automatically updating and refreshing

webpages. (*Id.*, ¶¶52-53, 124.) And Grounds 2-4 cite **Appelman** (EX1009) for unremarkable features of dividing server functionality across two computing systems, and filtering users based on profile information such as age or gender. (*Id.*, ¶¶127-128.) The challenged claims are obvious in view of the prior art.

B. Prior Art Status of Relied-Upon References

Each reference cited in the grounds listed in **Part II.B** qualifies as prior art. Zwicky and Hahn qualify as prior art because they are printed publications that were published more than one year before the '398 priority date. (Hall-Ellis, EX1015, ¶¶42-55.) Satapati and Appelman qualify as prior art under §102(e) (pre-AIA) because they are patents issuing from applications filed before the '398 priority date. (Schmandt, ¶¶49, 54.) Baal-Haness also qualifies as prior art under at least §102(e) because it is a published patent application filed before the '398 priority date.[1]

---

[1] Baal-Haness is prior art as of its filing date, but is also entitled to the filing date of a September 16, 2005 provisional to which it claims priority (EX1011). The provisional has no material differences provides support for and enables claims appearing in the published application. (Schmandt, ¶¶65-69.) Petitioner therefore reserves the right to rely on the Baal-Haness provisional in the event Patent Owner attempts to "swear behind" Baal-Haness.

Baig qualifies as prior art under at least §102(e). Petitioner acknowledges that the Baig application was filed on October 31, 2007 – *after* the '398 patent priority date – 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 its provisional filing date.

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 requirements are met.

With respect to (1), no material differences exist between Baig and the Provisional. (*See* Schmandt, ¶43 (citing EX1005 (redline comparison)).) All of the relied-upon disclosures in Baig, therefore, appear in the Provisional. For convenience, therefore, each citation to Baig (EX1003) below will be accompanied by a parallel citation to the Provisional (EX1004) where the same disclosure appears.

With respect to (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). Here, the Provisional included 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 claims thus clearly provide written description support for their corresponding claims in Baig, and Provisional would have enabled an ordinarily skilled artisan to practice their subject matter. (Schmandt, ¶¶44-45.)

And putting aside the originally-filed claims, the Provisional supports every limitation of at least published claim 1 and would have enabled an ordinarily skilled artisan to make and use its subject matter. (*Id.*) Baig therefore qualifies as §102(e) prior art as of November 10, 2006.

C. Ground 1: Claims 36 and 37 Are Obvious Over Baig in View of Zwicky, Satapati, and Hahn

1. Claim 36

The preamble recites "[**a**]**n article comprising a non-transitory tangible medium encoding computer-readable instructions that, when applied to one or more computers, instruct the one or more computers to perform a method comprising**…." The "**article**" in Baig takes the form of computer memory within "**one or more computers**," which correspond to one or more content servers, as depicted in Figure 1:

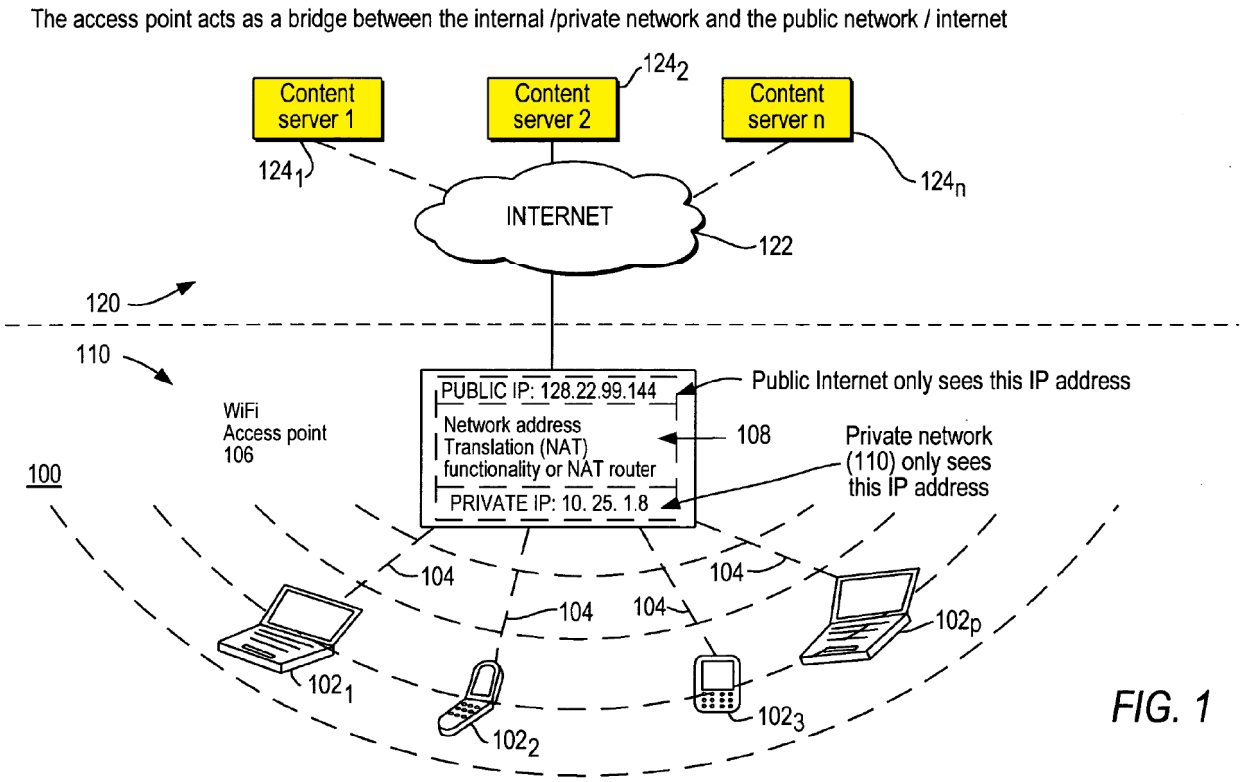


FIG. 1

(Baig, Fig. 1 (highlighting added).) Figure 1 above depicts three content servers **124** coupled to the Internet **122**, to which a WiFi wireless access point **106** is also coupled. (*See also* Baig, Fig. 2 (showing content server **224**).) For purposes of this Petition, any one of these content servers, or any collection of them, discloses "**one or more computers**." As explained in detail below, a content server "**perform**[s] **a method**," that renders obvious the steps of claim 36. The software in Baig would also have been encoded on a "**non-transitory tangible medium**," *e.g.*, memory for storing computer programs. Baig explains that each content server "includes at least one processor, **memory** and support circuitry for running **programs**…." (Baig,

¶0052; Provisional, 0012-0013.)[2] The content server in Baig could not run programs unless they were stored in a non-transitory tangible medium. (Schmandt, ¶72.) It would also have been apparent and obvious that the memory encodes "**computer-readable instructions**" for carrying out the programs when executed. (*Id.*, ¶73.)

(a) "receiving at one or more of the computers an electronic identifier of a first device;"

This limitation is disclosed and rendered obvious by Baig in view of Zwicky and Satapati. Figure 2 of Baig (below) depicts the connection of mobile devices through a wireless access point and hotspot:

[2] Unless noted, emphasis in prior art quotations was added by Petitioner.

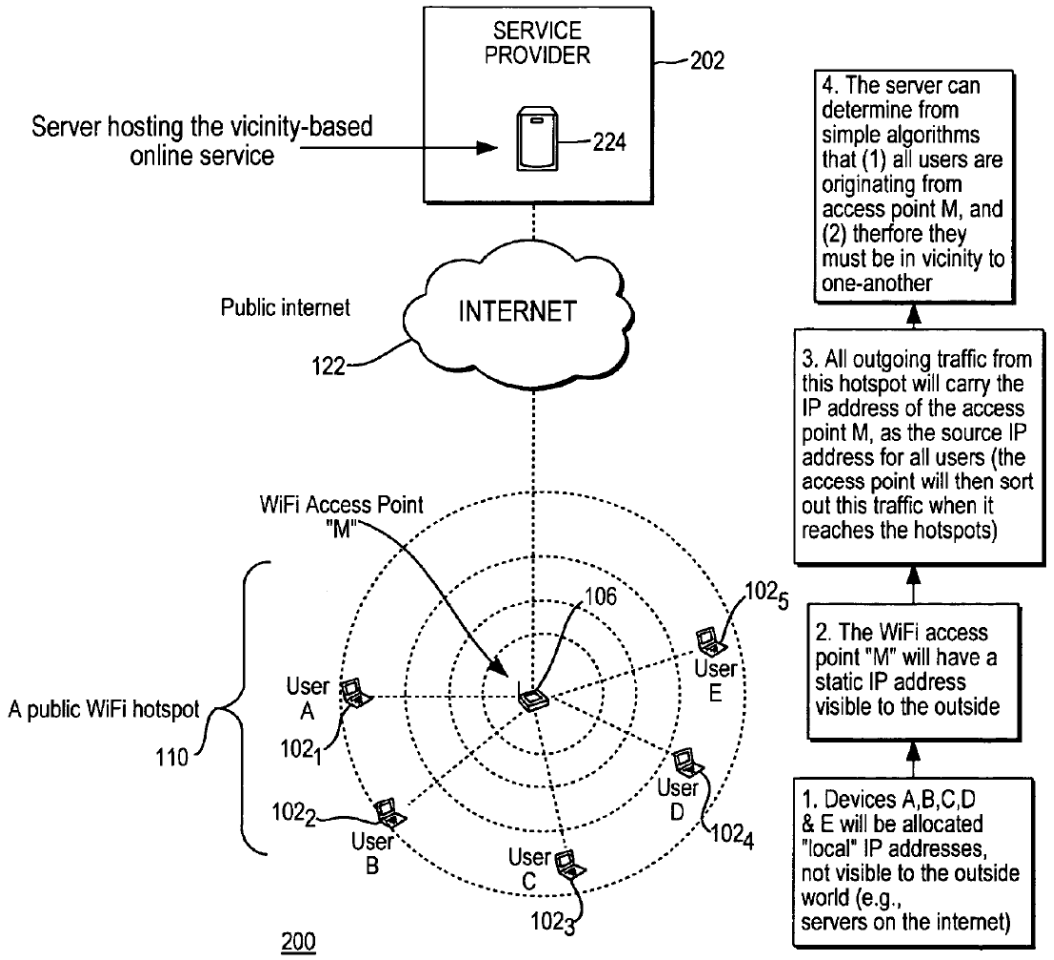


FIG. 2

(Baig, Fig. 2.) Figure 2 shows communications network **200** having a WiFi hotspot **110** with WiFi wireless access point "M" **106**. (Baig, ¶0049; Provisional, 0012.) Wireless access point **106** connects to mobile devices $\mathbf{102_1}$ through $\mathbf{102_5}$ and also connects to content server **224** through "the public Internet **122** in a conventional manner." (*Id.*) For purposes of claim 36(a), any one of the mobile devices **102** as shown in Figure 2 corresponds to a "**first device**." And as noted, a content server in Baig corresponds to "**one or more of the computers**."

A mobile device in Baig ("**first device**") has an "**electronic identifier**," which

includes an IP address transmitted by the access point **106** to the content server **224** over the Internet **122**. As stated in the Step 3 box of Figure 2 above, "[a]ll outgoing traffic from this hotspot will carry the IP address of the access point M, as the source IP address for all users (the access point will then sort out this traffic when it reaches the hotspots)." (Baig & Provisional, Fig. 2.) As was well-known to skilled artisans, packets sent over the Internet included an **IP address** of the source and destination devices. (Schmandt, ¶76.)

As explained below, the "**electronic identifier of a first device**" for claim 36(a) under the proposed combination takes the form of the combination of: **(a)** the IP address of the access point, and **(b)** a TCP/IP port number associated with the mobile device (the "**first device**") that is connected to the access point, based on Baig in view of Zwicky and Satapati. This electronic identifier is **received** by the content server under the proposed combination, as explained below.

Turning first to the IP address, Baig discusses "network address translation" (NAT), which was widely known. (Schmandt, ¶77; Baig, ¶0043 and Provisional, 0011 ("The access point **106**… provides network address translations (NAT)….").) NAT refers to industry-standard techniques for allowing devices to share a single connection to the Internet. (Schmandt, ¶77; *see also* Zwicky, EX1006, pp.0036-0037.) NAT enables an intermediary device (such as an access point) to receive network communications between a local device and a remote device connected to

the Internet, and then modify (or "translate") their IP addresses. (Schmandt, ¶¶48, 77.) Baig explains:

> The access point **106** utilizes a unique "public" IP address (e.g., 126.22.99.144 illustratively shown in FIG. 1) which 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**. An IP address is necessary because all data communications takes place in form of data packets. Each packet must contain the IP address of the source device and the IP address of the destination device….
>
> Whenever a mobile device **102** that is connected to a hotspot **110** requests information from the public network (e.g., the Internet) **120**, the mobile device **120** sends data packets containing a "local" IP address to the access point **106**… On the other hand, the access point **106** interacts with the public network **120** with a public IP address, which is visible to all devices on the public internet **122**.
>
> The access point **106** (which includes the NAT router **108**) 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, ¶¶0044-0046; Provisional, 0011.)

The techniques described above were not invented by Baig – they describe well-known NAT techniques for allowing multiple mobile devices to communicate over the Internet using a single external (or "public") IP address. (Schmandt, ¶78.) For example, when a mobile device in Baig wishes to *send* packets through the

Internet, access point **106** replaces the "local IP address" in those outgoing packets with the "public IP address" of access point **106**. (*Id.*; Baig, ¶¶0046, 0050; Provisional, 0011-0012.) These disclosures confirm existence of "**an electronic identifier of a first device**," which includes the IP address of the access point **106** to which the mobile device ("**a first device**") is connected.

To avoid any confusion, Petitioner has mapped the claimed "**electronic identifier**" to the "public" IP address of the access point in Baig – not the "local" IP address of the mobile device. This is because, as noted below, claim 36(a) further requires that the "**electronic identifier**" be received at the "**one or more computers**," but as noted by Baig above, the "local" IP address is not visible outside the private/local network.

But how does the public IP address of access point **106** in Baig disclose an "**electronic identifier of <u>a first device</u>**," as opposed to just an electronic identifier of access point **106**? The answer to this question is readily provided by the industry-standard network addressing translation (NAT) techniques mentioned above, which are expressly mentioned by Baig but not described in detail. (Baig, ¶¶0043 ("The access point **106**… provides network address translations (NAT)…."); Baig, 0011; *see also* Baig, ¶¶0046, 0049-0051 & Provisional, 0011-0012 (referring to "NAT router").) Ground 1 therefore cites **<u>Zwicky</u>** (EX1006) and **<u>Satapati</u>** (EX1007), which provide details about standard NAT techniques that Baig mentions but

appears to take for granted. (Schmandt, ¶¶79-80.)

As was well-known, packets sent over the Internet not only included an **IP address** of the source and destination devices, but also a source and destination **port number** to identify a process or endpoint associated with the source and destination IP addresses. (Schmandt, ¶81.) Port numbers in TCP/IP are commonly represented as a number added to the end of an IP address after a colon; for example, the string "151.207.240.107**:**443" would represent an IP address of "151.207.240.107" and a port number of "443." TCP/IP port numbers (like IP addresses) have been standard information fields in TCP/IP packets since at least the early 1980s. (*Id*.)

NAT includes a technique known as "port translation" that uses port numbers to allow multiple devices to share a common public IP address. (Satapati, 1:34-36; Schmandt, ¶82.) This is graphically depicted in Figure 5-4 of Zwicky:

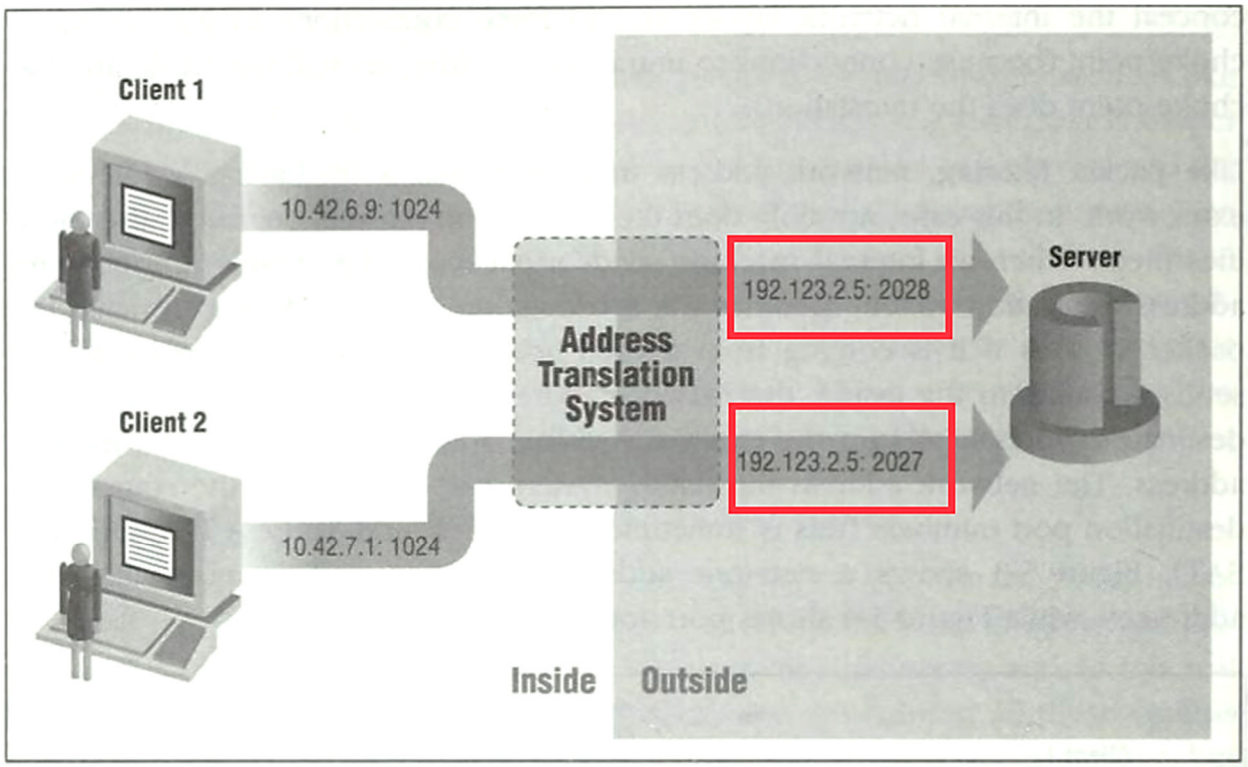


Figure 5-4. Port and address translation

(Zwicky, Fig. 5-4, p.0038 (red annotation added).) Figure 5-4 shows Client 1 and Client 2 inside a local network with locally-assigned IP addresses (*i.e.*, 10.42.6.9 and 10.42.7.1). Figure 5-4 shows an intermediary "Address Translation System" sitting between the clients and a remote server outside the local network. Like the access point **106** in Baig, this Address Translation System replaces the local IP addresses for Client 1 and Client 2 with the same IP address (*i.e.*, 192.123.2.5), to allow them to communicate with the remote server. The Address Translation System also assigns distinct TCP/IP **port numbers** to these computers (2028 for Client 1 and 2027 for Client 2), thus differentiating them. The port number thus allows multiple

distinct devices to use a single IP address yet be uniquely identified by port number when communicating over the Internet. (Satapati, 2:66-67; Schmandt, ¶50.)

For purposes of claim 36(a), therefore, "**an electronic identifier of a first device**" under the proposed combination of Baig, Zwicky and Satapati corresponds to the combination of **(a)** the IP address of the access point or hotspot to which a mobile device ("**first device**") was connected, and **(b)** the TCP/IP port number associated with the first device, as taught in Zwicky and Satapati. The IP address and port number thus provide "**an electronic identifier <u>of a first device</u>**" because, together, they uniquely identify a particular mobile device that seeks to connect with the content server in Baig. (Schmandt, ¶83.) Petitioner will explain below the rationale and motivation to combine Baig with Zwicky and Satapati.

Petitioner's mapping of the IP address and port number to the claimed "**electronic identifier**" is consistent with the '398 specification, which explains that the identifier may include any "identifying code or data element" and may be permanently or temporarily assigned to a device. ('398, 15:3-8.) The '398 specifically identifies an "IP address" as one example. ('398, *e.g.*, 15:13-17.)

Baig next discloses "**receiving at one or more of the computers**" the claimed electronic identifier. This is because the content server in Baig ("**one or more of the computers**") receives the IP address of the access point or hotspot when the mobile device attempts to connect. This is directly shown in Figure 2 above. (Baig,

Fig. 2 ("3. All outgoing traffic from this hotspot will carry the IP address of the access point M…."), *id.* (showing outgoing traffic routed to server **224** over Internet **122**); *see also* Baig, ¶¶0055-0057; Provisional, 0013; Schmandt, ¶85.)

The content server in Baig therefore receives, in response to a login request from a user at a mobile device ("**first device**"), the source IP address of the access point used to route packets to the mobile device. (Baig, *e.g.*, ¶¶0044 ("Each packet must contain <u>the IP address of the source device</u> and the IP address of the destination device."), 0045; Provisional, 0011.) Under the proposed combination, the content server would also have received, along with the IP address of the access point, the port number assigned to the mobile device seeking to connect.

Rationale and Motivation to Combine (Baig with Zwicky and Satapati): It would have been obvious to combine Baig with the port translation teachings of Zwicky and Satapati, predictably resulting in the content server of Baig ("**one or more of the computers**") receiving the IP address of the access point <u>and</u> a port number associated with the mobile device.

At the outset, Baig, Zwicky and Satapati are analogous references in the field of providing online access to information over the Internet and/or local networks. (Schmandt, ¶87.) Baig, Zwicky and Satapati would also have been reasonably pertinent to a number of problems facing the inventors, including how to differentiate devices connected to a common local network using IP addresses and

enable those devices to communicate with servers over the Internet. (*Id.*)

An ordinarily skilled artisan would have found the proposed combination straightforward and would have been amply motivated to make it. (Schmandt, ¶88.) As noted, Baig repeatedly refers to NAT techniques performed by "NAT router **108**" within access point **106**. (Baig, ¶¶0043, 0046, 0049-0050; Provisional, 0011-0012.) Figure 1 specifically requires that access point **106** have NAT functionality **108**:

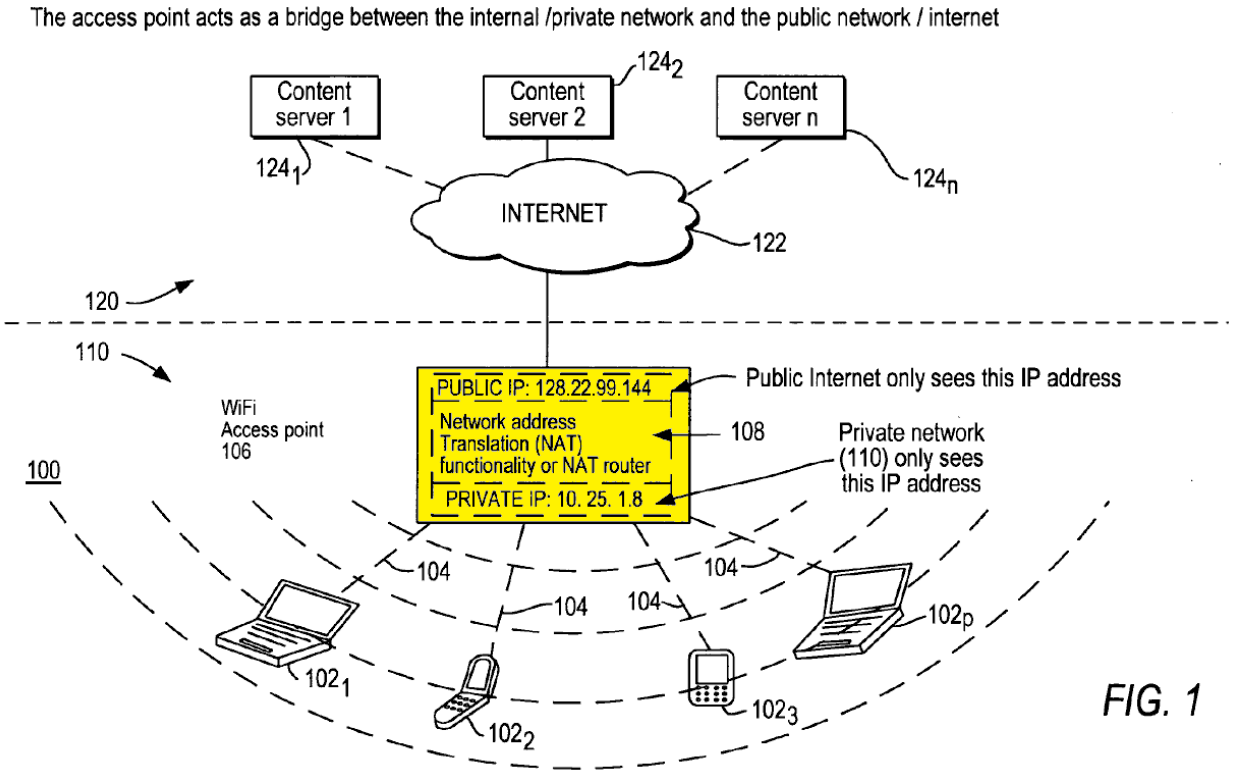


FIG. 1

(Baig & Provisional, Fig. 1 (highlighting added).) An ordinarily skilled artisan would have understood Baig's references to "NAT" as referring to the NAT techniques further described in Zwicky and Satapati. (Baig, ¶0050 ("The NAT router **108** at the access point **106** replaces the IP address of the source mobile device

with the IP address of the access point in a well known manner."); Provisional, 0012.) Baig's repeated references to NAT provide an express motivation to consult Zwicky and Satapati. (Schmandt, ¶88.)

An ordinarily skilled artisan would also have appreciated that the port translation techniques of Zwicky and Satapati would likely have been *required* to enable the system of Baig to function properly. As noted, the access point in Baig uses the same IP address for all mobile devices when communicating over the Internet. An additional level of translation would have been beneficial – and likely mandatory – to uniquely identify, differentiate and properly route traffic between individual mobile devices when communicating over the Internet. (Schmandt, ¶89.) This is echoed by Satapati, which explains that "NAT may use port address translation, where port numbers are used to further identify different devices with the same address." (Satapati, 1:34-36.)

Zwicky also provides several express motivations to use NAT port translation. (Schmandt, ¶90.) Zwicky explains that "[t]he main purpose of network address translation is to economize on address space, but it can also provide some security advantages." (Zwicky, p.0038.) With respect to the former purpose, it was well-known that the number of IP addresses available on the Internet is finite. (Schmandt, ¶90.) Port translation would have conserved IP addresses by allowing multiple devices to communicate over the Internet while sharing a single public IP address.

(*Id.*; *see also* Satapati, 1:63-2:3 (noting that port translation allows tens of thousands of users to share a common IP address).) As noted above, Zwicky also observes that NAT provides security benefits by facilitating greater monitoring and control of incoming network traffic from the Internet, providing a further motivation to combine. (*Id.*; Zwicky, pp.0038-0039.) Zwicky does identify potential disadvantages of NAT, but those would not have outweighed the benefits of using NAT or otherwise discouraged the combination. (Schmandt, ¶91.) And finally, an ordinarily skilled artisan would have had more than a reasonable expectation of success, as the disclosures in Baig, Zwicky and Satapati describe techniques that were known well and were fully enabling. (Schmandt, ¶¶92, 185-189.)

(b) "automatically generating and storing electronic indicia of an association between the first device identifier and an electronic identifier of a second device based on automatically recognizing that each of the first and second devices was connected, independently of the other, to a common local area network, wherein the computer system is connected to the local area network through the Internet but is not in the local area network; and"

After receiving a login request from a mobile device connected to an access point, as discussed above, the server determines if multiple mobile devices are connected to that same access point. This is shown in Step **306** of Figure 3:

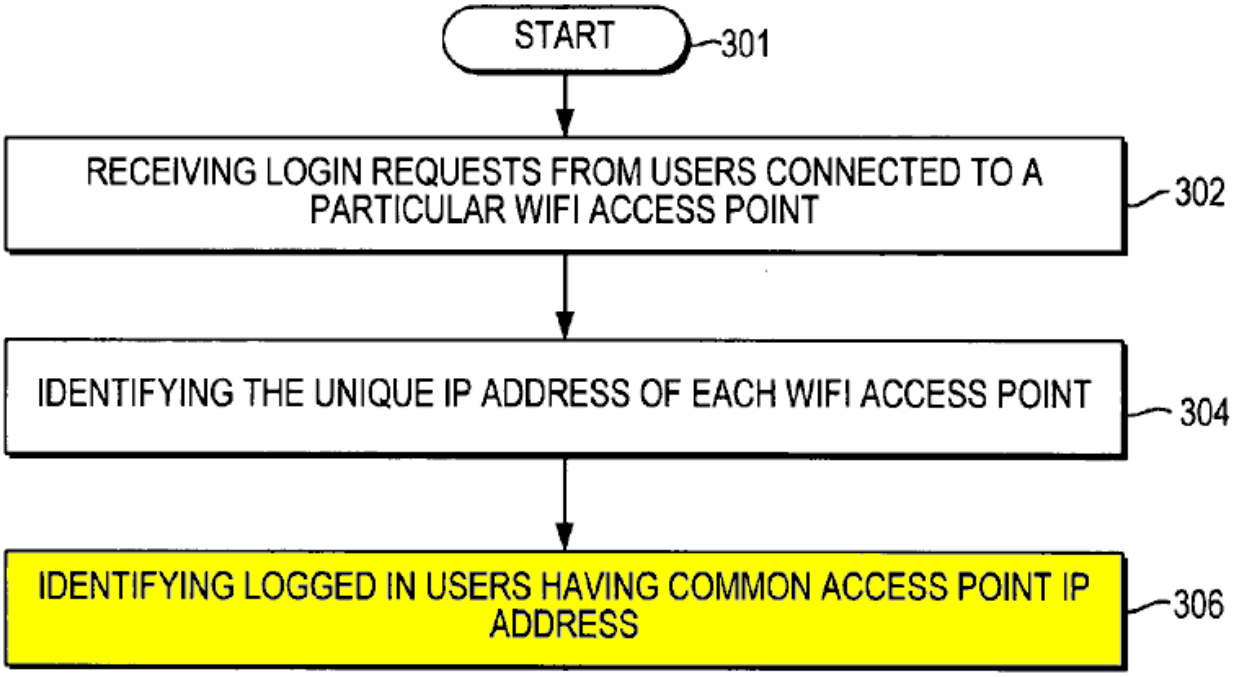


FIG. 3

(Baig & Provisional, Fig. 3 (partial figure; highlighting added).) "At step **306**, the server identifies <u>all the users who have logged in from a common hotspot as having the same access point IP address</u>." (Baig, ¶0056; Provisional, 0013 ("At step **306**, the server **224** identifies the logged-in users having the same access point IP address."); Schmandt, ¶93.)

The server in Baig therefore performs the step of "**automatically generating and storing electronic indicia of an association between the first device identifier and an electronic identifier of a second device**," when it identifies at least two mobile devices sharing the same access point IP address. (Baig, Fig. 3 (Step 306); Baig, ¶0056; Provisional, 0013.) The two mobile device IP addresses,

in fact, are more than simply "**associate**[ed]" with each other – they match, reflecting that they refer to the same access point. (Schmandt, ¶94.)

It would also have been apparent and obvious that the content server in Baig generates and stores "**electronic indicia**" of this association. (Schmandt, ¶95.) This is evidenced by the fact that Baig maintains a list of users whose devices are connected using the same access point IP address. For example, when the content server determines that the first device has connected using the same access point IP address as an already-connected second device, the server places both devices into a "vicinity-based" group of users. (Baig, *e.g.*, ¶0038; Provisional, 0010.) Baig explains that "[t]he server **224** includes at least one processor, memory and support circuitry for running programs that, for example, <u>identify users that are originating from a particular access point **106** and then groups those users having a common IP address to the same hotspot **110**</u>." (Baig, ¶0052; Provisional, 0012-0013.) This is shown in Figure 6 depicting webpage **600** presented on a mobile device that shows, among other things, a list **606** of users connected to the same access point:

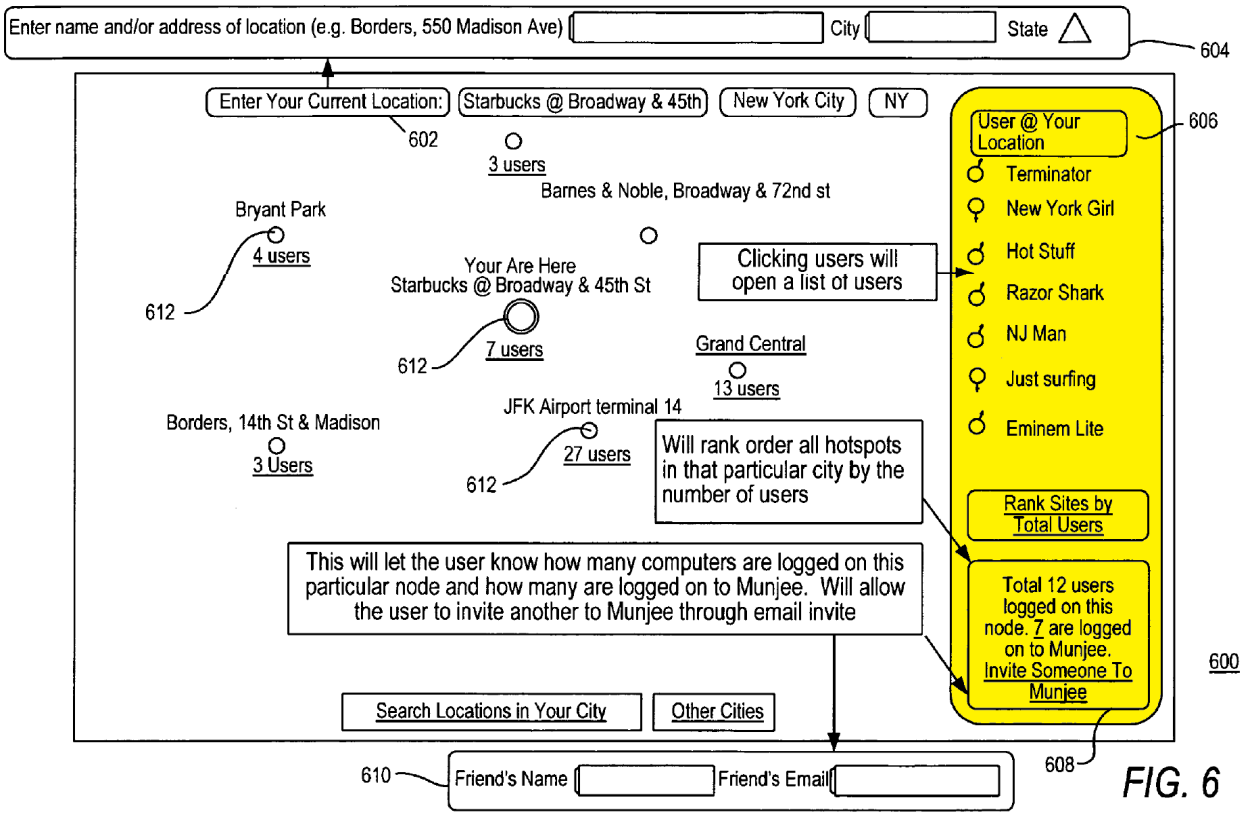


FIG. 6

(Baig, Fig. 6 (highlighting added).) The content server in Baig generates and transmits webpage **600** in Figure 6 to the mobile device. (Baig, ¶0074; Provisional, 0017.) Webpage **600** includes list **606** identifying several users whose devices were connected using the same access point/hotspot. (Baig, ¶0076; Provisional, 0018.) As noted, this means that those devices were connected using the common IP address of their access point. (Schmandt, ¶95.)

The list of users generated and stored by the content server in Baig confirms the existence of the claimed "**electronic indicia**," because the list indicates the users whose devices are connected using the common IP address – which in this example would have included at least the first device and the second device. (Schmandt,

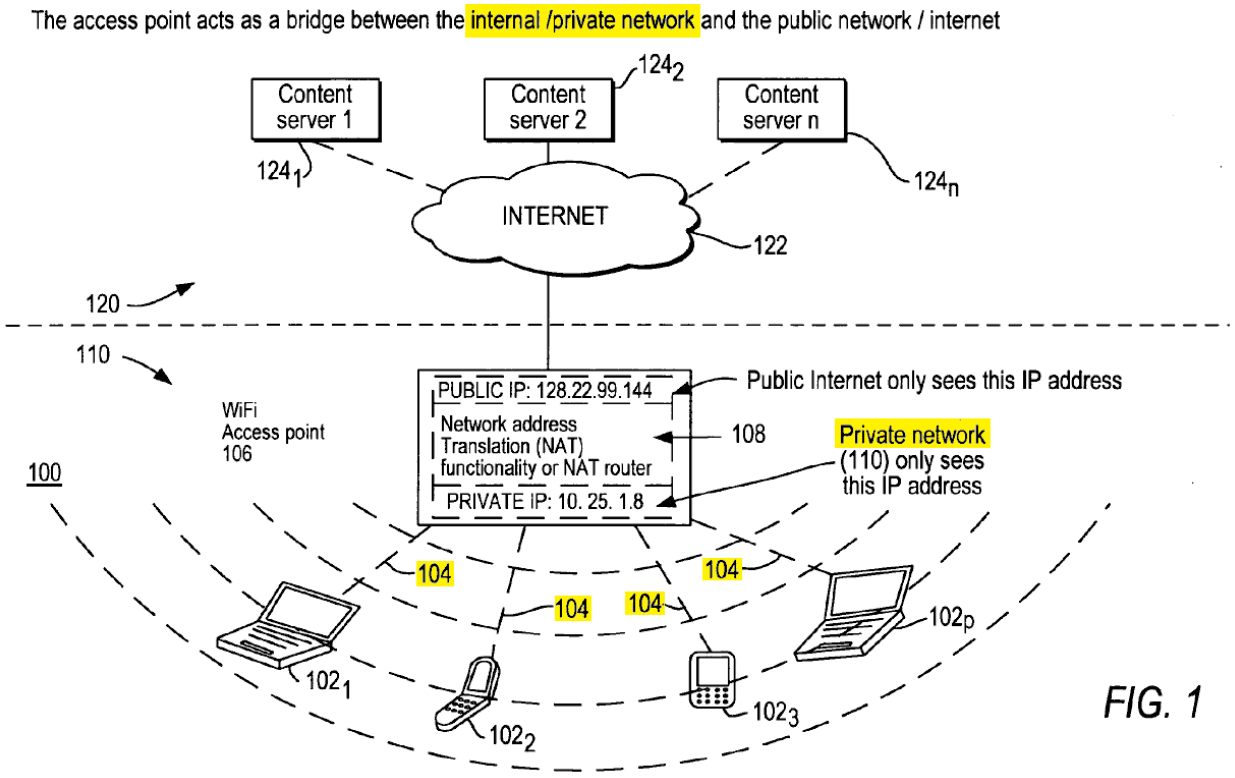
¶¶95-96.) The list thus confirms "**an association between the first device identifier and an electronic identifier of a second device**," because it associates (in a group) users connected using the same IP address. It would also have been apparent and obvious that the content server will "**generat**[e] and "**stor**[e]" such electronic indicia in order to keep track of the users that belong to a vicinity-based user group and produce list **606** in Figure 6. (Schmandt, ¶96.)[3]

This process in Baig is also performed "**automatically**" because the user did not take specific action to cause it to occur. (Schmandt, ¶98.) Step **306** from Figure 3 occurs without user action following completion of steps **302** and **304**. (Baig, Fig. 3, ¶¶0055-0056; Provisional, 0013.) In fact, Baig states that "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." (Baig, ¶0059; Provisional, 0014.) The only step here potentially involving user action is step **302** of Figure 3 in which server **224** receives the initial login request from a user. (Baig, ¶0055; Provisional, 0013.) But

[3] It is not clear from Baig how the content server *internally* formats and organizes the information it uses to generate a list of users at a hotspot. (Schmandt, ¶97.) But this is irrelevant as the claim imposes no restrictions on the implementation of the claimed "electronic indicia," and as explained in the text, Baig makes clear that the content server generates and stores such indicia. (*Id.,* ¶¶96, 97.)

this does not represent a request to perform the actual claimed step of "**generating and storing** [the] **electronic indicia**." (Schmandt, ¶98.) This is further confirmed by the '398 specification, which describes an embodiment in which the association between two device identifiers (IP addresses) is determined following user access to an online site. (Schmandt, ¶99 (citing '398, 13:42-47, 5:10-14).) This confirms that the claim does not exclude prior user action occurring earlier in the causal chain that ultimately led to performance of the claimed step.

The automatic generation of this electronic indicia was also "**based on automatically recognizing that each of the first and second devices was connected… to a common local area network**." This is because the content server in Baig, as discussed, can detect when two or more mobile devices are connected via the same access point IP address – and this in turn means that <u>those devices were connected to a common local area network</u>. (Schmandt, ¶100.) This is shown in Figure 1, which repeatedly refers to the network of devices connected to a particular hotspot or access point as forming a common private network:

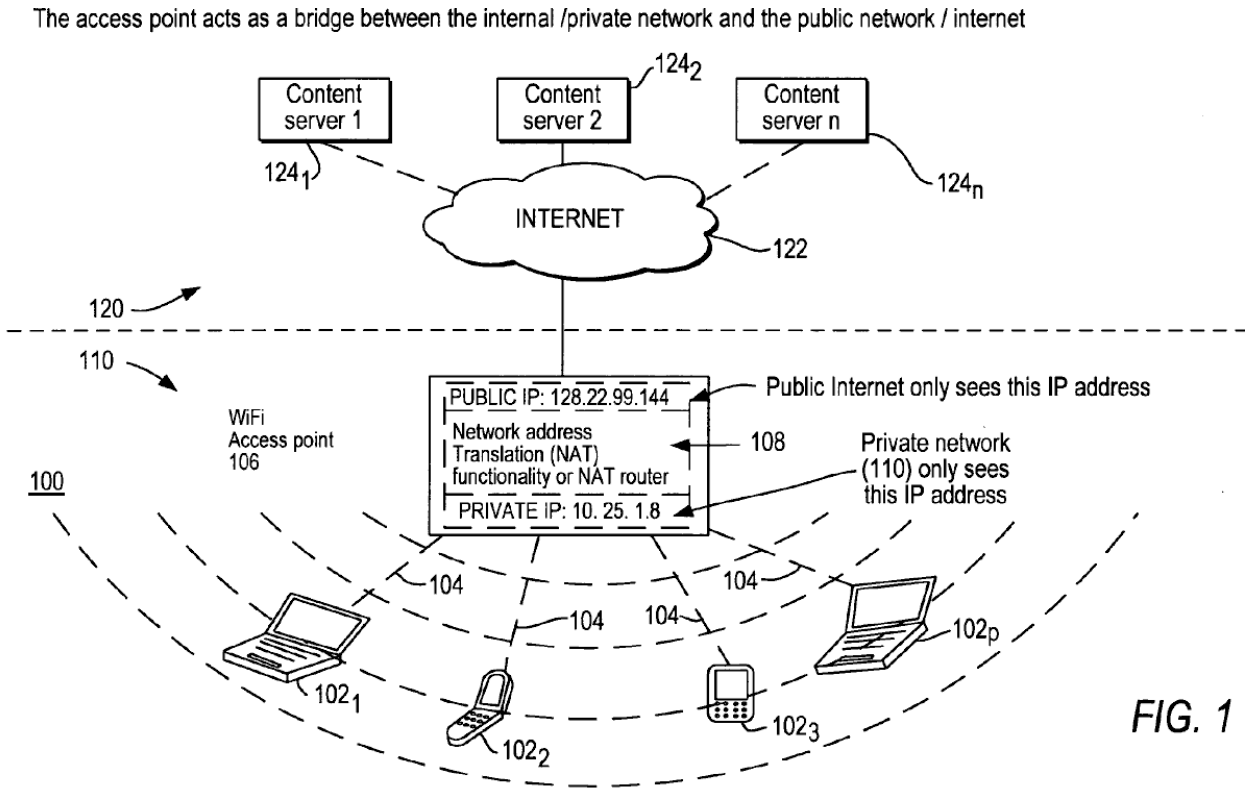


(Baig, Fig. 1 (highlighting added).) Each of the mobile devices **102** in Figure 1 is connected through a common local network **104**. (Baig, ¶0043 ("The mobile devices [in Fig. 1] **102** form a 'local network' **104** with the access point **106**…."); Provisional, 0011; Schmandt, ¶100.) Accordingly, when the content server automatically recognized that two mobile devices are connected using the same access point IP address (*see* Figure 3 (Step **306**)), it also automatically recognized that they are connected to a common local area network. (Schmandt, ¶101.)

It would also have been obvious that the first and second mobile devices in Baig were each connected "**independently of the other**" to the common local area network. (*Id.*, ¶102.) For example, each mobile device connected to the local

network has its own local or private IP address, and their connections to the network are independent. (Schmandt, ¶102; Baig, ¶0049, Fig. 2 (Step 1); Provisional, 0012, Fig. 2.) Figure 1 above, for example, does not show any links, connections, or other dependencies *between* mobile devices **102** connected to local network **104**. This is further confirmed by the fact that, as Baig expressly confirms, mobile devices need not be connected to the local network at the same time. Figure 3 of Baig, discussed, contemplates that a mobile device can wirelessly connect to a particular access point and make a login request (Steps **301-302**), after other users had <u>already</u> previously connected to that access point (Step **306**). (Baig, Fig. 3; Baig, ¶¶0055-0056; Provisional, 0013.) That mobile devices can connect at different times further confirms the independence of their respective connections. (Schmandt, ¶103.)

Finally, Baig discloses that "**wherein the computer system is connected to the local area network through the Internet but is not in the local area network**." Again referring to Figure 1, below, which shows a content server ("**the computer system**") communicating through public Internet **122** in order to connect to local network **104** through access point **106**:



(Baig, Fig. 1.)

Figure 1 above shows each content server (**124_1** through **124_n**) connected to local network **104** through Internet **122**. The Internet sits outside of local network **104**. (Baig, ¶0043; Provisional, 0011; Schmandt, ¶104.) The content server is thus "**connected to the local area network**" but "**not in the local area network**."

(c) "based on the electronic indicia of the association between the first and second device identifiers, automatically sending an electronic transmission that causes another programmed hardware computer system to take an action, based on first electronic profile data associated with the first device identifier, with respect to the second device, which is indicated at the time of the action by the second device identifier."

This final limitation is disclosed by Baig, in combination with **Hahn**.

As discussed, Baig discloses creating a vicinity-based group of users whose mobile devices are connected via the same hotspot/local area network. (Baig, *e.g.*, ¶¶0038, 0052; Provisional, 0010, 0012-0013.) After a user logs in, webpage **600** appears having list **606** of other users connected to the same hotspot:

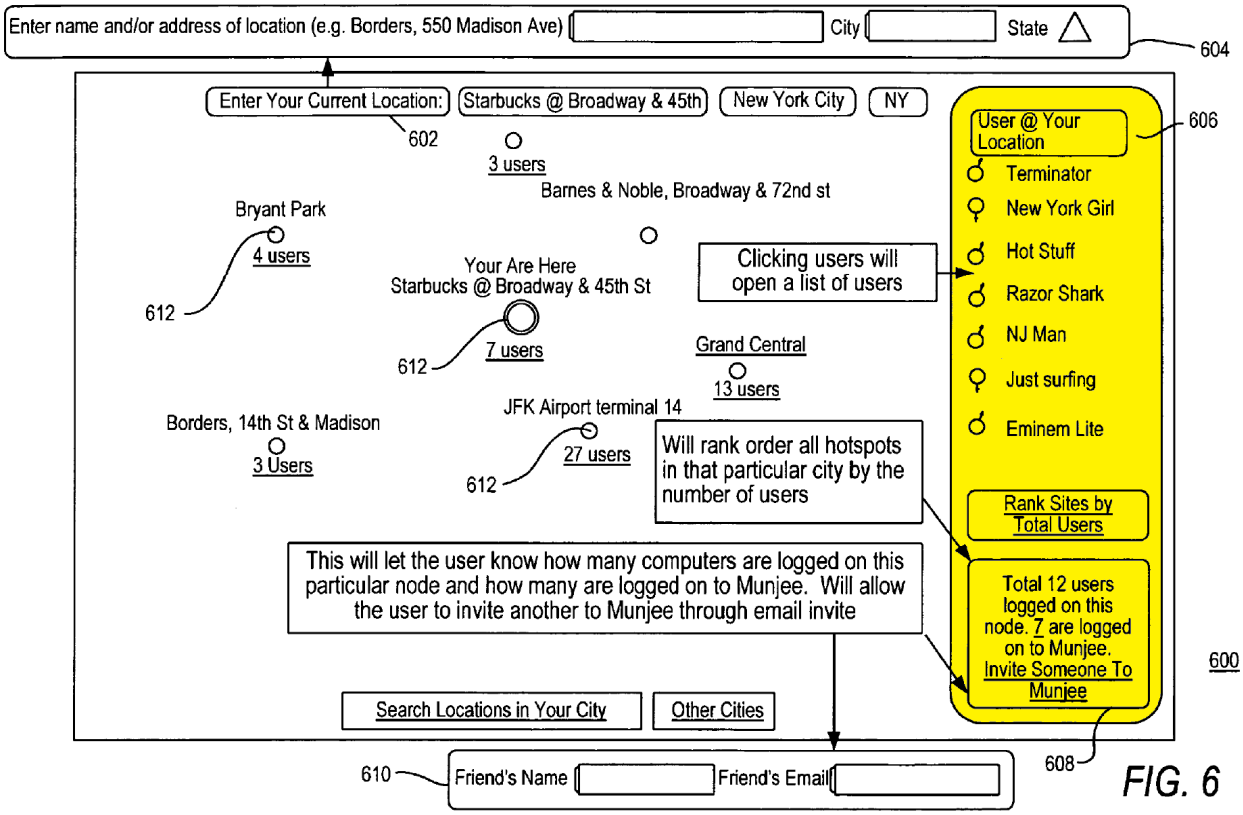
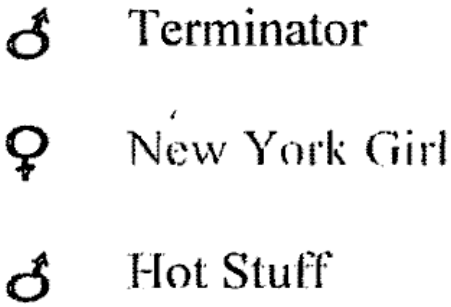


FIG. 6

(Baig, Fig. 6 (highlighting added); Baig, ¶0074; Provisional, 0017.) List **606**, as explained, lists seven other users who are logged-on (*e.g.* "Terminator," "New York Girl"), and either a male or female gender symbol next to each user. The gender symbols are visible in Figure 6 above but clearer in the Provisional (shown in part at right). (Provisional, Fig. 6.) The



list of users 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 36(c). More specifically, Baig discloses "**based on the electronic indicia of the association between the first and second device identifiers**," *i.e.* based on the list that includes the first and second users connected using the same access point IP address as explained for claim 36(b), "**sending an electronic transmission that causes another programmed hardware computer system to take an action… with respect to the second device**," *i.e.* sending list **606** to the mobile device of the second user ("**another programmed hardware computer system**"). This in turn causes the second mobile device to "**take an action**," *e.g.*, display list **606** that identifies the user logged in using the first mobile device.

Petitioner notes that claim 36 does not require that "**another programmed hardware computer system**" be a different device from the claimed "**second device**." Nevertheless, in the event it is argued by Patent Owner that claim 36 requires two physically separate devices, Petitioner has provided a separate **Ground 2** below to address this specific argument.

Turning back to claim 36(c), consider a concrete example. Suppose the user "Terminator" shown in Figure 6 connected using his mobile device (**the first**

device), and at that time, another user had previously connected via the same access point and was currently viewing the webpage of Figure 6 or Figure 7 on its mobile device (**the second device**). In this scenario, after "Terminator" logged in, the server would send the webpage to the second device ("**an electronic transmission**") including list **606**. This would have caused "**another programmed hardware computer system to take an action… with respect to the second device**," because the second device would have displayed "Terminator" on list **606** when displaying the webpage. (Baig, ¶0076 ("The web page **600** also displays a list **606** of other users at the present hotspot **110**."); Baig Provisional, 0018.)

Petitioner notes that the claim further requires "**automatically sending an electronic transmission**," and Baig is unclear as to the timing and triggering with respect to how list **606** gets updated. (Schmandt, ¶¶110, 114.) For this reason, Petitioner has cited Baig in further combination with **Hahn** for the "**automatically**" issue, discussed in further detail below.

Turning back to Baig, the webpage transmission and resulting display on the second device is also "**based on first electronic profile data associated with the first device identifier**." This is because, as explained, list **606** that was transmitted to and displayed on the second device identifies the gender of the other logged-in users. For "Terminator" using our example above, list **606** includes a gender symbol ("♂") indicating that he is male. (Baig & Provisional, Fig. 6.) The transmission and

display of list **606** to the second device is thus "**based on first electronic profile data associated with the first device identifier**," because it includes gender information ("**first electronic profile data**") of "Terminator," who has connected using the first device having the access point IP address as discussed above ("**associated with the first device identifier**"). The mapping of gender to "**profile data**" is consistent with the '398 patent, which broadly describes profile data as including "demographic or behavioral information," such as information "concerning the user's characteristics or activities." ('398, 5:65-6:2.)

Baig discloses a second way in which transmission and display of list **606** on the second device was based on first electronic profile data. Baig discloses another type of user profile data – a user's decision whether or not it wishes to be visible to other users. (Baig, *e.g.*, ¶¶0080 ("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 "**based on first electronic profile associated with the first device identifier**," because list **606** transmitted to the second device will only include "Terminator" (who is connected using access point IP address associated with the first device), if "Terminator" allowed himself to be visible to other users. (Schmandt, ¶112.) Terminator's visibility setting qualifies as "**profile data**"

because it reflects his decisions with respect to visibility to other users.

Baig also discloses taking an action with respect to the second device, "**which is indicated at the time of the action by the second device identifier**." This is because, when the webpage including list **606** is transmitted to and displayed on the device of the viewing user (**the second device**), at that point in time, the second device is identified and connected ("indicated") using the second device identifier which comprises (as discussed) the IP address of the access point. (Schmandt, ¶113.) As explained, under the proposed combination the "second device identifier" would also have included the TCP/IP port number associated with the second device.

"<u>Automatically</u> Sending An Electronic Transmission"

As mentioned, it is unclear if Baig alone discloses "**<u>automatically</u> sending an electronic transmission**." For example, consider again the scenario in which **(a)** the second device is already connected to the access point and viewing list **606** as shown in Figure 6 or Figure 7, 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 on the second device would have to be updated and sent to the second device at some point to display "Terminator" (assuming he chose to make himself visible), in order to present an accurate list of members of the vicinity-based group. (Schmandt, ¶114.) But it is unclear from Baig when or how updates to list **606** are triggered. (*Id.*, ¶115.)

But 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 in Figure 6 or Figure 7, when users are added to the access point vicinity group. This is confirmed by **Hahn** (EX1008), which describes well-known features of conventional web technologies. As Hahn explains:

> **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. As the information arrives, your browser (the web client) displays it for you. However, once the page is displayed, it does not change.
> 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, ¶¶117-118.) With respect to CLIENT PULL, Hahn explains that "the client program (your browser) is told to 'pull' information from the server without your intervention." (Hahn, p.0048.) Although the client

periodically requests a page update, the update is still "automatic" because both the client request and the server response occur without user action. (Schmandt, ¶118.) The SERVER PUSH technique is similarly automatic and, as noted, does not require a client request. (Hahn, p.0048; Schmandt, ¶118.)

Manner, Rationale, and Motivation to Combine (Baig with Hahn): It would have been obvious to adapt Baig to incorporate the automatic update techniques of Hahn, predictably resulting in the system of Baig in which the server **automatically** sends an updated or refreshed version of the webpage shown in Figure 6 and Figure 7 – which would have included a current and up-to-date list **606** of users currently connected to a hotspot – to the second device. (Schmandt, ¶119.)

Building on the scenario described above, therefore, when "Terminator" connects to the access point and logs into the website using his first device, the content server would have **automatically** sent an updated version of Figure 6 or Figure 7 – with an updated list **606** – to the second device for display. This "automatic" transmission could have been implemented using either the CLIENT PULL or SERVER PUSH techniques in Hahn. (*Id.*, ¶120.)

At the outset, Hahn is an analogous reference in the same field of the '398 patent and would have been reasonably pertinent to a number of problems facing the inventors, including how to automatically transmit information after determining

that two devices are connected to the same network. (Schmandt, ¶121.) An ordinarily skilled artisan would have been amply motivated to combine.

For example, Hahn provides an express motivation to combine 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 contents of list **606**) could have frequently changed. (Schmandt, ¶122.) The system in Baig, for example, is designed to work with locations where users commonly gather for short periods such as coffee shops or airport terminals. (Baig, *e.g.*, ¶¶0039, 0078; Provisional, 0010, 0018.) An ordinarily skilled artisan would thus have been motivated to adapt Baig to incorporate the automatic update techniques of Hahn so users have up-to-date information about users in the vicinity group. (Schmandt, ¶¶122-123.)

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, similar to the chat feature of Baig. (Hahn, pp.0048-0049, 0069; Schmandt, ¶123.) An ordinarily skilled artisan would have had more than a reasonable expectation of success and the proposed combination would have been fully enabled. (Schmandt, ¶¶124, 185, 187, 189.)

2. Claim 37: "The medium of claim 36 wherein the electronic association is recognized based on a common IP address, or portion thereof, wherein network traffic is routed via the common IP address for each of the first and second devices when each is connected to the local area network."

As explained, the content server in Baig recognizes the claimed electronic association by determining that two mobile devices are connected through the common IP address of the access point. (Baig, *e.g.*, ¶¶0038, 0052, 0056; Provisional, 0010, 0012-0013.) Baig therefore discloses that the "**electronic association is recognized based on a common IP address, or portion thereof**."

Baig further discloses that "**network traffic is routed via the common IP address for each of the first and second devices when each is connected to the local area network**." As explained for claim 36, access point **106** includes NAT router **108** that routes network traffic using the access point's public IP address, when each mobile device is connected to the local area network **104**. (Baig, ¶¶0046-0047; Provisional, 0011-0012.) The access point **106** thus uses the common IP address to route network traffic between the mobile devices and the Internet, when the mobile devices are connected to the local network. (Baig, ¶0047; Provisional, 0012; Schmandt, ¶126.)

D. Ground 2: Claims 36 and 37 Are Obvious Over Baig in View of Zwicky, Satapati, and Hahn, in Further View of Appelman

As explained for **Ground 1**, the challenged claims are obvious over Baig in view of Zwicky, Satapati, and Hahn. Petitioner has nevertheless provided Ground 2

that takes Ground 1 and adds an additional reference – **Appelman** (EX1009) for aspects of claim 36(c) to address possible arguments by Patent Owner.

First, claim 36 recites "**automatically sending an electronic transmission that causes another programmed hardware computer system to take an action… with respect to the second device**." As explained for Ground 1, nothing in claim 36 requires that the "**another programmed hardware computer system**" be different from "**the second device**." (Schmandt, ¶¶108, 127.) But in the event Patent Owner argues otherwise, the use of physically separate computing devices is amply disclosed by Appelman. The system in Appelman also sends the claimed transmission "**automatically**," and thus further renders this feature obvious.

Second, claim 36(c) recites that the claimed electronic transmission be "**based on first electronic profile data**." Ground 1 mapped this limitation to the first user's gender that can be displayed on list **606**, and/or the first user's visibility preferences. (Schmandt, ¶¶111-112.) But in the event Patent Owner argues that these features do not sufficiently disclose the use of the claimed first electronic profile data, Appelman provides a richer set of features for transmitting user information based on profile data. For all other limitations of claims 36-37, the analysis from Ground 1 applies.

Appelman, entitled "Dynamic Identification of Other Users to an Online User," discloses the ability to identify and display users with whom a user can interact. Appelman determines an "online context" for a user and then identifies

other users present within the same "online context." (Appelman, 2:27-42.) For example, Figure 6 shows a "Who's Here?" window showing other users currently viewing the same NFL sports channel:

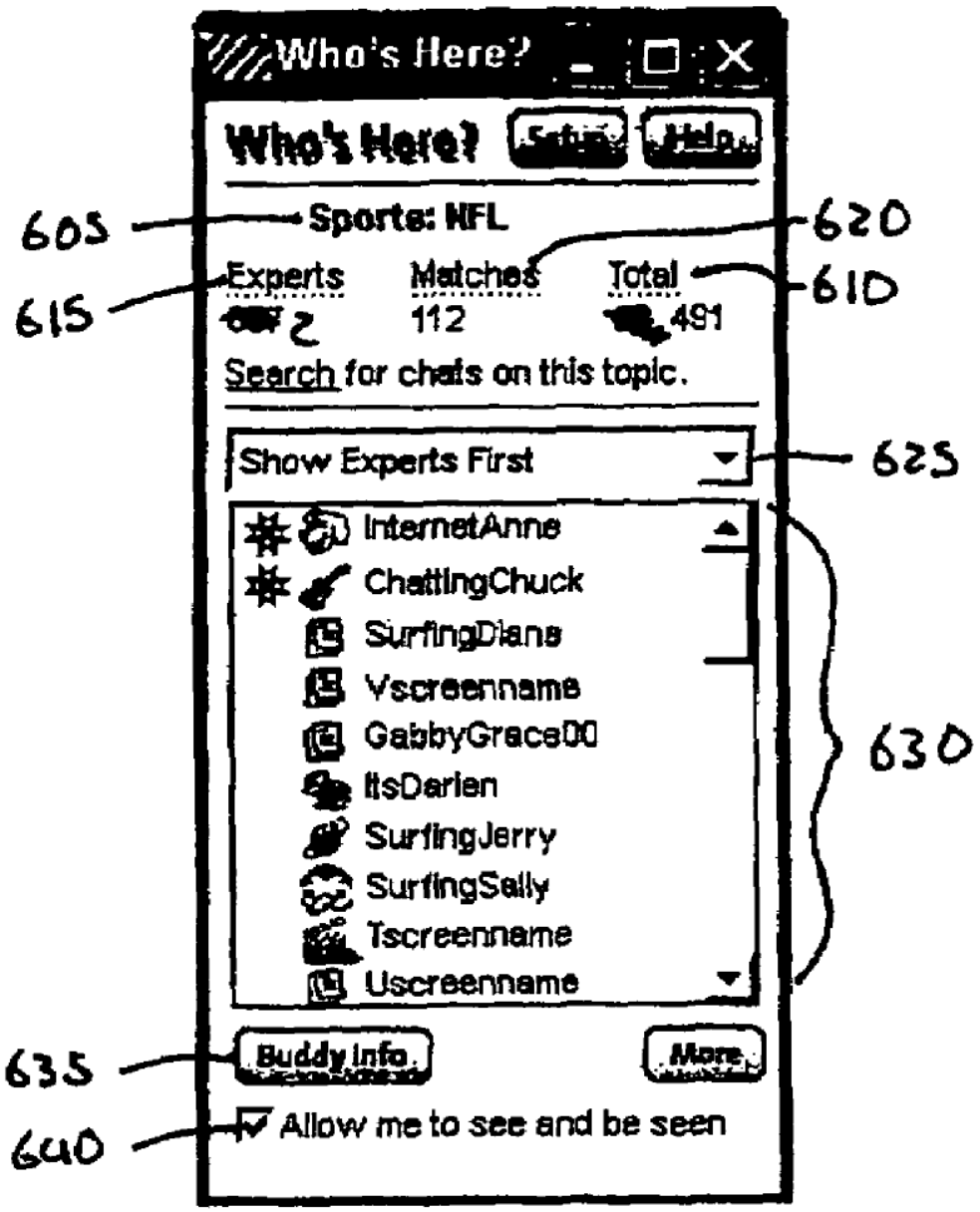


FIG. 6

(Appelman, Fig. 6; Appelman, 1:48-50, 2:6-9.) Figure 6 shows users within the online context of an NFL sports channel, but Appelman can identify users based on

a wide variety of other "online contexts," such as viewing the same web page. (Appelman, 2:30-33; *see also id.*, 1:61-63.) The "Who's Here" feature is similar to list **606** of users in Baig connected to the same hotspot and logged into the VCSP website. (Schmandt, ¶130; Baig, ¶0040, Provisional, 0010.)

Figure 3 depicts the overall system:

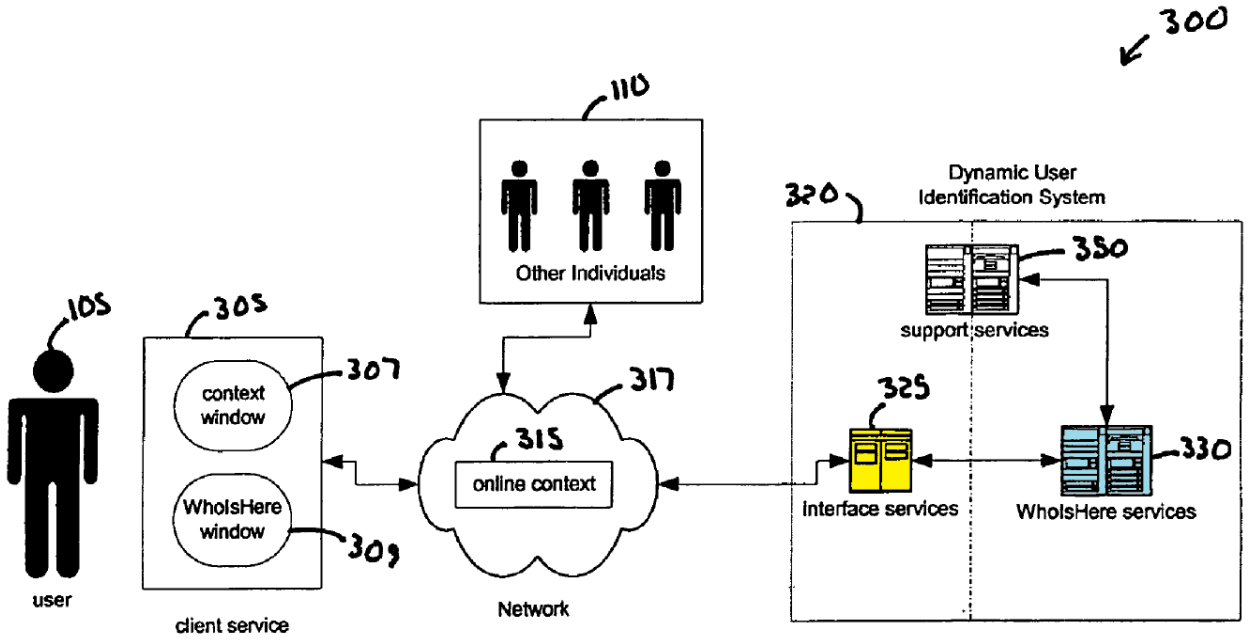


FIG. 3

(Appelman, Fig. 3 (highlighting added).) Dynamic user identification system **320** (at right) is responsible for identifying other users in the same online context and providing this information to the user. Dynamic user identification system **320** includes WhoIsHere services **330** and interface services **325**.

The WhoIsHere services **330** form part of the "back-end **323**" (Appelman 7:17-18, 7:59-62), and are responsible for "determin[ing] the other individuals **110**

presently within the online context **315** and… inform[ing] the user of at least one of the other individuals **110**." (Appelman, 7:59-62.) But WhoIsHere services **330** do not directly send this information to the user – they instead send it to interface services **325**. Interface services **325** form part of the "front-end **321**" (Appelman, 7:17-18, 29-30), and are responsible for "communicat[ing] information to the client **305** informing of one or more of the other individuals **110**," among other things. (Appelman, 7:34-37.) As Appelman explains, "[t]he WhoIsHere services **330** communicate trait, identification and/or contact information of other individuals **110** to the interfaces services **325** for suggestion to the user **105** through the client service **305**." (Appelman, 8:1-4.) In other words, (1) the WhoIsHere services **330** identify other users within the same online context as the user, and then (2) send the list of other users to support services **325**, which in turn provides those users to the user's device for display in the WhoIsHere? window. (Schmandt, ¶131.)

Appelman thus makes clear that WhoIsHere services **330** and interface services **325** can be implemented using two separate computer systems. Appelman explains that "[t]he front end **321** [which includes interface services **325**] and the back-end **323** [which includes WhoIsHere services **330**] may or may not be incorporated within the same hardware or software device, depending, for example, on an anticipated workload of the dynamic user identification system **320**." (Appelman, 7:18-22.) Appelman expressly encourages use of separate devices in

order to improve system scalability. (Appelman, 7:22-29.)

Appelman also discloses that the communication of the list to interface services **325** is done **automatically** when, for example, membership to the list changes or at a particular interval. (Appelman, *e.g.*, 8:12-22.) This is similar in many respects to the "CLIENT PULL" and "SERVER PUSH" techniques from Hahn in discussed in connection with **Ground 1**. (Schmandt, ¶132.)

Another key feature disclosed in Appelman is the ability to identify not only users within the same online context as the user, but to filter those users based on the traits or characteristics of the other users. As Appelman explains:

> For example, the user may perceive when buddy list members view a web page concurrently with the user, or may perceive when other users having a shared trait with the user (e.g., male over 35) view a web page concurrently with the user, or combination of connectivity criteria and trait matching information may be used to identify others who concurrently perceive common web pages or other contact such as television programming. The user may perceive other users based on a trait of the other users and/or based on a trait of the user.

(Appelman, 1:63-2:5.) Appelman describes a broad range of trait information that can be used to identify other users in the same online context, such as "age, gender, nationality, race, disability… and/or information indicative of an expertise, interest, preference, education… and/or other quality of the other individual **110**." (Appelman, 2:62-3:2; *see also id.*, 3:32-26.)

Rationale and Motivation to Combine (Ground 1 Prior Art with Appelman): It would have been obvious to combine the prior art for Ground 1 with Appelman, predictably resulting in the system of Baig, as discussed in connection with Ground 1, with the following additional features from Appelman: **(1)** the ability to divide the functions of the content server of Baig into separate "front-end" and "back-end" computing systems (as discussed below), and **(2)** the ability to filter the display of users on list **606** of Baig based on profile data of other users. An ordinarily skilled artisan would have been motivated to make this combination.

With respect to feature **(1)**, the combination discloses and renders obvious "**based on the electronic indicia of the association between the first and second device identifiers, automatically sending an electronic transmission that causes <u>another programmed hardware computer system</u> to take an action… with respect to <u>the second device</u>**." The proposed combination would have involved a straightforward modification to Baig – divide functions of the content server in Baig between "front-end" and "back-end" systems. The "back-end" would have performed the functions of identifying users within the same vicinity-based user group (*i.e.* users connected to the same hotspot using the same access point IP address), and then automatically sending the identification of the users to a "front-end" system ("**another programmed hardware computer system**"), as taught by Appelman. (Appelman, 8:10-19.) This would have caused the front-end, in turn, to

transmit list **606** to the mobile device of the user viewing the webpage ("**take an action… with respect to the second device**") for display on the web browser of that device. Under the proposed combination, therefore, the "**another programmed hardware computer system**" and "**the second device**" are physically separate devices. (Schmandt, ¶136.)

With respect to feature **(2)**, the combination discloses and renders obvious causing another programmed hardware computer system to take an action, "**based on first electronic profile data associated with the first device identifier**," as claimed. The proposed combination would have involved another straightforward enhancement to Baig of allowing identification of users within the vicinity-based group to be further filtered based on profile data. Using the example from **Ground 1**, the user viewing list **606** of Figure 6 or Figure 7 on its mobile device ("**the second device**") could have specified desired characteristics or traits that other users in the vicinity-based group must match before appearing on the list. For example, using the example from Appelman, the user viewing list **606** in Baig could choose to limit the list to males over 35. (Appelman, 1:63-2:5.) In combination with Baig, therefore, list **606** under the proposed combination would only show "Terminator" (the first user) if he was a male over 35. The action taken with respect to the second device, *i.e.*, the display of list **606** on the web browser, would have been "**based on first electronic profile data associated with the first device identifier**," because

the profile data of the first user (*e.g.* "Terminator") was used to determine whether or not to include him on the list. (Schmandt, ¶137.)

Appelman is an analogous reference in the same field of providing techniques for facilitating online access between devices through a network. (Schmandt, ¶138.) Appelman would also have been reasonably pertinent to a number of problems facing the inventors, including determining an online context for a user (such as being logged-in) and taking action in response to that determination and based on user profile information. (*Id.*)

An ordinarily skilled artisan would have been amply motivated to make this combination. With respect to feature **(1)**, Appelman itself provides an express motivation to adopt a separated "front-end" and "back-end" approach by explaining that it "<u>may improve the ability of the dynamic user identification system **320** to serve the many users</u> of a large scale network such as the Internet. In other words, the front-end/back-end structure <u>may improve the scalability of the dynamic user identification system **320**</u>." (Appelman, 7:22-28.) Dividing the content server into separate front-end and back-end systems would have improved performance, especially during times of increased network traffic. (Schmandt, ¶¶139-140.) A skilled artisan would also have been motivated to adapt the back-end to send the user list to the front-end "automatically," as disclosed in Appelman, to provide an up-to-date identification of connected users as fully explained in **Ground 1**.

With respect to feature **(2)**, Appelman itself provides an express motivation to use profile data by explaining that identifying users who have "a common age grouping or common demographic identifier" can provide a "more focused and relevant disclosure" to the user. (Appelman, 3:25-32.) An ordinarily skilled artisan would have been motivated to enhance Baig with this feature to allow users to focus attention on other users in the vicinity-based group who have certain desired or common characteristics. (Schmandt, ¶141.) An ordinarily skilled artisan would have had more than a reasonable expectation of success, as the proposed combination could have been implemented using conventional techniques and would have been fully enabled. (*Id.*, ¶¶142, 188-189.)

E. Ground 3: Claims 36 and 37 Are Obvious Over Baal-Haness and Appelman

1. Claim 36

The preamble recites "[**a**]**n article comprising a non-transitory tangible medium encoding computer-readable instructions that, when applied to one or more computers, instruct the one or more computers to perform a method comprising**…." The "**article**" in Baal-Haness takes the form of computer memory that stores software for carrying out the features described in Baal-Haness.

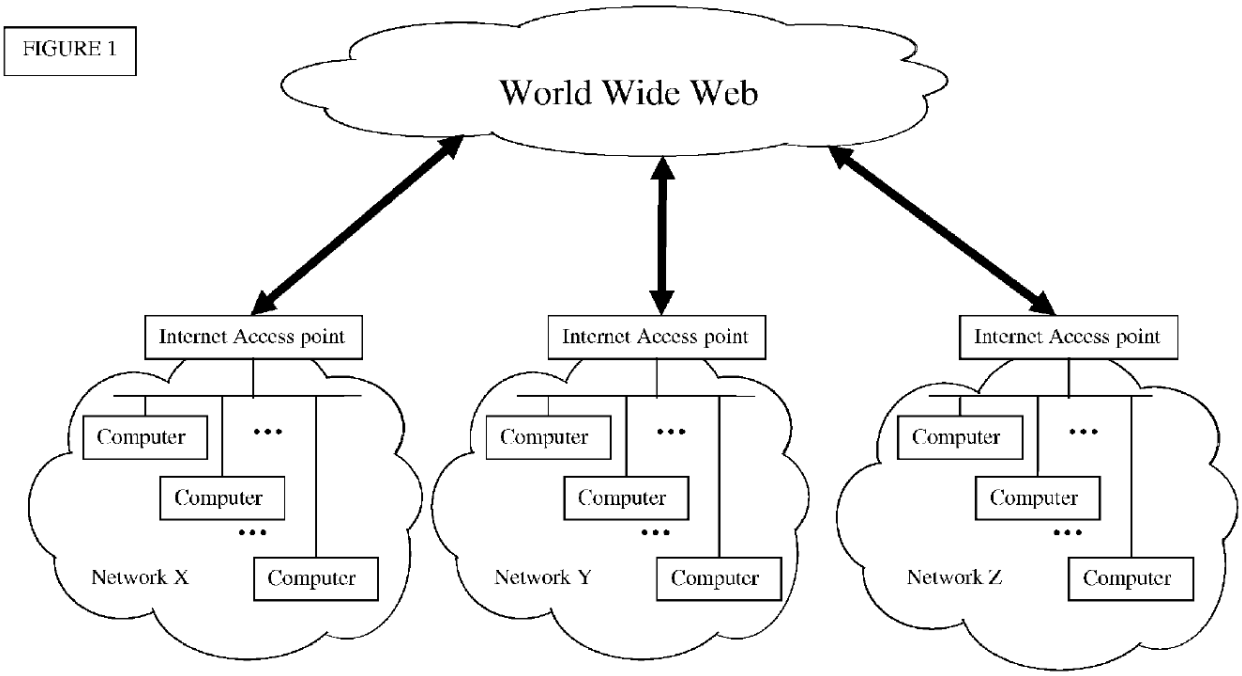
Baal-Haness discloses software for operating a website that separates users into different area networks (ANs) and provides services to users within those networks. (Baal-Haness, ¶0016 ("The main objective of the present invention is to

provide software, a business method, and an internet website….").) It would have been apparent and obvious that the website software in Baal-Haness would have included "**computer-readable instructions**." (Schmandt, ¶145.) It would have also been apparent and obvious that Baal-Haness would have included a "**non-transitory tangible medium**," *e.g.*, a memory for storing the those instructions. (*Id.*)

The "**one or more computers**" correspond to at least one server that provides the features of the website. Baal-Haness specifically refers to an "application" server that carries out the features of the website software. (Baal-Haness, ¶¶0039-0040, 0046.) Nevertheless, it would have been obvious that the website in Baal-Haness would have required at least one server. (Schmandt, ¶146.) The software running on that server, as explained in more detail below, will "**instruct the one or more computers to perform a method**," that satisfies the claimed steps below.

(a) "receiving at one or more of the computers an electronic identifier of a first device;"

As explained below, the server in Baal-Haness ("**one or more of the computers**") receives the claimed electronic identifier from a computer connected to an Internet access point. Figure 1 of Baal-Haness below depicts the connection of each computer ("**a first device**") to the World Wide Web:



(Baal-Haness, Fig. 1.) Figure 1 shows three networks, *i.e.* "**Network X**," "**Network Y**," and "**Network Z**," each containing an "**Internet Access point**" connected to computers within its respective network. Baal-Haness refers to each network as an "**area network**" (AN). (Baal-Haness, ¶¶0049-0050.) Each Internet access point, in turn, is connected to the World Wide Web as shown.

Any computer in Figure 1 discloses "**a first device**" for purposes of claim 36(a). A computer within a particular area network ("**first device**") also has an "**electronic identifier**," which for purposes of claim 36(a), takes the form of the combination of **(a)** a username associated with a user and **(b)** the network IP address of the area network (AN) to which the user is connected, as noted above.

More specifically, Baal-Haness describes a login process that "creates a database for each different LAN from which the website is used." (Baal-Haness,

¶0037.) Baal-Haness confirms that, during this process, the server receives the username and the network IP address:

> The login process creates a database for each different LAN from which the website is used. This process ensures that the services provided under the specific network will be available only to that network's users. Users on each LAN will be able to view and contact only those users that are on the same LAN.
>
> The login process and the application use the network IP address as the basis for network segmentation.
>
> In the login process:
>
> 1. The **user inserts username** or nickname
> 2. The user clicks on the login button
> 3. **The user's network IP address is automatically sent to the application** (chat room, instant messaging, etc.) **server**
> 4. If there is a database for that IP address, the username is added to that database
> 5. If there is no database for that IP address, a database is created for that IP address and the username is added to that database

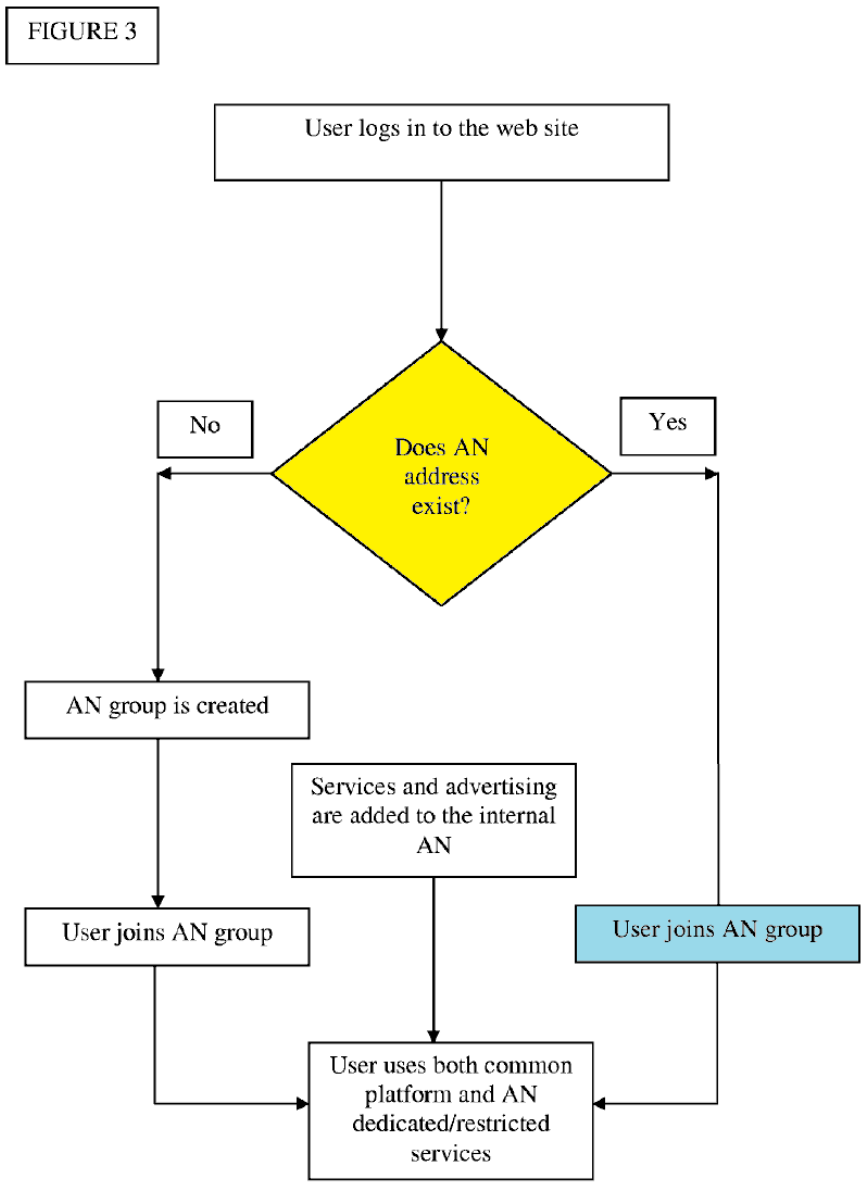
(Baal-Haness, ¶¶0037-0039.)

Baal-Haness therefore discloses "**receiving at one or more of the computers**," *i.e.*, the server, "**an electronic identifier of a first device**," an identifier that includes a username and the user's network IP address. These two pieces of information provide an "**electronic identifier of a first device**" because they identify the IP address of the local area network (LAN) to which the first device

is connected, as well as the username associated with the user operating the device. (Schmandt, ¶149.) This is consistent with the '398 patent, which specifically identifies a "username" and an "IP address" as examples of device identifiers. ('398, 15:4-8 ("Examples of such identifiers could include… a <u>username</u>… or any other identifying code or data element."), 15:13-17 ("The identifier can include the <u>IP address</u> the STB is using when in contact with the CAS….").)

(b) "automatically generating and storing electronic indicia of an association between the first device identifier and an electronic identifier of a second device based on automatically recognizing that each of the first and second devices was connected, independently of the other, to a common local area network, wherein the computer system is connected to the local area network through the Internet but is not in the local area network; and"

After receiving the login request, the server in Baal-Haness determines whether the IP address of the users' area network (AN) (part of the "**first device identifier**") already exists in the database, and if so, adds the logging-on user to that database. This is shown in Figure 3:



(Baal-Haness, Fig. 3 (highlighting added).) Figure 3 depicts a step (in yellow) in which the server checks if the IP address of the area network (AN) exists, and based on that check, can go down one of two paths. Petitioner will focus on the "Yes" path that performs a step (in blue) of adding that user to the area network (AN) group. Referring again to the discussion of the login process, Baal-Haness explains:

> <u>The login process creates a database for each different LAN from which</u>

> the website is used. This process ensures that the services provided under the specific network will be available only to that network's users. Users on each LAN will be able to view and contact only those users that are on the same LAN.
>
> The login process and the application use the network IP address as the basis for network segmentation.
>
> In the login process:
>
> 1. The user inserts username or nickname
> 2. The user clicks on the login button
> 3. The user's network IP address is automatically sent to the application (chat room, instant messaging, etc.) server
> 4. **If there is a database for that IP address, the username is added to that database**
> 5. If there is no database for that IP address, a database is created for that IP address and the username is added to that database

(Baal-Haness, ¶¶0037-0039.)

These disclosures confirm that the server performs the step of "**automatically generating and storing electronic indicia of an association between the first device identifier and an electronic identifier of a second device**," which occurs when the server (a) determines that a database for the user's network IP address already exists, and then (b) adds the username to that database. Baal-Haness repeatedly confirms that it uses the network IP address in order to identify the particular local area network to which the user belongs. (Baal-Haness, *e.g.*, ¶¶0036,

0038.) An ordinarily skilled artisan would have understood that, in the scenario outlined above in which a database for that IP address *already exists*, another user may have already logged in using the network IP address ("**an electronic identifier of a second device**"), in which case the username of the new user is simply added to the existing database rather than creating a new database. (Schmandt, ¶151; *see also* Baal-Haness, ¶¶0051 ("[E]ach user can communicate with other users on the same network…."), 0037, 0047.) Baal-Haness therefore generates and stores "**electronic indicia of an association**" between the first and second device identifiers by recording, when the first user logs in, the username of the first user in the database for the IP address to which both users are connected. This clearly creates an "**association**" between the electronic identifiers of the first and second devices because both usernames are recorded in the same database, *i.e.*, the database for their common network IP address.

This process in Baal-Haness is also performed "**automatically**" because the user did not take specific action to cause it to occur. (Schmandt, ¶152.) Adding the username to the database occurs automatically during the login process – as Baal-Haness states: "The separation between different LANs is done **automatically** and saved on the application server." (Baal-Haness, ¶0040.) Baig therefore discloses "**automatically generating and storing** [the] **electronic indicia**." The only step in the login process that potentially involves user action is the user entering a username

and pressing the login button. (Baal-Haness, ¶0039.) But these login steps do not represent a request to perform the actual step of "**generating and storing** [the] **electronic indicia**." As explained for **Ground 1**, the'398 patent does not exclude prior user action preceding the claimed step. (Schmandt, ¶¶153, 99.)

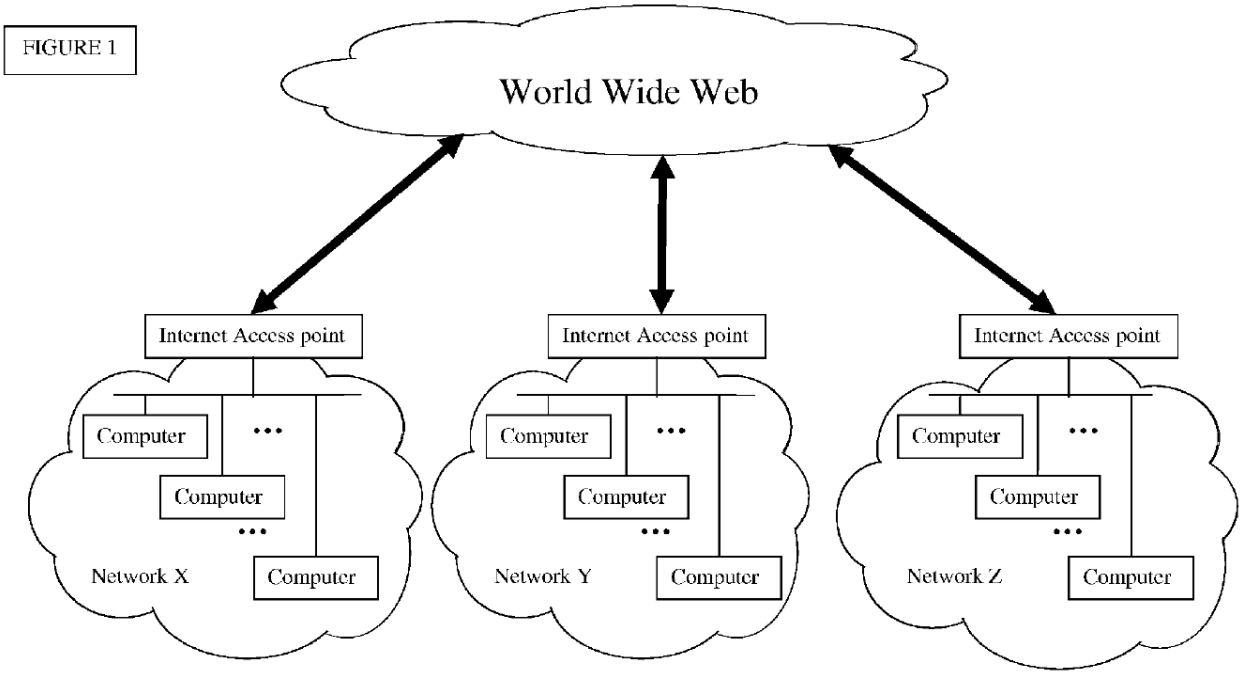
The generation of this electronic indicia was also "**based on automatically recognizing that each of the first and second devices was connected… to a common local area network**." As explained, Baal-Haness uses the network IP address to determine that two users are on the same local area network. (Baal-Haness, *e.g.*, ¶¶0030, 0035.) As Baal-Haness further explains:

> The following describes the preferred embodiment, which <u>utilizes the network IP address to achieve segmentation of users into LANs</u>.
>
> The Login Process
>
> <u>The login process creates a database for each different LAN from which the website is used</u>. This process ensures that the services provided under the specific network will be available only to that network's users. <u>Users on each LAN will be able to view and contact only those users that are on the **same LAN**</u>. ·
>
> <u>The login process and the application use the network IP address as the basis for network segmentation.</u>

(Baal-Haness, ¶¶0036-0038.) As the above makes clear, the segmentation process uses the network IP address to identify users who are all connected to the "same LAN," *i.e.*, "**a common local area network**." Accordingly, when the content server

automatically recognized that two mobile devices are connected using the same network IP address, it also automatically recognized that they are connected to a common local area network. (Schmandt, ¶154.)

It would also have been obvious that each of the first and second devices in Baal-Haness was connected "**independently of the other**" to the common local area network. (Schmandt, ¶155.) This is shown in Figure 1, which shows three area networks (ANs) and computers connected within those networks:



(Baal-Haness, Fig. 1.) Figure 1 does not show any links, connections, or other dependencies between the computers connected within a particular local area network. It therefore would have been obvious that each computer is connected "**independently of**" other computers. (Schmandt, ¶155.) This is further confirmed by the fact that, as explained above, computers in Baal-Haness need not be logged-

into the website at the same time. (*Id.*, ¶156.) The independence of these connections would also have been obvious to any ordinarily skilled artisan with a basic understanding of IP-based local area networks. (*Id.*)

Finally, Baal-Haness discloses that "**wherein the computer system is connected to the local area network through the Internet but is not in the local area network**." This is also shown in Figure 1 above, showing that computers on each network can connect (through the network's Internet access point) to the "World Wide Web," which sits outside the local area networks. It would have been apparent and obvious that the server in Baal-Haness ("**the computer system**"), which creates the website, is connected to the local area network via the World Wide Web as depicted in Figure 1. (Schmandt, ¶157.) Baal-Haness repeatedly refers to the website as an "internet website." (Baal-Haness, *e.g.*, ¶¶0028, 0016-0017.) This means that the server "**is not on the local area network**," because the Internet resides outside local area networks. (Schmandt, ¶157.)

(c) "based on the electronic indicia of the association between the first and second device identifiers, automatically sending an electronic transmission that causes another programmed hardware computer system to take an action, based on first electronic profile data associated with the first device identifier, with respect to the second device, which is indicated at the time of the action by the second device identifier."

This final limitation of claim 36 is disclosed and rendered obvious by Baal-Haness, in combination with **Appelman**.

After the user is logged in using the process in Baal-Haness discussed for claim 36(b), the user can access particular services (such as chat and instant messaging) and interact with other users who are also connected to the same local area network. (Baal-Haness, ¶¶0040-0043.) But Baal-Haness does not describe these features in detail. For this reason, Petitioner relies on Baal-Haness in combination with **Appelman**, which together render claim 36(c) obvious.

As explained in detail for **Ground 2**, **Appelman** determines an "online context" for a user and then identifies other users present with the same "online context." (Appelman, 2:27-42.) Figure 6 shows a screenshot of a "Who's Here?" feature listing other users currently viewing the same NFL sports channel:

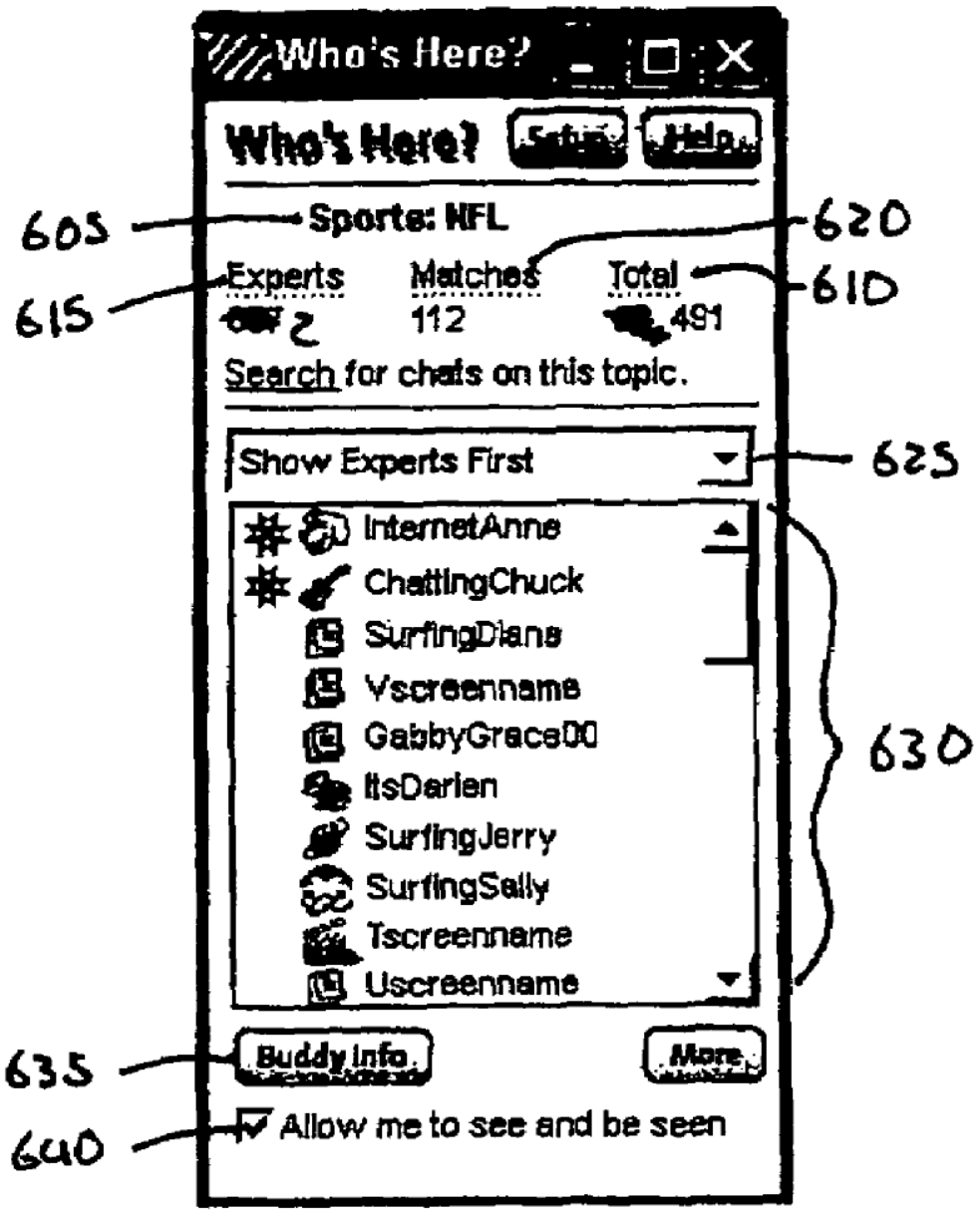


FIG. 6

(Appelman, Fig. 6.) As explained for **Ground 2**, beyond the example in Figure 6, Appelman can identify users based on a wide variety of other "online contexts" such as viewing the same web page or being present in a particular chat room. (Appelman, 2:30-33; *see also id.*, 1:61-63.) Referring again to Figure 3:

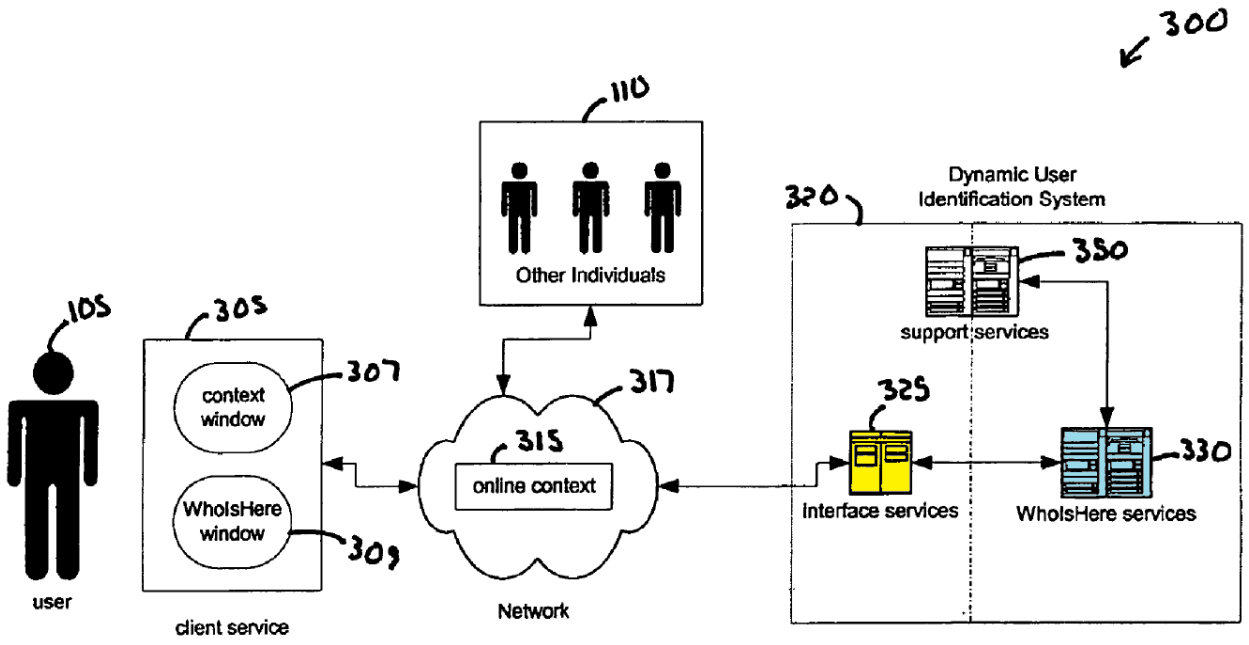


FIG. 3

(Appelman, Fig. 3 (highlighting added).) Dynamic user identification system **320** (on the right) includes WhoIsHere services **330** and interface services **325**. As discussed, WhoIsHere services **330** forms part of the "back-end **323**" (Appelman 7:17-18, 7:59-62), and is responsible for "determin[ing] the other individuals **110** presently within the online context **315** and… inform[ing] the user of at least one of the other individuals **110**." (Appelman, 7:59-62.)

But as noted, WhoIsHere services **330** do not <u>directly</u> send this information to the user – they instead rely on interface services **325**. Interface services **325** form part of the "front-end **321**" (Appelman, 7:17-18, 29-30), and are responsible for "communicat[ing] information to the client **305** informing of one or more of the other individuals **110**," among other things. (Appelman, 7:34-37, 8:1-4.) The user

at the client device, in turn, can be informed of the other users via a list, pop-up window or other means. (Appelman, 4:15-23.)

Appelman thus makes clear that WhoIsHere services **330** and interface services **325** can be implemented using two separate computer systems. Appelman explains that "[t]he front end **321** [which includes interface services **325**] and the back-end **323** [which includes WhoIsHere services **330**] <u>may or may not be incorporated within the same hardware or software device</u>, depending, for example, on an anticipated workload of the dynamic user identification system **320**." (Appelman, 7:18-22.) Appelman provides an express encouragement to use separate devices, explaining that separating the functions into front-end and back-end systems may improve the scalability of the system. (Appelman, 7:22-29.)

Appelman also discloses that the communication of the list to interface services **325** is done **automatically** when, for example, membership to the list changes or at a particular interval. (Appelman, *e.g.*, 8:12-22 ("The WhoIsHere services **330** may communicate the WholsHere list to the interface services **325** <u>**automatically**</u> after a change in the online context of the user **105** and also at any time that the WholsHere list changes. The WholsHere services **330** also may communicate the WhoIsHere list to the interface services **325** at short periodic intervals, such as, for example, every 30 or 60 seconds.").)

As explained in detail for **Ground 2**, another key feature disclosed in

Appelman is the ability to identify not only users within the same online context as the user, but to filter those users based on the traits or characteristics of the other users. (Appelman, 1:63-2:5; Schmandt, ¶165.) Appelman describes a broad range of trait information that can be used to identify other users in the same online context. (Appelman, 2:62-3:2, 3:32-26.)

Rationale and Motivation to Combine (Baal-Haness with Appelman): It would have been obvious to combine Baal-Haness with Appelman, predictably resulting in the system of Baal-Haness enhanced to include the features Appelman discussed above. Under the proposed combination, after the "**first user**" in Baal-Haness logs in and is assigned to the appropriate area network (AN), the "**second user**" connected to the same area network (AN) would have been informed of the presence of the "first user," for example by showing the first user in a list or pop-up window as disclosed in Appelman. (Appelman, 4:15-23; Schmandt, ¶166.)

The combination would thus have rendered obvious "**based on the electronic indicia of the association between the first and second device identifiers**," *i.e.*, the addition of the first user to the network IP address database for a particular area network (AN) as described in Baal-Haness, "**automatically sending an electronic transmission that causes another programmed hardware computer system to take an action… with respect to the second device**," *i.e.*, a back-end system (such as the WhoIsHere services **330** of Appelman) automatically communicating a list of

other users from the same network to a front-end system (such as interfaces services **325**) ("**another programmed hardware computer system**"), which in turn sends the list to the second device for display. (Schmandt, ¶167.)

The combination would also have rendered obvious causing another programmed hardware computer system to take an action "**based on first electronic profile data associated with the first device identifier**." This is because, as explained, Appelman allows the user list to be filtered based on profile data, such as gender or age. (Appelman, 1:63-2:5.) Under the proposed combination, therefore, the first user in Baal-Hannes would only have been displayed to the second user if the first user met the criteria specified by the second user (*e.g.* a male over the age of 35). In other words, the action taken with respect to the second device, *i.e.*, the display of at least the first user, would have been "**based on first electronic profile data associated with the first device identifier**," because profile or demographic data of the first user was used to make this determination. (Schmandt, ¶168.)

As explained previously, Appelman is an analogous reference in the same field as the '398 patent. (Schmandt, ¶138.) Baal-Haness is also analogous because it describes techniques for facilitating online access between devices through a local network and the Internet. (*Id.*, ¶169.)

An ordinarily skilled artisan would have been amply motivated to enhance Baal-Haness to allow for automatic notification of other users logged into an area

network (AN) website. As noted, Baal-Haness discloses the ability of users in an area network (AN) to participate in chat room or instant messaging exchanges. (Baal-Haness, ¶¶0041-0043; Baal-Haness, 0010-0011.) These features would have benefited from Appelman by notifying users of the area network (AN) who are available for interaction. (Schmandt, ¶170; Appelman, 4:15-23.) Appelman, as noted, confirms that it is specifically adaptable to chat room systems. (Appelman, 2:30-33 ("The online context **115** may be… [a] chat-room….").)

An ordinarily skilled artisan would have also been motivated to use demographic information of the first user ("**first electronic profile data associated with the first device identifier**") to decide whether to inform the second user of the first user's presence. As explained for **Ground 2**, Appelman provides an express motivation by explaining that identifying users who have "a common age grouping or common demographic identifier" can provide a "<u>more focused and relevant disclosure</u>" to the user. (Appelman, 3:25-32; Schmandt, ¶¶171, 141.) This is further enhanced by the fact that an area network (AN) in Baal-Haness could have included a large number of users. (Schmandt, ¶171 (citing Baal-Haness, ¶¶0044-0045).) Appelman's targeting features would have allowed a user of Baal-Haness to locate and focus its attention on other users in the area network who have common or desired characteristics. (Schmandt, ¶171.)

For the same reasons as discussed for **Ground 2**, an ordinarily skilled artisan would have been motivated to implement the server in Baal-Haness into one or more "front-end" and "back-end" computer systems, to improve efficiency and reduce performance bottlenecks. (Schmandt, ¶139.) As noted, Appelman itself provides an express motivation to adopt such an architecture. (Appelman, 7:22-28.) And as explained for **Ground 2**, a skilled artisan would also have been motivated to adapt the back-end to send the user list to the front-end "automatically," as disclosed in Appelman, to provide a current identification of connected users. An ordinarily skilled artisan would have had more than a reasonable expectation of success, as explained. (Schmandt, ¶¶173, 142.)

2. Claim 37: "The medium of claim 36 wherein the electronic association is recognized based on a common IP address, or portion thereof, wherein network traffic is routed via the common IP address for each of the first and second devices when each is connected to the local area network."

As explained, the content server in Baal-Haness recognizes the claimed electronic association based on two or more computers having the IP address associated a particular area network (AN). (Baal-Haness, Fig. 3 ("Does AN address exist?...Yes…User joins AN group…"), ¶0039 ("3. The user's network IP address is automatically sent to the application… server [;] 4. If there is a database for that IP address, the username is added to that database.").) The server in Baal-Haness, in other words, creates the claimed electronic association by storing the usernames

associated with the first and second devices in the common database assigned to the network IP address used by both devices. It thus would have been apparent and obvious that, in order to store the usernames in the same database based on a particular network IP address, the two devices would have been using the same network IP address. The electronic association would thus have been "**recognized based on a common IP address, or portion thereof**." (Schmandt, ¶175.)

Claim 37 continues by reciting that "**network traffic is routed via the common IP address for each of the first and second devices when each is connected to the local area network**," which adds nothing of patentable significance. In any IP-based network (such as the Internet used in Baal-Haness), devices communicate with remote servers over the internet using their IP addresses. (Schmandt, ¶175.) Baal-Haness states, for example, that when a computer connects to the website, "[t]he user's network IP address is automatically sent to the application… server." (Baal-Haness, ¶0039 (step 3).) It thus would have been obvious to an ordinarily skilled artisan that network traffic is routed to computers within an area network "**via the common IP address for each of the first and second devices**." This routing obviously also occurs "**when each device is connected to the local area network**," because the computers have to be connected to the local area network (*see* Baal-Haness, Fig. 1) in order to initiate and receive network traffic with the website over the Internet. (Schmandt, ¶175.)

F. Ground 4: Claim 37 Is Obvious Over Baal-Haness and Appelman, in Further View of Zwicky and Satapati

As just discussed, it would have been apparent and obvious based on Baal-Haness that the claimed "**electronic association**" is "**recognized based on a common IP address, or portion thereof**," as recited in claim 37. But Baal-Haness does not provide specific and concrete examples of IP addresses. It is thus possible that Patent Owner may attempt to speculate that the network IP addresses used by the computers in Baal-Haness are not the same, and thus, the association is not "**based on a common IP address, or portion thereof**."

Petitioner has therefore provided this **Ground 4**, which combines Baal-Haness with the network address translation (NAT) teachings of **Zwicky** (EX1006) and **Satapati** (EX1007), to address any such argument and provide another basis for finding claim 37 obvious. As explained for claim 36(a) of **Ground 1** (**Part VI.C.1(a)**), these references discuss standard NAT techniques.

As discussed, packets sent over the Internet using TCP/IP include not only an **IP address** of the source and destination devices, but also a source and destination **port number**. A technique known as "port translation" use this port number to allow multiple devices to share a common network IP address. This is graphically depicted in Figure 5-4 of Zwicky:

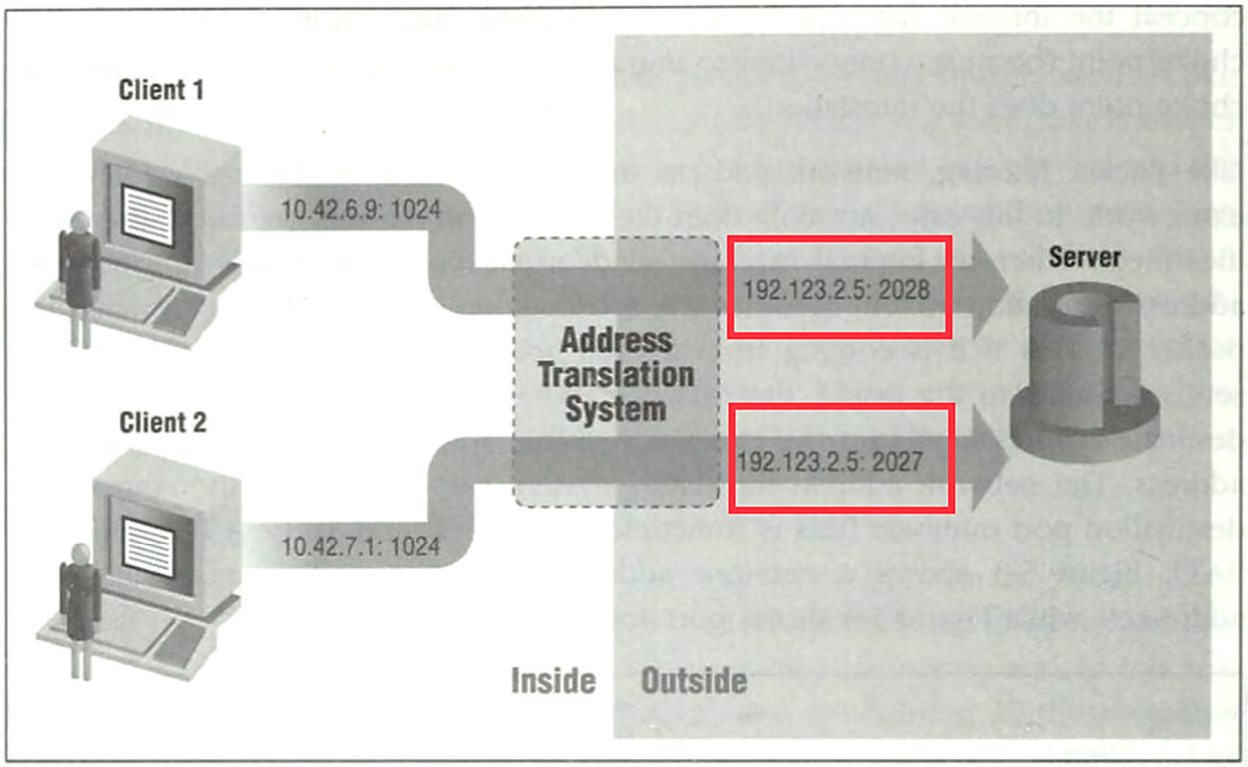


Figure 5-4. Port and address translation

(Zwicky, Fig. 5-4, p.0038 (red annotation added).) Figure 5-4 shows Client 1 and Client 2 inside a local network with locally-assigned IP addresses (*i.e.*, 10.42.6.9 and 10.42.7.1). As explained, Figure 5-4 shows an "Address Translation System" that, like the "Internet Access point" in Figure 1 of Baal-Haness, sits between the clients and a remote server and replaces the local IP addresses for both Client 1 and Client 2 with the same IP address (*i.e.*, 192.123.2.5). The Address Translation System also assigns distinct TCP/IP **port numbers** to these computers (2028 for Client 1 and 2027 for Client 2) to differentiate them, as explained. As explained in the Background of Satapati, "NAT may use port address translation, where port numbers are used to further identify devices with the **same address**." (Satapati, 1:34-36.)

These port numbers can then be used to translate between the common IP addresses of incoming and outgoing packets and local addresses to route packets between local network devices and outside servers. (Satapati, 2:4-58.)

Zwicky and Satapati therefore disclose two devices having "**a common IP address, or portion thereof**," and further disclose that "**network traffic is routed via** [a] **common IP address for each of** [a] **first and second devices when each is connected to** [a] **local area network**," as recited in claim 37.

Rationale and Motivation to Combine (Ground 3 Art with Zwicky and Satapati): It would have been obvious to combine Baal-Haness with the port translation teachings of Zwicky and Satapati, predictably resulting in the system of Baal-Haness in which two computers within the local area network, when communicating over the Internet, provided the <u>same</u> network IP address to the server. This would have predictably resulted in the "**electronic association**" generated by the server in Baal-Haness being "**recognized based on a common IP address, or portion thereof**," as recited in claim 37. And because the common IP address was being used to communicate with the server over the Internet, "**network traffic** [would have been] **routed via the common IP address for each of the first and second devices when each is connected to the local area network**," as the common IP address would have been used to route communications between the computers in Baal-Haness and the server when the computers are connected to the

network. (Schmandt, ¶180.) As explained, Baal-Haness, Zwicky and Satapati are analogous references. (*Id.*, ¶¶181, 87.)

Baal-Haness itself suggests this combination by repeatedly referring to the IP address received by the application server as a "network IP address," indicating that the IP address pertains to the network itself, not a particular computer on that network. This is shown by Figure 3, in which the following check is performed after the user logs into the website: "Does AN address exist?" (Baal-Haness, Fig. 3; *see also* Baal-Haness, ¶¶0037 ("The login process creates a database for each different LAN [local area network] from which the website is used."), 0039 ("The user's network IP address is automatically sent to the application… server… [i]f there is a database for that IP address, the username is added to that database.").) An ordinarily skilled artisan would thus have been motivated to use the port translation techniques of Zwicky and Satapati in order to differentiate computers within an area network (AN) that will use the common network IP address. (Schmandt, ¶182; *see also* Satapati, 1:34-36.) As noted for **Ground 1**, port translation would have enabled the system of Baal-Haness to more easily differentiate and properly route traffic to and from computers when communicating over the Internet through the common network IP address. (Schmandt, ¶¶182, 89.) Moreover, port translation as discussed in Zwicky and Satapati was a well-known and industry-standard practice for

allowing multiple devices connected to a local network to communicate over the Internet. (*Id.*, ¶182.)

The motivations to combine articulated for **Ground 1** also apply here. As explained, Zwicky itself provides several motivations to use NAT and port translation, including economizing IP address space and security benefits. (Schmandt, ¶¶183, 90 (citing Zwicky, p.0038).) An ordinarily skilled artisan would have had a reasonable expectation of success. (*Id.*, ¶¶184, 92, 186.)

VII. CONCLUSION

Petitioner respectfully requests IPR institution.

Dated: March 28, 2022

Respectfully submitted,

COOLEY LLP
ATTN: Patent Group
1299 Pennsylvania Avenue NW
Suite 700
Washington, DC 20004
Tel: (650) 843-5001
Fax: (650) 849-7400

By: */ Heidi L. Keefe /*
Heidi L. Keefe
Reg. No. 40,673
Counsel for Petitioner

CERTIFICATE OF COMPLIANCE WITH WORD COUNT

Pursuant to 37 C.F.R. § 42.24(d), I certify that this petition complies with the type-volume limits of 37 C.F.R. § 42.24(a)(1)(i) because it contains 13,858 words, according to the word-processing system used to prepare this petition, excluding the parts of this petition that are exempted by 37 C.F.R. § 42.24(a) (including the table of contents, a table of authorities, mandatory notices, a certificate of service or this certificate word count, appendix of exhibits, and claim listings).

DATED: March 28, 2022

COOLEY LLP
ATTN: Patent Docketing
1299 Pennsylvania Avenue NW
Suite 700
Washington, D.C. 20004
Tel: (650) 843-5001
Fax: (650) 849-7400

/ Heidi L. Keefe /
Heidi L. Keefe
Reg. No. 40,673

CERTIFICATE OF SERVICE

I hereby certify, pursuant to 37 C.F.R. Sections 42.6 and 42.105, that a complete copy of the attached **PETITION FOR INTER PARTES REVIEW OF U.S. PATENT NO. 8,677,398 B2,** including all exhibits (**Nos. 1001-1016**) and related documents, are being served via Federal Express on the 28th day of March, 2022, the same day as the filing of the above-identified document in the United States Patent and Trademark Office/Patent Trial and Appeal Board, upon Patent Owner by serving the correspondence address of record with the USPTO as follows:

Intent IQ, LLC
37-18 Northern Boulevard
Suite 404
Long Island City, NY 11101

And, via Federal Express upon counsel of record for Patent Owner in the litigation pending before the U.S. District Court for the Western District of Texas entitled *AlmondNet, Inc. and Intent IQ, LLC v. Meta Platforms, Inc.*, Case No. 6:21-cv-00896-ADA (W.D. Tex.) as follows:

Reza Mirzaie
Russ August & Kabat
12424 Wilshire Blvd., 12th Floor
Los Angeles, CA 90025
310-826-7474
Fax: 310-826-6991
Email: rmirzaie@raklaw.com

DATED: March 28, 2022

/ Heidi L. Keefe /
Heidi L. Keefe
Reg. No. 40,673
COOLEY LLP
1299 Pennsylvania Ave. NW, Suite 700
Washington, D.C. 20004
Tel: (650) 843-5001

Trials@uspto.gov
571-272-7822

Paper No. 6
Entered: October 21, 2022

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

META PLATFORMS, INC.,
Petitioner,

v.

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

IPR2022-00773
Patent 8,677,398 B2

Before KRISTEN L. DROESCH, THOMAS L. GIANNETTI, and STACEY G. WHITE, *Administrative Patent Judges.*

DROESCH, *Administrative Patent Judge*.

DECISION
Institution of *Inter Partes* Review
35 U.S.C. § 314

I. INTRODUCTION

A. Background

Meta Platforms, Inc. ("Petitioner") filed a Petition requesting *inter partes* review ("IPR") of claims 36 and 37 of U.S. Patent No. 8,677,398 B2 (Ex. 1001, "'398 Patent"). Paper 2 ("Pet."). Petitioner filed a Declaration of Christopher M. Schmandt with its Petition. Ex. 1002. AlmondNet Inc. and Intent IQ, LLC (collectively "Patent Owner") did not file a preliminary response.

We have authority to determine whether to institute review under 35 U.S.C. § 314 and 37 C.F.R. § 42.4(a). An *inter partes* review may not be instituted unless it is determined that "the information presented in the petition filed under section 311 and any response filed under section 313 shows that there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition." 35 U.S.C. § 314(a).

For the reasons provided below, we determine, based on the record before us, there is a reasonable likelihood Petitioner would prevail in showing at least one of the challenged claims is unpatentable.

B. Related Matters

The parties indicate the '398 Patent is or was the subject of the following proceedings:

AlmondNet, Inc., v. Oath Holdings Inc., 1–19-cv-00247 (D. Del.);
Roku, Inc. v. AlmondNet, Inc., 1:21-cv-01035 (D. Del.);
AlmondNet, Inc., v. Roku, Inc., 6:21-cv-00731 (W.D. Tex.);
AlmondNet, Inc., v. Samsung Elecs. Co., 6:21-cv-00891 (W.D. Tex.);
AlmondNet, Inc., v. Facebook, Inc., 6:21-cv-00896 (W.D. Tex.);

AlmondNet, Inc., v. Microsoft Corp., 6:21-cv-00897 (W.D. Tex.); *AlmondNet, Inc., v. Amazon.com, Inc.*, 6:21-cv-00898 (W.D. Tex.); Pet. 1; Paper 4, 1.

Petitioner also indicates that the '398 Patent was the subject of *Yahoo! Inc. v. Intent IQ, LLC*, Case No. IPR2017-01299, in which institution was denied. Pet. 1.

C. The '398 Patent (Ex. 1001)

The '398 Patent discloses a method for delivering targeted television advertisements based on online behavior. *See* Ex. 1001, Abstract.

Figure 7 of the '398 Patent is reproduced below:

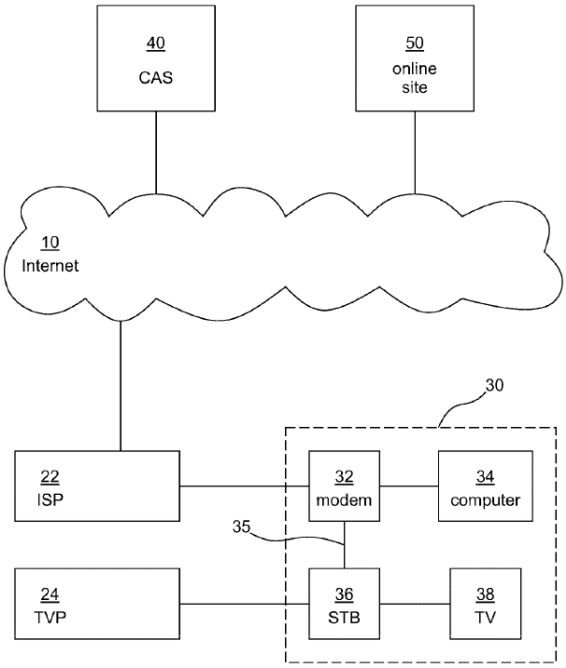


Figure 7 depicts central ad server (CAS) 40 and online site 50 connected to Internet 10, modem 32 connected to Internet service provider (ISP), computer 34 and set-top box (STB) 36, and TV 38 connected to STB 36 and television provider (TVP) 24. *See* Ex. 1001, 12:47–13:21. An identifier can be assigned to STB 36, such as an equipment serial number, a device MAC address, a username, a pseudonym, a tag, or other identifying code or data

element, and may include the IP address STB 36 is using when in contact with CAS 40. *See id*. at 15:1–14.

> Once a STB is confirmed to have been using a certain IP address at a certain date and time (for example by having a uniquely tagged STB consecutively communicate with the CAS using the same IP address . . .), the CAS database can be searched to find all computers, mobile devices, and other STBs that used the same IP address at the same date and time, and those will be assumed to be devices that are part of the same household and same LAN. Then, an association or link is created among the devices, by linking the device identifiers or tags with the STB's identifier in the CAS database . . . .
>
> Once the association is created, profile information (both behavioral and demographic) collected about the computers and mobile devices before and after the association was created could be used to target ads to the STB, regardless of the IP addresses used by the computers and mobile devices (such as cell phones) to access the web at the time the profiles were collected.

Ex. 1001, 18:24–50.

D. Illustrative Claim

Claim 36 is independent, and claim 37 depends therefrom. *See* Ex. 1001, 26:57–27:15. Claim 36 is illustrative and reproduced below.

> An article comprising a non-transitory tangible medium encoding computer-readable instructions that, when applied to one or more computers, instruct the one or more computers to perform a method comprising:
>
> (a) receiving at one or more of the computers an electronic identifier of a first device;
>
> (b) automatically generating and storing electronic indicia of an association between the first device identifier and an electronic identifier of a second device based on automatically recognizing that each of the first and second devices was connected, independently of the other, to a common local area network, wherein the computer system is connected to the local area network

through the Internet but is not in the local area network; and

(c) based on the electronic indicia of the association between the first and second device identifiers, automatically sending an electronic transmission that causes another programmed hardware computer system to take an action, based on first electronic profile data associated with the first device identifier, with respect to the second device, which is indicated at the time of the action by the second device identifier.

Ex. 1001, 26:57–27:11.

E. Asserted Challenges to Patentability and Asserted Prior Art

Petitioner asserts that claims 36 and 37 would have been unpatentable based on the following grounds (Pet. 3):

Claim(s) Challenged	35 U.S.C. §	Reference(s)/Basis
36, 37	103(a)[1]	Baig[2], Zwicky[3], Satapati[4], Hahn[5]
36, 37	103(a)	Baig, Zwicky, Satapati, Hahn, Appelman[6]
36, 37	103(a)	Baal-Haness[7] and Appelman
36, 37	103(a)	Baal-Haness, Appelman, Zwicky, Satapati

[1] The Leahy-Smith America Invents Act, Pub. L. No. 112-29, 125 Stat. 284 (2011), amended 35 U.S.C. §§ 102 and103 effective March 16, 2013. Because the '398 Patent has a filing date prior to the effective date of the applicable AIA amendment, we refer to the pre-AIA versions of §§ 102 and 103.

[2] US 2008/0113674 A1, published May 15, 2008 (Ex. 1003).

[3] Building Internet Firewalls, Elizabeth D. Zwicky et al., 2000 (Ex. 1006).

[4] US 7,356,045 B2, issued Apr. 8, 2008 (Ex. 1007).

[5] Internet Complete Reference, Harley Hahn, 1996 (Ex. 1008).

[6] US 7,899,862 B2, issued Mar. 1, 2011 (Ex. 1009).

[7] US 2007/0067459 A1, published March 22, 2007 (Ex. 1010).

II. ANALYSIS

A. Claim Construction

In an *inter partes* review proceeding, the Board applies the same claim construction standard as applied in federal courts in a civil action under 35 U.S.C. § 282(b), which is generally referred to as the *Phillips* standard. *See* 37 C.F.R. § 42.100(b); *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc). Under the *Phillips* standard, "words of a claim 'are generally given their ordinary and customary meaning.'" *Phillips*, 415 F.3d at 1312.

Petitioner asserts that it "does not believe an express claim construction is necessary at this stage of the proceeding." Pet. 7. As demonstrated in the analysis below, at this stage of the proceeding, we need not construe any claim terms and phrases. *See, e.g.*, *Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) ("[W]e need only construe terms 'that are in controversy, and only to the extent necessary to resolve the controversy.'" (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999))).

B. The Level of Ordinary Skill in the Art

Petitioner asserts:

> [a] person of ordinary skill in the art as of April 17, 2007 (the earliest priority date for the '398 patent) would have possessed at least 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). A person could also have qualified with more formal education and less technical experience, or vice versa.

Pet. 4–5 (citing Ex. 1002 ¶¶ 10–14). For the purpose of institution, we adopt Petitioner's definition of a person of ordinary skill in the art because it is consistent with the level of skill reflected by the '398 Patent Specification and the asserted prior art.

C. Principles of Law

A claim is unpatentable under 35 U.S.C. § 103 if the differences between the claimed subject matter and the prior art are such that the subject matter, as a whole, would have been obvious at the time the invention was made to a person having ordinary skill in the art to which the subject matter pertains. *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). The question of obviousness is resolved on the basis of underlying factual determinations, including: (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of skill in the art; and (4) if in evidence, so-called secondary considerations. *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).[8]

D. Challenge to Claims 36 and 37 over Baig, Zwicky, Satapati, and Hahn

1. Overview of Baig (Ex. 1003)

Baig is directed to an apparatus and method for providing services for mobile devices which are in communication with local area network wireless access points. *See* Ex. 1003 ¶ 2.

[8] Petitioner does not present evidence related to secondary considerations.

Figure 1 of Baig is reproduced below.

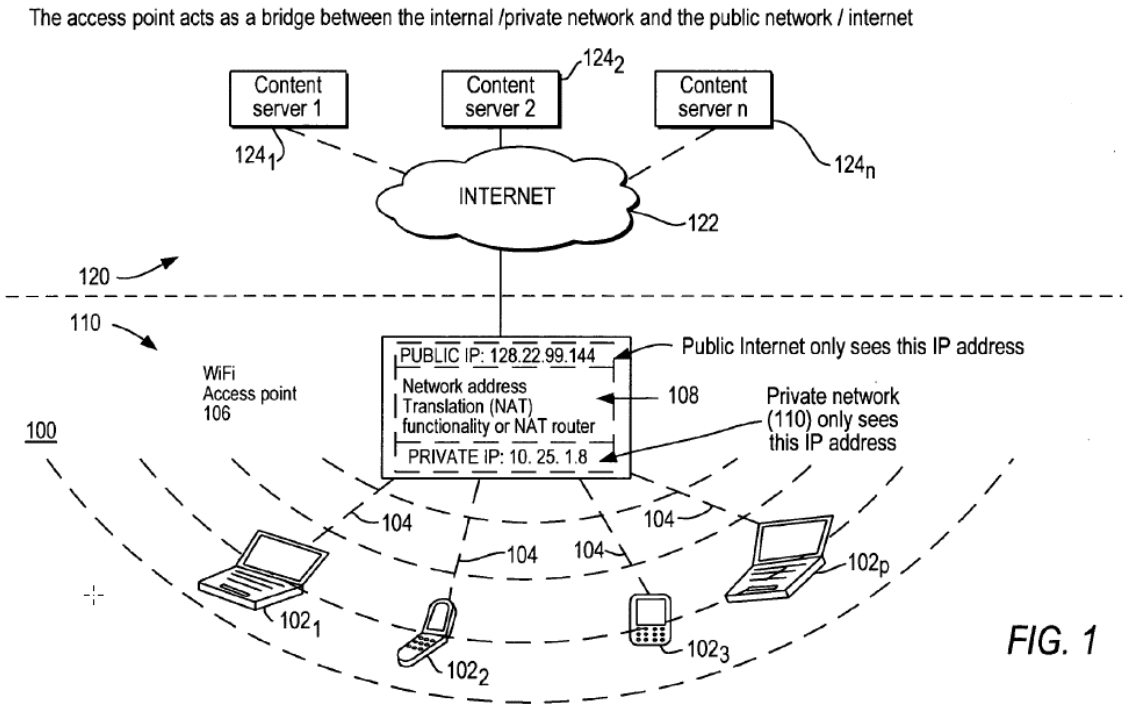


Figure 1 depicts a block diagram of communications network 100 including public wireless hotspot 110 communicatively coupled to public network 120 via access point 106. *See* Ex. 1003 ¶¶ 13, 42. Public network 120 includes content servers 124_1, 124_2, 124_n that store and host information from websites. *See id.* ¶ 42. WiFi hotspot 110 enables at least one mobile device 102_1 through 102_p to communicate over local private network 104 and communicate with content servers 124_1, 124_2, 124_n over Internet 122. *See id.* ¶ 43.

Access point 106 includes a network address translation (NAT). router 108 that provides network address translation. *See* Ex. 1003 ¶ 43. Access point 106 utilizes a unique public IP address which relays data between public network 120 and wireless mobile devices 102 connected to local private wireless network 104. *See id.* ¶¶ 44–45. When mobile device 102 requests information from public network 120, it sends data

packets containing a local IP address to access point 106. *See id.* ¶ 45. All devices on local private network 104 use local IP addresses that are not visible to public networks. *See id.* Access point 106 interacts with public network 120 with a public IP address, which is visible to all devices on public internet 122. *See id.* Access point 106, which includes NAT router 108, replaces the local IP address with its own public IP address and forwards the packets to content server 124 on public network 120. *See id.* ¶¶ 46, 51. When public network 120 sends packetized information back to requesting mobile device 102, NAT router 108 replaces the public IP address with the local IP address for mobile device 102 and routs the packetized information to the requesting mobile device 102. *See id.* ¶ 51.

Baig also discloses a vicinity-based community service provider (VCSP) having at least one content server that discovers wireless users within physical vicinity of each other at a WiFi hotspot. *See* Ex. 1003 ¶¶ 38, 52. The VCSP content server includes programs and data for hosting a VCSP website. *See id.* ¶ 53. The VCSP server receives a login request from a user that is connected to a particular WiFi access point (hotspot), identifies the unique IP address of each WiFi access point, and identifies all users who have logged in from a common hotpot as having the same access point IP address, and forms a vicinity-based user group at each hotspot. *See id.* ¶¶ 38, 52, 55–59, Fig. 3. When a user at a hotspot logs onto the VCSP website, the user automatically becomes part of the vicinity-based user group, and then can access VCSP webpages to participate in or receive an offered service and communicate with other VCSP users via a chat room. *See id.* ¶ 59. Once the user logs into the VCSP website, the server presents a webpage to the user on his or her mobile device. *See id.* ¶ 74.

Figure 6 of Baig is reproduced below.

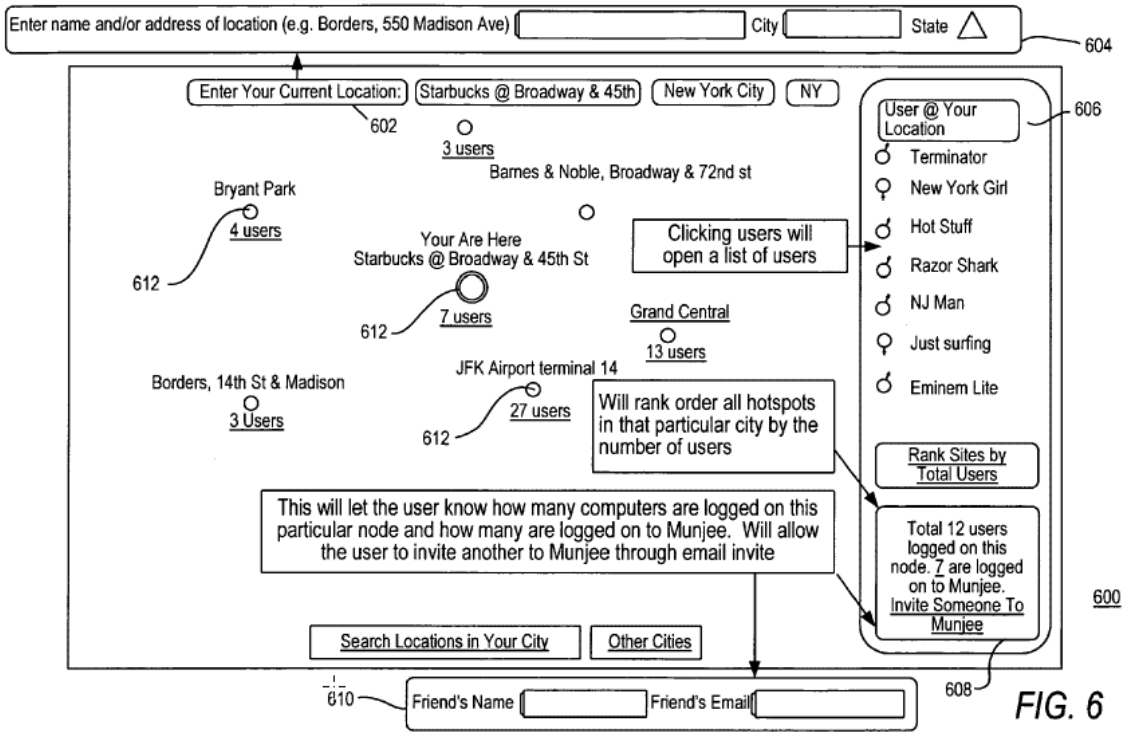


FIG. 6

Figure 6 depicts a graphical user interface displaying a webpage. *See* Ex. 1003 ¶¶ 18, 75. The webpage includes list 606 of other users by username (e.g., "Terminator," "Just surfing") at the present hotspot. *See id.* ¶ 76. List 606 includes gender symbols for each username. *See id.* at Fig. 6.

2. Entitlement of Baig to Earlier Effective Filing Date

Petitioner asserts that Baig is entitled to the November 10, 2006, earlier effective filing date of Provisional Application No. 60/858,204 (Ex. 1004, "'204 Provisional"), and is prior art to the '398 Patent under pre-AIA 35 U.S.C. § 102(e). *See* Pet. 10. Petitioner asserts that the '204 Provisional provides support for the disclosure of Baig and provides § 112 support for at least one claim in Baig. *See id.* More specifically, Petitioner asserts that there are no material differences between Baig and the '204 Provisional. *See id.* (citing Ex. 1002 ¶ 43 (citing Ex. 1005 (redline

comparison of Ex. 1003 and Ex. 1004))). Petitioner further contends that the ’204 Provisional includes 17 claims that are identical to the claims in Baig, and, therefore, provide written description support for the corresponding claims in Baig. *See id.* Petitioner also asserts the ’204 Provisional provides enablement. *See id.*

For the purpose of institution only, Petitioner has shown sufficiently that Baig is entitled to the earlier effective filing date of the ’204 Provisional Application. Although the burden of production may shift between the parties during trial, the burden of persuasion to show that Baig is entitled to an earlier effective filing date always remains with Petitioner. *See Dynamic Drinkware, LLC v. Nat’l Graphics, Inc.*, 800 F.3d 1375, 1379–80 (Fed. Cir. 2015).

3. Overview of Zwicky (Ex. 1006)

Zwicky is a textbook titled “Building Internet Firewalls,” which includes a section disclosing Network Address Translation (NAT). Ex. 1006, 3, 36. Zwicky discloses that NAT allows a network to use one set of network addresses internally and a different set of addresses with dealing with external networks. *See id.* at 36. When an internal machine sends a packet to the outside, a NAT system of a router modifies the source address of the packet to make the packet look like it is coming from a valid address. *See id.* at 37. When an external machine sends a packet to the inside, the NAT system modifies the destination address to turn the externally visible address into the correct internal address. *See id.* The NAT system also can modify the source and destination port numbers, known as Port and Address Translation (PAT). *See id.* at 37–38, Figs. 5–3, 5–4. The use of port mapping enables multiple internal machines to use the same external address. *See id.* at 38. The main purpose of NAT is to economize on

address space. *See id.* NAT also has security advantages, such as, helping to enforce the firewall's control over outbound connections, restricting incoming traffic, and concealing the internal network's configuration. *See id.* at 38–39.

4. Overview of Satapati (Ex. 1007)

Satapati is directed to a method for transparently sharing at least one Internet Protocol version 4 (IPv4) address among a plurality of hosts, where at least a first host uses IPv4 protocol and at least a second host uses Internet Protocol version 6 (IPv6) protocol. *See* Ex. 1007, code (57). Satapati discloses a system that allows a network address translator to provide network address translation between a private IPv4 network with a plurality of IPv4 users and a public network such as the Internet, which is connected to a plurality of web servers using IPv4 protocol. *See id.* at 1:49–54. The network address translator is able to provide a plurality of users Internet access using a small number of IPv4 addresses. *See id.* at 1:54–56. The network address translator uses port address translation (PAT) to multiplex a single Internet public address by port number, thereby providing user definable ports 1025–65,535. *See id.* at 1:63–2:3.

5. Overview of Hahn (Ex. 1008)

Hahn is a textbook titled "Internet Complete Reference," which includes a description of updating information automatically. *See* Ex. 1008, 3, 48. Hahn discloses that it is desirable to display information on a webpage that can be updated automatically. *See id.* at 48. The webpage can be set up so that it tells the browser to reload itself automatically, which is called CLIENT PULL. *See id.* In the alternative, the server is allowed to send new data on its own, without the browser making a request, which is

called SERVER PUSH. *See id.* Client pull and server push are useful in situations where data changes, such as financial market data. *See id.*

6. Analysis of Independent Claim 36

For the reasons that follow, we are persuaded that, for the purpose of institution, Petitioner establishes sufficiently that the combination of Baig, Zwicky, Satapati, and Hahn teaches or suggests all of the limitations recited in independent claim 36.

a. Preamble

Petitioner contends that Baig teaches "[a]n article comprising a non-transitory tangible medium encoding computer-readable instructions that, when applied to one or more computers, instruct the one or more computers to perform a method, comprising: . . ." based on Baig's disclosure of a computer memory within one or more of the content servers 124_1, 124_2, 124_n. *See* Pet. 12–13 (reproducing Ex. 1003 Fig. 1 (with annotations); citing Ex. 1002 ¶¶ 72–73; Ex. 1003 ¶ 52; Ex. 1004, 12–13).

At this stage of the proceeding, we determine Petitioner shows sufficiently that Baig teaches or suggests the preamble[9] recitation.

b. (a) receiving at one or more of the computers an electronic identifier of a first device;

Petitioner asserts that Baig in view of Zwicky and Satapati teach or suggest "receiving at one or more of the computers an electronic identifier of a first device." *See* Pet. 13–24. Petitioner asserts that Baig's discloses WiFi access point 106 that connects mobile devices 102_1 through 102_5 to content server 224 through public Internet 122, and that any one of mobile

[9] We need not decide whether the preamble recitation is limiting because Petitioner establishes a reasonable likelihood that the cited art teaches it.

devices 102_1 through 102_5 corresponds to the claimed first device. *See id.* at 13–14 (reproducing Ex. 1003, Fig. 2 (with annotations)). Petitioner contends that Baig's first mobile device has an electronic identifier which includes an IP address transmitted by the access point 106 to content server 224 over Internet 122. *See id.* at 14–15. According to Petitioner, Baig discloses that "[a]ll outgoing traffic from this hotspot will carry the IP address of the access point M, as the source IP address for all users (the access point will then sort out this traffic when it reaches the hotspots)." *Id.* at 15 (quoting Ex. 1003, Fig. 2, step 3; citing Ex. 1002 ¶ 76).

Petitioner asserts that Baig discusses NAT, which is widely known and enables an intermediary device such as an access point to receive network communications between a local device and a remote device connected to the Internet and then modify or translate their IP addresses. *See* Pet. 15–16 (quoting Ex. 1003 ¶¶ 44–46; citing Ex. 1002 ¶¶ 48, 77, 78; Ex. 1003 ¶ 43; Ex. 1006, 36–37). Petitioner contends that Baig's public IP address of access point 106 discloses an electronic identifier of a first device based on the industry standard NAT techniques mentioned in Baig. *See id.* at 17 (quoting Ex. 1003 ¶ 43; citing Ex. 1003 ¶¶ 46, 49–51).

Petitioner acknowledges that the industry standard NAT techniques are not described in detail in Baig. *See* Pet. 17 (quoting Ex. 1004 ¶ 43; citing Ex. 1004 ¶¶ 46, 49–51). Petitioner asserts that Zwicky and Satapati provide details about standard NAT techniques, including the use of a port number to identify an endpoint associated with the source and destination addresses. *See id.* at 17–19 (reproducing Ex. 1006, p. 38, Fig. 5–4; citing Ex. 1002 ¶¶ 79–82). According to Petitioner, "[t]he port number [] allows multiple distinct devices to use a single IP address yet be uniquely identified by port number when communicating over the Internet." *Id.* at 19–20 (citing

Ex. 1002 ¶ 50; Ex. 1007, 2:66–67). Petitioner asserts that the claimed "electronic identifier of a first device" is taught by the combination of the IP address of the access point or hotspot to which a first mobile device was connected and the TCP/IP port number associated with the first device, as taught by Zwicky and Satapati. *See id.* at 20 (citing Ex. 1002 ¶ 83).

For the purpose of institution and based on Petitioner's citations to Baig, Zwicky, Satapati, and Mr. Schmandt's testimony (Ex. 1002), we are persuaded Petitioner sets forth sufficient articulated reasoning with rational underpinning to support the conclusion that it would have been obvious to one of ordinary skill in the art to use the NAT port translation techniques of Zwicky and Satapati in the system of Baig. *See* Pet. 21–24; *KSR*, 550 U.S. at 418. According to Petitioner, a person of ordinary skill in the art "would [] have appreciated that the port translation techniques of Zwicky and Satapati would likely have been *required* to enable the system of Baig to function properly. . . . to uniquely identify, differentiate[,] and properly route traffic between individual mobile devices when communicating over the Internet." *Id.* at 23 (quoting Ex. 1007, 1:34–36; citing Ex. 1002 ¶ 89). According to Petitioner, "[p]ort translation would have conserved IP addresses by allowing multiple devices to communicate over the Internet while sharing a single public IP address." *Id.* at 23–24 (quoting Ex. 1006, 38; citing Ex. 1002 ¶ 90; Ex. 1007, 1:63–2:3). Petitioner also points out that "NAT provides security benefits by facilitating greater monitoring and control of incoming network traffic from the Internet, providing a further motivation to combine." *Id.* at 24 (citing Ex. 1002 ¶ 91; Ex. 1006, 38–39).

Petitioner further asserts that Baig discloses receiving at one or more of the computers the claimed first electronic identifier of the first device, based on Baig's disclosure of the content server receiving the IP address of

the access point or hotspot when the mobile device attempts to connect. *See* Pet. 20–21 (quoting Ex. 1003 ¶ 44, Fig. 2; citing Ex. 1002 ¶ 85; Ex. 1003 ¶¶ 55–57). Petitioner contends that, based on the combined teachings of Baig, Zwicky, and Satapati, the content server also would receive, along with the IP address of the access point, the port number assigned to the mobile device. *Id.* at 21.

At this stage of the proceeding, we determine Petitioner shows sufficiently that the combined teachings of Baig, Zwicky, and Satapati teaches or suggests this limitation of claim 36.

c. (b) automatically generating and storing electronic indicia of an association between the first device identifier and an electronic identifier of a second device based on automatically recognizing that each of the first and second devices was connected, independently of the other, to a common local area network, wherein the computer system is connected to the local area network through the Internet but is not in the local area network;

Petitioner contends that Baig teaches or suggests "automatically generating and storing electronic indicia of an association between the first device identifier and an electronic identifier of a second device" based on Baig's disclosure of the server determining if multiple mobile devices are connected to the same access point, as shown in Figure 3, step 306. *See* Pet. 24–26 (reproducing a portion of Ex. 1003, Fig. 3 (with annotations); quoting Ex. 1003 ¶ 56; citing Ex. 1002 ¶¶ 93–94). Petitioner asserts that it would have been apparent and obvious that Baig's content server generates and stores electronic indicia of this association as evidenced by the fact that Baig maintains a list of users whose devices are connected using the same access point IP address. *See id.* at 26 (quoting Ex. 1003 ¶ 52; citing Ex. 1002 ¶ 95; Ex. 1003 ¶ 38). Petitioner asserts that Baig's Figure 6depicts

webpage 600 presented on a mobile device that shows list 606 of users connected to the same access point. *See id.* at 26–28 (reproducing Ex. 1003, Fig. 6 (annotations added); citing Ex. 1002 ¶¶ 95–96; Ex. 1003 ¶¶ 74, 76). According to Petitioner, "[i]t would [] have been apparent and obvious that the content server will 'generate' and 'store' such electronic indicia [of the association] in order to keep track of the users that belong to a vicinity-based user group and produce list 606." *Id.* at 28 (emphasis omitted, citing Ex. 1002 ¶ 96). Petitioner also asserts Baig's process is performed automatically because the user did not take specific action to cause it to occur. *See id.* at 28–29 (quoting Ex. 1003 ¶ 59; citing Ex. 1002 ¶¶ 98–99; Ex. 1003 ¶¶ 55–56, Fig. 3).

Petitioner further contends that the automatic generation of the electronic indicia of the association is "based on automatically recognizing that each of the first and second devices was connected independently to a common local area network," because Baig's content server can detect when two or more mobile devices are connected via the same access point IP address, which means that the two or more mobile devices are connected to a common local area network. *See* Pet. 29–30 (reproducing Ex. 1003, Fig. 1 (with annotations); quoting Ex. 1003 ¶ 43 citing Ex. 1002 ¶¶ 100–101). According to Petitioner, "[i]t would [] have been obvious that the first and second mobile devices in Baig were connected 'independently of the other' to the common local area network" because "each mobile device connected to the local network has its own local or private IP address," "a mobile device can wirelessly connect to a particular access point and make a login request," and "mobile devices can connect at different times." *Id.* at 30–31 (emphasis omitted, citing Ex. 1002 ¶¶ 102–103; Ex. 1003 ¶¶ 49, 55–56, Fig. 2, step 1; Fig. 3 steps 301, 302, 306).

Petitioner also asserts that Baig teaches or suggests "wherein the computer system is connected to the local area network through the Internet but is not in the local area network." *See* Pet. 31–32. Petitioner contends that Baig's Figure 1 discloses content servers 124_1, 124_2, 124_n communicating through public Internet 122 in order to connect to local network 104 through access point 106. *See id.* (reproducing Ex. 1003, Fig. 1; citing Ex. 1002 ¶ 104; Ex. 1003 ¶ 43).

At this stage of the proceeding, we determine Petitioner shows sufficiently that Baig teaches or suggests this limitation of claim 36.

d. (c) based on the electronic indicia of the association between the first and second device identifiers, automatically sending an electronic transmission that causes another programmed hardware computer system to take an action, based on first electronic profile data associated with the first device identifier, with respect to the second device, which is indicated at the time of the action by the second device identifier.

Petitioner contends that Baig in combination with Hahn teaches or suggests

> based on the electronic indicia of the association between the first and second device identifier . . . sending an electronic transmission that causes another programmed hardware computer system to take an action, based on first electronic profile data associated with the first device identifier, with respect to the second device, which is indicated at the time of the action by the second device identifier.

See Pet. 32–40. Petitioner asserts that Baig discloses sending list 606 to the second user's mobile device, where the second mobile device displays list 606 of vicinity-based group of users connected to the same hotspot, which includes a user logged in using the first mobile device. *See* Pet. 33 (reproducing Ex. 1003, Fig. 6 (with annotations); citing Ex. 1003 ¶¶ 38, 52, 74), 34–35 (quoting Ex. 1003 ¶ 76). Petitioner points out that list 606

includes the first electronic profile data associated with a first device, including the user's username and gender symbol. *See id*. at 33–34 (reproducing Ex. 1003, Fig. 6 (with annotations); citing Ex. 1003 ¶ 80, Fig. 7), 35–36. Petitioner further points out that Baig also discloses that a user decides whether or not it wishes to be visible to other users, and, therefore, the transmission and display of list 606 is based on the first electronic profile data. *See id.* at 36–37 (quoting Ex. 1003 ¶¶ 80, 124). Petitioner asserts that that the action with respect to the second device is indicated at the time of the action by the second device identifier because the webpage with list 606 is transmitted to and displayed on the second device, which, at that point in time, is identified and connected using the access point IP address and the TCP/IP port number associated with the second device. *See id.* at 37 (citing Ex. 1002 ¶ 113).

Petitioner acknowledges that it is unclear if Baig alone discloses "automatically sending an electronic transmission," because it is unclear as to the timing and triggering with respect to how list 606 gets updated. *See* Pet. 35 (citing Ex. 1002 ¶¶ 110, 114), 37 (citing Ex. 1002 ¶ 115). Petitioner asserts that Hahn teaches displaying information which can be updated automatically by using a "CLIENT PULL" technique or a "SERVER PUSH" technique. *See id.* at 38–39 (citing Ex. 1002 ¶¶ 117–118; Ex. 1008, 48–49).

For the purpose of institution and based on Petitioner's citations to Baig, Hahn, and Mr. Schmandt's testimony (Ex. 1002), we are persuaded Petitioner sets forth sufficient articulated reasoning with rational underpinning to support the conclusion that it would have been obvious to one of ordinary skill in the art to implement Baig's list 606 such that it gets automatically updated in order to present an up-to-date and accurate list of

members of the vicinity-based group. *See* Pet. 37–40 (citing Ex. 1002 ¶¶ 114, 119–124, 185, 187, 189; Ex. 1008, 48–49, 69); *KSR*, 550 U.S. at 418. Petitioner asserts that Hahn teaches there are times when it is desirable to display information which can be updated automatically, and the CLIENT PULL and SERVER PUSH techniques are useful in situations where data changes. *See id.* at 40 (quoting Ex. 1008, 48). Petitioner contends that Baig is designed to work with locations where users commonly gather for short periods such as coffee shops and airport terminals. *See id.* (citing Ex. 1003 ¶¶ 39, 78). Petitioner also asserts that Hahn explains that automatic updates are suitable for "web-based talk facilities," in which users send messages back and forth, which is similar to Baig's chat feature. *See id.* (citing Ex. 1002 ¶ 123; Ex. 1008, 48–49, 69).

At this stage of the proceeding, we determine Petitioner shows sufficiently that Baig, Zwicky, Satapati, and Hahn teaches or suggests this limitation of claim 36.

e. Summary

For all of the foregoing reasons, for the purpose of institution and based on the record before us, Petitioner establishes sufficiently that the subject matter of claim 36 would have been obvious over Baig, Zwicky, Satapati, and Hahn.

7. Analysis of Dependent Claim 37

Claim 37 depends from claim 36. *See* Ex. 1001, 27:12–16. Petitioner asserts that Baig teaches or suggests "wherein the electronic association is recognized based on a common IP address, or portion thereof," as recited in claim 37, based on Baig's disclosure of determining that two mobile devices are connected through the common IP address of the access point. *See* Pet. 41 (citing Ex. 1003 ¶¶ 38, 52, 56). Petitioner contends that Baig teaches

or suggests "wherein network traffic is routed via the common IP address for each of the first and second devices when each is connected to the local area network," as recited in claim 37, based on Baig's disclosure of access point 106 that includes NAT router 108 that routes network traffic using the access point's public IP address, when each mobile device is connected to the local area network. *See id.* (citing Ex. 1002 ¶ 126; Ex. 1003 ¶¶ 46–47).

At this stage of the proceeding, we determine Petitioner shows sufficiently that Baig teaches or suggests the limitations of claim 37. For the purpose of institution and based on the record before us, including the reasons explained above addressing claim 36, Petitioner establishes sufficiently that the subject matter of claim 37 would have been obvious over Baig, Zwicky, Satapati, and Hahn.

8. Summary

For all of the foregoing reasons, based on the record before us, we determine there is a reasonable likelihood Petitioner would prevail in showing that claims 36 and 37 are unpatentable under 35 U.S.C. § 103 over Baig, Zwicky, Satapati, and Hahn. Although Patent Owner elected not to file a preliminary response, we note that the burden remains on Petitioner to demonstrate unpatentability. *See Dynamic Drinkware*, 800 F.3d at 1378.

E. Challenge to Claims 36 and 37 over Baal-Haness and Appelman

1. Overview of Baal-Haness (Ex. 1010)

Baal-Haness is directed to internet web-based personal communications, applications, and services, wherein visitors participate in chat rooms and instant messaging. *See* Ex. 1010 ¶ 1. Entrants to a website are divided into segments or area networks (ANs) based upon common interests, locations, business, or other factors, and permits segmentation by

network IP address, subnetwork IP address, or any other categorization or identification data. *See id.* ¶ 35. Segmentation of users into LANs can be achieved by utilizing the network IP address during the login process. *See id.* ¶¶ 36–39. During the login process, the user inserts a username or nickname and clicks on the login button. *See id.* ¶ 39. The user's network address is automatically sent to the application server, and if there is a database for that IP address, the username is added to that database. *See id.* ¶ 39, Fig. 3. If there is no database for that IP address, a database is created for that IP address and the username is added to that database. *See id.*

Figure 1 of Baal-Haness is reproduced below.

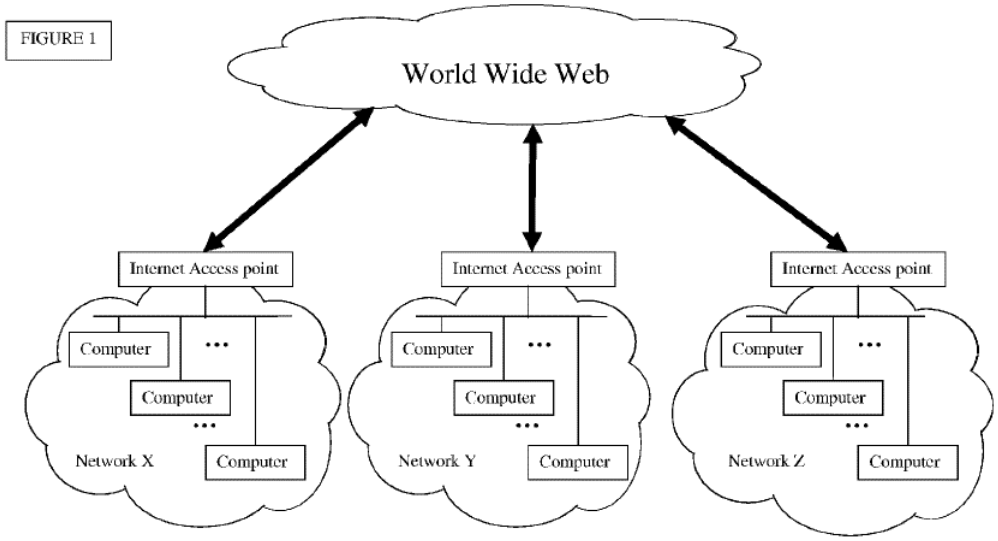


Figure 1 depicts the separation of area networks and the access from internal area networks to the World Wide Web. *See* Ex. 1010 ¶¶ 49–50.

2. Overview of Appelman (Ex. 1009)

Appelman is directed to dynamically informing a user of a large-scale network of other users including dynamically determining an online context of other users. *See* Ex. 1009, code (57). The online context may be based on the online presence of the user, such as presence at a particular URL, chat room, message board, or newsgroup. *See id.* at 2:30–33. An identification

service identifies individuals within an online context and includes mechanisms to log an individual's entry within and exit from the online context. *See id.* at 2:40–44, 4:1–6. An information storage service stores trait information, identification information and/or contact information indicative of the other users identified within an online context of the user. *See id.* at 2:48–52, 4:7–11.

Figure 3 of Appelman is reproduced below.

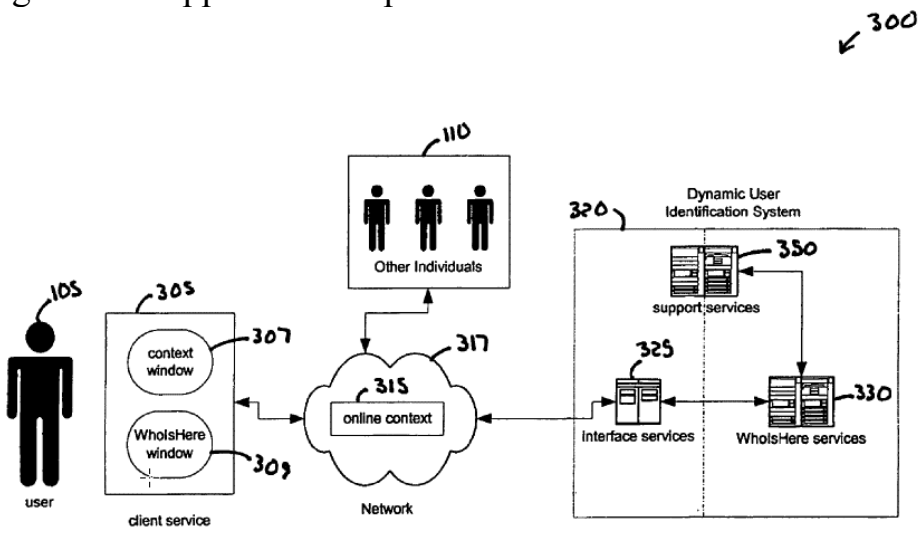


Figure 3 depicts a schematic diagram of a user identification system. *See* Ex. 1009, 1:41–42, 4:24. Generalized system 300 includes dynamic user identification system 320 having a WhoIsHere service 330 to dynamically identify to user 105 at client service 305 at least one other individual 110 also within online context 315 of large-scale network 317. *See id.* at 4:24–28, 7:59–62, 8:10–12. Client service 305 is configured to provide user 105 online access to network 317 and includes context window 307 associated with online context, and WhoIsHere window 309 associated with WhoIsHere service 330. *See id.* at 4:31–35.

Dynamic user identification system 320 includes front-end 321 and back-end 323 that may or may not be incorporated within the same hardware or software device. *See* Ex. 1009, 7:17–22. Front-end 321 includes one or

more interface services that communicate online activity of the user or other individuals to one or more WhoIsHere services 330 or support services 350 of back-end 323. *See id.* at 7:29–34. Interface services 325 communicate service requests from client service 305 to back-end 323 and to client service 305 informing user 105 of one or more other individuals 110. *See id.* at 7:34–37. Interface services 325 communicates information to the WholsHere services 330 identifying the online context 315 of the user 105 and information based upon a current online location or online activity of user 105. *See id.* at 7:38–45.

Figure 6 of Appelman is reproduced below.

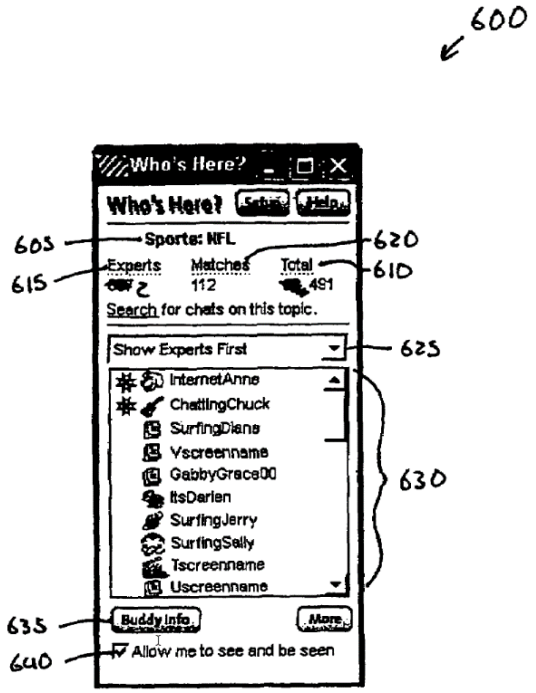


Figure 6 depicts an exemplary graphical user interface (GUI) window to dynamically and in real time identify a list of other users currently accessing the same online NFL sports channel as the online user viewing the GUI window. *See* Ex. 1009, 1:48–50, 2:6–9, 12:58–60. GUI window includes WhoIsHere window 600 that indicates a Sports:NFL context 605, total count 610 of other individuals within Sports:NFL context 605, number of

individuals 615 within the Sports:NFL context 605 who are NFL experts, and other individuals 620 within context 605 whose interests match a specified interest of user 105. *See id.* at 12:60–67.

3. Analysis of Independent Claim 36

For the reasons that follow, we are persuaded that, for the purpose of institution, Petitioner establishes sufficiently that the combination of Baal-Haness and Appelman teaches or suggests all of the limitations recited in independent claim 36.

a. Preamble

Petitioner contends that Bal-Haness teaches "[a]n article comprising a non-transitory tangible medium encoding computer-readable instructions that, when applied to one or more computers, instruct the one or more computers to perform a method, comprising: . . ." based on Baal-Haness's disclosure of a computer memory within an application server that stores software for operating a website that separates users into different area networks and provides services to the users. *See* Pet. 50–51 (quoting Ex. 1010 ¶¶ 16, 39, 40, 46; citing Ex. 1002 ¶ 146). At this stage of the proceeding, we determine Petitioner shows sufficiently that Baal-Haness teaches or suggests the preamble[10] recitation.

b. (a) receiving at one or more of the computers an electronic identifier of a first device;

Petitioner asserts that Baal-Haness teaches or suggests "receiving at one or more of the computers an electronic identifier of a first device," based on Baal-Haness's disclosure in Figure 1 of three networks each containing

[10] We need not decide whether the preamble recitation is limiting because Petitioner establishes a reasonable likelihood that the cited art teaches it.

an Internet Access point connected to computers within each respective network, where each computer within a particular area network has an electronic identifier which is a user's username and the network IP address. *See* Pet. 51–54 (reproducing Ex. 1010, Fig. 1; quoting Ex. 1010 ¶¶ 37–39; citing Ex. 1002 ¶ 149; Ex. 1010 ¶¶ 49–50). At this stage of the proceeding, we determine Petitioner shows sufficiently that Baal-Haness teaches or suggests this limitation of claim 36.

c. (b) automatically generating and storing electronic indicia of an association between the first device identifier and an electronic identifier of a second device based on automatically recognizing that each of the first and second devices was connected, independently of the other, to a common local area network, wherein the computer system is connected to the local area network through the Internet but is not in the local area network;

Petitioner contends that Baal-Haness teaches or suggests "generating and storing electronic indicia of an association between the first device identifier and an electronic identifier of a second device" based on Baal-Haness's disclosure of a server, after receiving a login request, determining whether the IP address of the user's area network already exists in the database, and if, so, adding the logging-on user to that database. *See* Pet. 54–57 (reproducing Ex. 1010, Fig. 3 (with annotations); quoting Ex. 1010 ¶¶ 37–39; citing Ex. 1010 ¶¶ 36, 38). Petitioner asserts that a person of ordinary skill in the art would have understood that, when a database for an IP address already exists, another user may have already logged in using the network IP address, in which case a new user's username is added to the existing database. *See id.* at 57 (quoting Ex. 1010 ¶ 51; citing Ex. 1002 ¶ 151; Ex. 1003 ¶¶ 37, 47). Petitioner further contends that Baal-Haness's process is performed automatically because the user does not take

specific action to cause it to occur. *See id.* at 57–58 (quoting Ex. 1010 ¶ 40; citing Ex. 1002 ¶¶ 99, 152–153; Ex. 1010 ¶ 39).

Petitioner also contends that the generation of the electronic indicia of the association is "based on automatically recognizing that each of the first and second devices was connected . . . to a common local area network," based on Baal-Haness' disclosure of using the network IP address to determine that two users are on the same local area network. *See* Pet. 58–59 (quoting Ex. 1010 ¶¶ 36–38; citing Ex. 1002 ¶ 154; Ex. 1010 ¶¶ 30, 35). According to Petitioner, "[i]t would [] have been obvious that each of the first and second devices in Baal-Haness was connected 'independently of the other' to the common local area network" based on Baal-Haness's Figure 1 "which shows three area networks (ANs) and computers connected within those networks," and because the "computers in Baal-Haness need not be logged into the website at the same time." *Id.* at 59–60 (emphasis omitted, reproducing Ex. 1010, Fig. 1; citing Ex. 1002 ¶¶ 155–156).

Petitioner asserts that Baal-Haness teaches or suggests "wherein the computer system is connected to the local area network through the Internet but is not in the local area network," based on Baal-Haness's Figure 1 showing computers in each network that can connect to the World Wide Web which sits outside the local area networks. *See* Pet. 60 (citing Ex. 1002 ¶ 157; Ex. 1010, Fig. 1). According to Petitioner, "[i]t would have been apparent and obvious that the server in Baal-Haness ('the computer system'), which creates the website, is connected to the local area network via the World Wide Web as depicted in Figure 1." *Id.* (emphasis omitted, citing Ex. 1002 ¶ 157; Ex. 1010 ¶¶ 16–17, 28).

At this stage of the proceeding, we determine Petitioner shows sufficiently that Baal-Haness teaches or suggests this limitation of claim 36.

d. (c) based on the electronic indicia of the association between the first and second device identifiers, automatically sending an electronic transmission that causes another programmed hardware computer system to take an action, based on first electronic profile data associated with the first device identifier, with respect to the second device, which is indicated at the time of the action by the second device identifier.

Petitioner contends that Baal-Haness in combination with Appelman teaches or suggests

> based on the electronic indicia of the association between the first and second device identifier automatically sending an electronic transmission that causes another programmed hardware computer system to take an action, based on first electronic profile data associated with the first device identifier, with respect to the second device, which is indicated at the time of the action by the second device identifier.

See Pet. 60–68. Petitioner asserts that, after the user is logged in using Baal-Haness's process, the user can access particular services and interact with other users who are also connected to the same local area network. *See id.* at 61 (citing Ex. 1010 ¶¶ 40–43). Petitioner acknowledges that Baal-Haness does not describe these features in detail, and relies on the teachings of Appelman to provide details. *See id.*

Petitioner contends that Appelman determines an online context for a user and identifies other users present with the same online context. *See* Pet. 61–62 (reproducing Ex. 1009, Fig. 6; citing Ex. 1009, 2:27–42). Petitioner asserts that Appelman discloses that users can be identified based on a wide variety of online contexts including viewing the same webpage or being present in a particular chat room. *See id.* at 62 (citing Ex. 1009, 1:61–63, 2:30–33). Petitioner contends that Appelman discloses dynamic user identification system 320 that includes WhoIsHere services 330 and interface services 325. *See id.* at 62–63 (reproducing Ex. 1009, Fig. 3).

Petitioner asserts that WhoIsHere services 330 forms part of back-end 323 and is responsible for determining the other individuals presently within the online context and informing the user of at least one of the other individuals. *See id.* (quoting Ex. 1009 7:59–62; citing Ex. 1009, 7:17–19). Petitioner contends WhoIsHere services 330 do not directly send the information to the user, but rely on interface services 325 which form part of front-end 321 and are responsible for communicating information to the client. *See id.* (quoting Ex. 1009, 7:36–37 citing Ex. 1009, 7:17–18, 7:29–30, 7:34–37, 8:1–4). Petitioner asserts that the user at the client device, in turn, can be informed of the other users via a list, pop-up window or other means. *See id.* at 63–64 (citing Ex. 1009, 4:15–23). According to Petitioner, "Appelman [] makes clear that WhoIsHere services 330 and interface services 325 can be implemented using two separate computer systems." *Id.* at 64 (quoting Ex. 1009, 7:18–22; citing Ex. 1009 7:22–29). Petitioner contends that Appelman discloses that the communication of the list to interface services 325 is done automatically, such as, when the membership to the list changes, or at a particular interval. *See id.* (quoting Ex. 1009, 8:12–22). Petitioner further asserts that Appelman teaches the ability to identify not only users within the same online context as the user, but to filter those users based on traits or characteristics of the users. *See id.* at 64–65 (citing Ex. 1002 ¶ 165; Ex. 1009, 1:63–2:5, 2:62–3:2, 3:32–4:26).

Petitioner asserts that, based on the combined teachings of Baal-Haness and Appelman, after the first user in Baal-Haness logs in and is assigned to the appropriate area network, the second user connected to the same area network would have been informed of the presence of the first user, for example, by showing the first user in a list or pop-up window as disclosed by Appelman. *See* Pet. 65 (citing Ex. 1002 ¶ 166; Ex. 1009,

4:15–23). Petitioner also contends that, based on the combined teachings of Baal-Haness and Appelman, Appelman's back-end system, such as WhoIsHere services 330, automatically communicates a list of other users from the same network to front end system, such as interface services 325, which in turn sends the list to the second device for display. *See id.* at 65–66 (citing Ex. 1002 ¶ 167). Petitioner further asserts that, based on the combined teachings of Baal-Haness and Appelman, the first user in Baal-Haness would only have been displayed to the second user if the first user met the criteria specified by the second user, and would have been based on first electronic profile data associated with the first device identifier. *See id.* at 66 (citing Ex. 1002 ¶ 168; Ex. 1009, 1:63–2:5)

For the purpose of institution and based on Petitioner's citations to Baal-Haness, Appelman, and Mr. Schmandt's testimony (Ex. 1002), we are persuaded Petitioner sets forth sufficient articulated reasoning with rational underpinning to support the conclusion that it would have been obvious to one of ordinary skill in the art to combine the teachings of Baal-Haness with Appelman to enhance the system of Baal-Haness to include the features of Appelman. *See* Pet. 65–67; *KSR*, 550 U.S. at 418. Petitioner asserts that a person of ordinary skill in the art would have been motivated to enhance Baal-Haness to allow for automatic notification of other users logged into an area network website. *See id.* at 66–67 (citing Ex. 1002 ¶ 170). Petitioner asserts that Baal-Haness teaches the ability of users in an area network to participate in a chat room or instant message exchanges, and these features would have benefited from the enhancement taught by Appelman by notifying users of the area network of other users who are available for interaction. *See id.* at 67 (quoting Ex. 1009, 2:30–33; citing Ex. 1002 ¶ 170; Ex. 1009, 4:15–23; Ex. 1010 ¶¶ 41–43). Petitioner further contends that a

person or ordinary skill in the art would have been motivated to use demographic information of the first user to decide whether to inform the second user of the first user's presence, because "identifying users who have 'a common age grouping or common demographic identifier' can provide a 'more focused and relevant disclosure' to the user." *Id.* (quoting Ex. 1009, 3:25–32 (emphasis omitted); citing Ex. 1002 ¶¶ 141, 171; Ex. 1010 ¶¶ 44–45). According to Petitioner, "Appelman's targeting features would have allowed a user of Baal-Haness to locate and focus its attention on other users in the area network who have common or desired characteristics." *Id.* (citing Ex. 1002 ¶ 171).

At this stage of the proceeding, we determine Petitioner shows sufficiently that the combined teachings of Baal-Haness and Appelman teaches or suggests this limitation of claim 36.

e. Summary

For all of the foregoing reasons, for the purpose of institution and based on the record before us, Petitioner establishes sufficiently that the subject matter of claim 36 would have been obvious over Baal-Haness and Appelman.

4. Analysis of Dependent Claim 37

Claim 37 depends from claim 36. *See* Ex. 1001, 27:12–16. Petitioner asserts that Baal-Haness teaches or suggests "wherein the electronic association is recognized based on a common IP address, or portion thereof," as recited in claim 37, based on Baal-Haness's disclosure of a server recognizing the electronic association based on two or more computers having the IP address associated with a particular area network and creates the electronic association by storing the usernames associated with the first

and second devices in the common database assigned to the network IP address used by both devices. *See* Pet. 68–69 (quoting Ex. 1010, Fig. 3, ¶ 39; citing Ex. 1002 ¶ 175). Petitioner further contends that Baal-Haness teaches or suggests "wherein network traffic is routed via the common IP address for each of the first and second devices when each is connected to the local area network," as recited in claim 37. *See id.* at 69 (quoting Ex. 1010 ¶ 39 (step 3); citing Ex. 1002 ¶ 175).

At this stage of the proceeding, we determine Petitioner shows sufficiently that Baal-Haness teaches or suggests the limitations of claim 37. For the purpose of institution and based on the record before us, including the reasons explained above addressing claim 36, Petitioner establishes sufficiently that the subject matter of claim 37 would have been obvious over Baal-Haness and Appelman.

5. Summary

For all of the foregoing reasons, based on the record before us, we determine there is a reasonable likelihood Petitioner would prevail in showing that claims 36 and 37 are unpatentable under 35 U.S.C. § 103 over Baal-Haness and Appelman. Although Patent Owner elected not to file a preliminary response, we note that the burden remains on Petitioner to demonstrate unpatentability. *See Dynamic Drinkware*, 800 F.3d at 1378.

F. Remaining Challenges to Patentability

As set forth in the above detailed analysis, after considering the evidence and arguments presented in the Petition, we determine that Petitioner demonstrates a reasonable likelihood of prevailing in showing claims 36 and 37 are unpatentable under 35 U.S.C. § 103 as obvious over Baig, Zwicky, Satapati, and Hahn, as well as over Baal-Haness and

Appelman. *See* 35 U.S.C. § 314; 37 C.F.R. § 42.4(a). Accordingly, we institute an *inter partes* review of all of the challenged claims on all grounds articulated in the Petition, including the patentability challenges to claims 36 and 37 based on Baig, Zwicky, Satapati, Hahn, and Appelman, and based on Baal-Haness, Appelman, Zwicky, and Satapati. *See SAS Inst. Inc. v. Iancu*, 138 S. Ct. 1348 (2018); Guidance on the Impact of SAS on AIA Trial Proceedings (Apr. 26, 2018), https://www.uspto.gov/patents-application/process/patent-trial-and-appeal/board/trials/guidance-impact-sas-aia-trial.

III. CONCLUSION

For the foregoing reasons, we determine there is a reasonable likelihood that Petitioner would prevail in showing at least one of the challenged claims of the '398 Patent is unpatentable.

IV. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that, pursuant to 35 U.S.C. § 314(a), an *inter partes* review of claims 36 and 37 of the '398 Patent is instituted with respect to all grounds set forth in the Petition; and

FURTHER ORDERED that pursuant to 35 U.S.C. § 314(c) and 37 C.F.R. § 42.4(b), *inter partes* review of the '398 Patent shall commence on the entry date of this Order, and notice is hereby given of the institution of a trial.

PETITIONER:

Heidi Keefe
hkeefe@cooley.com

Phillip Morton
pmorton@cooley.com

Andrew Mace
amace@cooley.com

PATENT OWNER:

Reza Mirzaie
rmirzaie@raklaw.com

Jonathan Link
jlink@raklaw.com

Trials@uspto.gov
571-272-7822

Paper No. 16
Entered: June 2, 2023

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

META PLATFORMS, INC.,
Petitioner,

v.

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

IPR2022-00773
Patent 8,677,398 B2

Before KRISTEN L. DROESCH, THOMAS L. GIANNETTI, and STACEY G. WHITE, *Administrative Patent Judges.*

DROESCH, *Administrative Patent Judge*.

TERMINATION
Due to Settlement After Institution of Trial
35 U.S.C. § 317; 37 C.F.R. § 42.74

I. DISCUSSION

Pursuant to authorization by the Board, the parties filed the following: (1) a Joint Motion to Terminate the proceeding (Paper 15) and (2) a true copy of the parties' settlement agreement (Ex. 2007). Subsequently, Amazon[1] requested a conference call with the Board because Amazon filed a "copy-cat" Petition and Motion for Joinder to this proceeding in IPR2023-00227. *See* IPR2023-00227, Papers 2, 3. On April 17, 2022 the Board held a conference call with counsel for the parties, as well as counsel for Amazon. During the conference call, Amazon requested that the Board delay termination of this proceeding to allow the Board to issue a decision on Amazon's Petition and Motion for Joinder in IPR2023-00227.

Oral argument has not been held, and a final written decision has not been entered. In the Joint Motion to Terminate, the parties indicate that they have settled all their disputes between them regarding U.S. Patent No. 8,677,398, including those relating to this proceeding and the related district court action, and have agreed to terminate the proceeding. *See* Paper 15, 1–2. In addition, "[t]he Parties certify that there are no other collateral agreements or understandings, oral or written, between the Parties made in connection with, or in contemplation of, the termination of this proceeding." *Id.* at 3. Under these particular circumstances, we determine that it is appropriate to terminate the proceeding without rendering a final written decision. *See* 35 U.S.C. § 317; 37 C.F.R. § 42.72.

[1] Amazon.com, Inc., Amazon Web Services, Inc., and Amazon.com Services LLC. IPR 2023-00227, Paper 2, 6.

II. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that the Joint Motion to Terminate (Paper 15) is *granted*, and the proceeding is terminated.

PETITIONER:

Heidi Keefe
hkeefe@cooley.com

Phillip Morton
pmorton@cooley.com

Andrew Mace
amace@cooley.com

PATENT OWNER:

Reza Mirzaie
rmirzaie@raklaw.com

Jonathan Link
jlink@raklaw.com